# DCS SOLUTIONS CATALOG

Datapro Computer Systems

*The Total Enterprise IT Solution and Service Provider*

CALL: 02-684-8408

Datapro Computer Systems Co., Ltd. (DCS) is a subsidiary of Premier Technology Public Company Limited under the Premier Group of Companies. DCS is Thailand's leading Enterprise IT Solutions and Services provider. With years of experience since 1986 and a deep understanding of the technological landscape, DCS is committed to delivering innovative and reliable IT solutions that meet the dynamic needs of businesses across various industries.

Our mission is to empower organizations by providing cutting-edge IT Solutions that drive efficiency, enhance security, and foster growth. We pride ourselves on our ability to deliver comprehensive IT services, from initial consultation and solution design to implementation and ongoing support.

As a testament to our commitment to excellence, DCS has earned numerous certifications and recognitions, establishing itself as a trusted partner in the IT sector. Our partnerships with world-leading IT vendors ensure that we offer only the best solutions to our clients.

Code of Conduct

Supplier
Code of Conduct

Anti-Corruption
Policy

PDPA Policy

Premier Technology PCL

# Our Represented Brands


## Our Own Brands

# Solution Index

## Brand Index

| Brand | Solutions / Products / Services | | Page |
|---|---|---|---|
| **ManageEngine** | IT Service Solution | IT Service Solution | 63 |
| **Microsoft** | IT Infrastructure | Virtualization | 60 |
| | | Active Directory | 50 |
| | | Email | 54 |
| | IT Service Solution | Office365 | 64 |
| | OS & Database | Product | 79 |
| | Software Tools | Product | 83 |
| **N2N Solution Provider** | Digital Transformation | OCR | 49 |
| **Netcode** | Collaboration & Contact Center | Collaboration | 3 |
| **NetScaler** | Cyber Security | Load Balancer | 21 |
| **Newline** | Innovative Workplace | Meeting room solution<br>Classroom solution | 49 |
| **NICE** | Collaboration & Contact Center | Contact Center | 5 |
| | Digital Transformation | Digital Process Automation | 48 |
| **Nutanix** | Server & Storage | | 82 |
| **OneSpan** | Cyber Security | Multi Factor Authentication | 22 |

| Brand | Solutions / Products / Services | | Page |
|---|---|---|---|
| **Razr** | Innovative Workplace | Meeting room solution<br>Classroom solution | 50 |
| **Recorded Future** | Cyber Security | Threat Intelligence Service | 37 |
| **RedHat** | IT Infrastructure | Container Platform | 51 |
| | | IT Automation | 54 |
| | Middleware | Product | 65 |
| | OS & Database | Product | 79 |
| **RSA** | Cyber Security | Multi-factor Authentication | 23 |
| **Sangfor** | Cyber Security | Next Generation Firewall | 30 |
| | | Web Security | 40 |
| **Schneider** | IT Infrastructure | Data Center Solution | 52 |
| | | Data Center Monitoring | 52 |
| **ScreenBeam (Barbados) Inc.** | Innovative Workplace | Meeting room solution<br>Classroom solution | 50 |
| **SentinelOne** | Cyber Security | AD Protection | 6 |
| | | Asset Discovery | 9 |
| | | Deception Protection | 13 |
| | | Endpoint Security | 16 |
| | | Threat Hunting Service | 37 |
| | | XDR | 45 |
| **ServiceNow** | IT Service Solution | IT Operation Management | 63 |
| | | IT Service Management | 63 |
| | Risk & Compliance | Integrated Risk Management | 80 |

| Solution | Brand | Product / Service | Description |
|---|---|---|---|
| **Collaboration & Contact Center** | | | |
| Collaboration | Bainisys | Bainisys Advanced Call Management (BACM) | Bainisys Advanced Call Management (BACM) is a powerful accounting and reporting tool for Cisco Voice over IP (VoIP) Communication Manager which collects Call Detail Records (CDR) from the Communication Manager. It also provides searching from CDR's and reporting through an advanced filtering engine. These reports can be created and scheduled to analyze and monitor the usage of the IP Telephone in each department or even individual user.<br><br>It also enables IT administrators to monitor their VoIP network for voice quality, call traffic and keep track of active calls and failed calls. |
| | Cisco | Cisco Desk Series | The all-in-one collaboration and productivity device for your desk—at home, in the office, or in a shared space. It is purpose-built for collaborating, whether you're in a meeting, sharing your laptop screen, or brainstorming with a teammate. The Desk device features a 24-inch, interactive 1080p display, 64-degree 8MP camera, full-range speaker, and a mic array with AI-powered background noise removal.<br><br>This powerful device creates a clutter-free desk space, enabling you to be organized and productive. Manage your workday with dynamic layouts and custom views, take the strain off your laptop, and optimize your meetings—all from a single system. Meet without distractions or background noise. Rock a presentation with immersive sharing. Co-create with digital whiteboarding and live content annotations.<br><br>Easy setup and management capabilities allow customers to deploy and support thousands of devices at once. And with Control Hub you'll gain insight into environmental health and device usage with the ability to triage issues from anywhere. |
| | | Cisco Headset | These headsets are designed for mobile or office workers, enabling productivity in any environment with superior audio, adaptive noise cancellation, enterprise-grade security, and a sleek microphone design. Deep integrations with Cisco collaboration applications and devices allow for intuitive user experiences and intelligent IT headset management. |
| | | Cisco IP Phones | Cisco IP Phones empower your business with a new collaboration experience that connects you with the right people, with the right information at the right time, so you can accelerate team performance and maximize your business results. Effective collaborative experiences among individuals and teams can help you harness the power of your busy professional staff by enabling them to collaborate confidently with customers, partners, colleagues, and suppliers. |
| | | Cisco Microphones | Bring directional, crisp voice pickup into meeting rooms for a fully immersive, undisrupted sound experience for remote participants.<br>• Table Microphone / Table Microphone pro<br>• Celling Microphone |

| Solution | Brand | Product / Service | Description |
|---|---|---|---|
| | | Cisco Room Navigator | Simplicity, inside and out : Transform your workplace with simple and intelligent experiences while eliminating the friction from the in-office journey. Running natively on Cisco RoomOS or Microsoft Teams, the Cisco Room Navigator table-stand and wall-mount touch device is a purpose-built room peripheral designed to bring ease and convenience into modern workspaces via instant access to conference controls, smart room booking, room controls, and your go-to workspace experience apps. |
| | | Cisco Room Series | The Room Series runs on RoomOS, the hybrid work platform optimized for a native Webex experience while supporting seamless join to third-party meeting solutions like Microsoft Teams, Zoom and Google Meet. These intelligent video collaboration systems bring your meeting rooms to life. Whether you are redesigning your workspaces or upgrading your video conferencing equipment, the Room Series offers high-quality video, crisp audio, rich content experiences and embedded room intelligence to power engaging and productive hybrid workflows. |
| | | Cisco Unified Border Element | Session border control for any company size. Get highly secure voice and video connectivity from the enterprise IP network to service provider SIP trunks. Cisco Unified Border Element (CUBE) performs the four critical functions of a session border controller: session control, security, interworking, and demarcation. Migrate to SIP in a way that works for your business by controlling the pace and strategy.<br><br>Cisco Unified Border Element (CUBE) version 14 is an enterprise-class Session Border Controller (SBC) solution that makes it possible to connect and interwork large, midsize, and small business unified communications networks with public and private IP communication services.<br><br>As a licensed feature set of Cisco IOS® XE Software, CUBE has a wide range of capabilities that may be used to secure, monitor, and maintain business-critical connections and to ensure compliance with industry standards. Collectively, CUBE features provide exceptional flexibility when architecting highly available enterprise communications networks that save money and offer richer voice and video collaboration experiences to users. |
| | | Cisco Unified Communication Manager | Cisco Unified Communications Manager is the heart of Cisco collaboration services, enabling session and call control for video, voice, messaging, mobility, instant messaging, and presence.<br><br>Telephony remains a critical part of doing business for many organizations and supporting remote work from a voice and unified communications perspective remains a top priority for Cisco.<br><br>Cisco® Unified Communications Manager (UCM) is the core of Cisco's collaboration portfolio. UCM has a rich feature set that supports calling, mobility, conferencing, and messaging |

| Solution | Brand | Product / Service | Description |
|---|---|---|---|
| | | | features. Release 14 of UCM extends the product with new features for remote workers.<br><br>UC Manager is the industry leader in enterprise call and session management platforms, with more than 300,000 customers worldwide, and more than 120 million Cisco IP phones and soft clients deployed |
| | | Cisco Unity Connection | Cisco Unity Connection is a robust unified messaging and voicemail solution that provides users with flexible message access options and IT with management simplicity.<br><br>Cisco Unity Connection lets users access and manage messages from an email inbox, web browser, Cisco Jabber, Cisco Unified IP Phone, smartphone, or tablet. Unity Connection also provides flexible message access and delivery format options, including support for voice commands, speech-to-text transcription, and even video greetings.<br><br>Cisco Unity Connection is highly secure. It is designed for complex distributed global deployments with support for high availability, redundancy, and branch office survivability. It is fully virtualized and can be run on specification-based hardware. |
| | | Cisco Voice Gateway | With Cisco VG Gateways, you can enjoy the benefits of unified communications while using your existing analog devices, including analog phones and fax machines. There's no need to replace your entire phone system. Cisco VG Series Gateways help you migrate at your own pace and budget by taking full advantage of the investments you have already made. |
| | | Webex Meetings | Webex Suite. Integrated, effortless collaboration.<br>Meeting, messaging, calling, events, and more all on one secure platform built for modern hybrid work. Maximize teamwork. Minimize costs.<br><br>One suite of solutions for seamless collaboration<br>• Calling / Meeting / Messaging / Polling /Webinars / Event / Whiteboarding / Video Messaging |
| | Netcode | Intellibill | The call accounting and billing can report call activity and tightly integrate with your Cisco Unified Communications Manager to ease administration and enjoy the benefits of IP telephony solutions.<br><br>Intellibill will provide you with visibility into your IP telephony usage, including graphical and text reports, as well as extensive details or summaries at the cluster-wide, Department, Trunk, or Individual level.<br><br>With a web-based interface, administrators can access Intellibill from a laptop, desktop, tablet, or anywhere on the network using a standard web browser.<br><br>Intellibill's exclusive design for the Cisco solution provides call activity information for external, incoming, and internal calls. Reports can be seen as graphical and exportable for further processing as PDF, XLS, and CSV. |

| Solution | Brand | Product / Service | Description |
|---|---|---|---|
| | Poly | Poly Headset/Plantronics Headset | Poly/Plantronics creates premium audio and video products so you can have your best meeting and collaboration — anywhere, anytime, every time. Our headsets are beautifully designed and engineered to connect people with incredible clarity. They work seamlessly with leading hybrid work platforms. And our union with HP means they also are part of an ecosystem of innovative and easy-to-use solutions and services that simplify hybrid working. Why just show up when you can stand out? |
| Contact Center | Calabrio | Calabrio Voice Recording | Calabrio Call Recording is an enterprise recording solution that allows you to prove adherence to regulations, clear up transaction disputes, and defend the interest of the business while still upholding excellence in customer service. Calabrio Call Recording captures and stores each transaction securely to protect private data and meet mandatory security regulations and recommended guidelines:<br>• Visibility to recordings can be restricted to users with maximum security clearance, or access can be provided to other specific roles.<br>• Recordings are compressed using voice-specific algorithms before they're sent to the designated storage device, allowing you to maximize your investment in storage devices.<br>• Meets PCI (Payment Card Industry) data security standards, including flexible API for start, stop and pause of recording |
| | Cisco | Unified Contact Center Express | Cisco Unified Contact Center Express (CCX) helps businesses and organizations deliver a connected digital experience, enabling contextual, continuous, and capability-rich journeys for your customers, across time and channels. This easy-to-deploy and easy-to-use solution supports up to 400 agents and is designed for midmarket companies or enterprise branch offices. Secure and highly available, it supports powerful agent- based services and fully integrated self-service applications, including Automatic Call Distributor (ACD), Interactive Voice Response (IVR), Computer Telephony Integration (CTI), and digital channels including email and chat, and customer experience management tools. |
| | | Webex Contact Center | Webex Contact Center is a next-generation cloud contact center solution inspired by customers and architected for business. Designed and built from its foundation as a Software-as-a-Service (SaaS) cloud solution, Webex Contact Center's best-of-breed platform architecture brings your business the innovation, flexibility, scalability, and agility of the cloud without sacrificing security. As a cloud-based subscription, Webex Contact Center enables rapid time to market and time to new revenue while minimizing upfront capital investment. |
| | | Webex Workforce Optimization | Webex Workforce Optimization transforms the supervisor experience, giving supervisors access to more data and more powerful tools in simplified and flexible views so they are better equipped to lead their teams in delivering exceptional customer experiences. The powerful Webex Workforce Optimization suite of applications includes:<br>• Call Recording and Quality Management |

| Solution | Brand | Product / Service | Description |
|---|---|---|---|
| | | | • Workforce Management Analytics |
| | DCS | Case management | Case management and incident tracking system. Enables users to open tickets and log information for task tracking which can be dynamically initiated from web portal and/or API-based triggers. Also provides user activity for supervisors to determine team performance, analyze issues handling. |
| | | Chat Bot Systems | Rule-based chatbot with workflow and productivity tracking. Integration with Cisco Webex to enable logging task progress step-by-step with state transition. Productivity and provides guideline for work optimization as benefit. |
| | | Contact Center Chat Integration | Chat channel queue distributed system for handling customer chat request and assign to designated agents by given conditions, similar to telephony channel. Integrates with multiple popular social platforms and simplified chat experience to agents. |
| | | Contact Center Customization | Unified smart agent platform integrates various customer channels into the single application. Enable agents to work with less distraction by less windows switching and more productivity by improved on information focusing. |
| | | Knowledge Base Management | Provides resources, documents, training manuals and/or frequently asked questions as shared information between users in the organization to enable self-service. Features with rich-content editor and file uploading. Able to integrate with external services and/or tailor-made customized pages. |
| | Jabra | Jabra Headset | Contact Centre headsets Keeping customers satisfied, one crystal-clear call at a time Our range of professional contact center headsets work in complete harmony with your people and your platforms. So your agents can focus on helping your customers, whether they're working from the contact center or their coach. That means happier customers, happier agents, and more efficient contact centers. |
| | NICE | NICE CXOne | NICE CXOne is a cloud-based call center software that helps businesses to maximize the quality of leads and minimize the cost of client interaction. The solution comprises many features required to process inbound support requests and helps businesses connect with their customers via multiple channels such as inbound/outbound voice calls, email, voicemail, chat, social media and more.<br><br>NICE CXone offers various call routing features, like IVR, CTI and ACD. The system also includes workforce optimization capabilities such as e-learning, hiring and workforce management. The blended predictive dialer tool offers call blending, message lay-down dialing, call suppression and auto dialer for blended call centers. The solution seamlessly integrates with popular CRM applications like Salesforce and Oracle Service Cloud.<br><br>NICE CXOne can be used by small business and large enterprises alike and is in place across a wide variety of vertical markets. Customer service and support applications are also available as part of the integrated suite. |

| Solution | Brand | Product / Service | Description |
|---|---|---|---|
| | | NICE Engage | A complete recording of omnichannel interactions!<br>Every minute, thousands of interactions from multiple channels take place between your customers and your organization. These interactions contain a wealth of information about your customers and your services. Nice Engage allows you to record, store and retrieve this data from any channel including voice, chat, email, video and social media.<br><br>Nice Engage is a scalable, secure and robust platform that allows you to manage this interaction data in one place. This platform enables contact centers to comply with the most stringent regulations, including PCI-DSS, and to leverage every customer interaction for maximum return on investment. With Nice Engage you can record interactions: for compliance, quality management, better customer understanding, and rapid authentication. |
| | Poly | Poly Headset/Plantronics Headset | Poly/Plantronics creates premium audio and video products so you can have your best meeting and collaboration — anywhere, anytime, every time. Our headsets are beautifully designed and engineered to connect people with incredible clarity. They work seamlessly with leading hybrid work platforms. And our union with HP means they also are part of an ecosystem of innovative and easy-to-use solutions and services that simplify hybrid working. Why just show up when you can stand out? |
| **CRM** | | | |
| Café Membership Solution | D-MEMb | D-MEMb | Membership system for Café / Coffee shop |
| POS Solution | ADA Soft | More Plus Point of Sales | POS system, or point-of-sale system, is a set of devices, software and payment services merchants. A POS system manages customer purchases, accepts payments and provides receipts |
| | | Mini POS Point of Sales | |
| | Ambient Soft | Ambient POS | |
| **Cyber Security** | | | |
| AD Protection | SentinelOne | S1 Singularity Ranger AD | AD and Azure AD are common targets of identity-based cyber-attacks. Their compromise can give attackers the foothold to expand access, establish persistence, escalate privileges, identify more targets, and move laterally. SentinelOne Singularity Ranger AD, a component of the Singularity XDR platform, is an identity configuration assessment solution that identifies misconfigurations, vulnerabilities, and active threats targeting Active Directory (AD) and Azure AD. By delivering prescriptive, actionable insight into exposures in your identity attack surface, Ranger AD helps you reduce the risk of compromise and brings your assets in line with security best practices. |
| Advanced Threat Protection | Trellix | Trellix Network Security | Trellix Network Security is an effective cyberthreat protection solution that helps your organization minimize the risk of costly breaches by accurately detecting and immediately |

| Solution | Brand | Product / Service | Description |
|---|---|---|---|
| | | | stopping advanced, targeted, and other evasive attacks hiding in internet traffic. It facilitates efficient resolution of detected security incidents in minutes with concrete evidence, actionable intelligence, and response workflow integration.<br><br>With Network Security, your organization is effectively protected against today's threats, whether they ƒ Exploit Microsoft Windows, Apple OS X operating systems, or application vulnerabilities. Are directed at the headquarters or branch offices. Are hidden in a large volume of inbound internet traffic that must be inspected in real time.<br><br>At the core of Network Security are the Trellix Multi-Vector Virtual Execution (MVX) and dynamic machine learning and artificial intelligence (AI) technologies.<br><br>MVX is a signature-less, dynamic analysis engine that inspects suspicious network traffic to identify attacks that evade traditional signature- and policy-based defenses. Multiple machine learning, AI, and correlation engines represent a collection of contextual dynamic rules engines that detect and block malicious activity in real time and retroactively, based on the latest machine, attacker, and victim intelligence. Network Security also includes intrusion prevention system (IPS) technology to detect common attacks using conventional signature matching. |
| | Trend Micro | Deep Discovery Inspector | Targeted attacks and advanced threats are customized to evade your conventional security defenses, and remain hidden while stealing your corporate data, intellectual property, and communications, or encrypting critical data until ransom demands are met. To detect targeted attacks and advanced threats, analysts and security experts agree that organizations should utilize advanced detection technology as part of an expanded strategy. Trend Micro™ Deep Discovery™ Inspector is a physical or virtual network appliance that monitors 360 degrees of your network to create complete visibility into all aspects of targeted attacks, advanced threats, and ransomware. By using specialized detection engines and custom sandbox analysis, Deep Discovery Inspector identifies advanced and unknown malware, ransomware, zero-day exploits, command and control (C&C) communications, and evasive attacker activities that are invisible to standard security defenses. Detection is enhanced by monitoring all physical, virtual, north-south, and east-west traffic. |
| Application Security Testing | Opentext | Fortify On Demand | Fortify on Demand delivers application security as a service, providing customers with the security testing, vulnerability management, expertise, and support needed to easily create, supplement, and expand a Software Security Assurance program. |
| | | Fortify Software Security Center | The combination of static (SAST) and dynamic (DAST) application security testing methodologies provides a more comprehensive view of an application's risk posture. Here are 5 reasons why SAST + DAST with Fortify makes sense. |
| | | Fortify Static Code Analyzer | Fortify Static Code Analyzer (SCA) pinpoints the root cause of security vulnerabilities in the source code, prioritizes the most |

| Solution | Brand | Product / Service | Description |
|---|---|---|---|
| | | | serious issues, and provides detailed guidance on how to fix them so developers can resolve issues in less time with centralized software security management. |
| | | Fortify WebInspect | Fortify WebInspect by OpenText™ is an automated DAST solution that helps security professionals and QA testers identify vulnerabilities and configuration issues by simulating real-world external security attacks on a running application. It prioritizes issues for root-cause analysis and offers numerous REST APIs for integration. |
| | | Fortify Software Composition Analysis | The world runs on open source. With Fortify's software composition analysis and intelligence solutions, you can empower your developers to use it effectively and securely. |
| | SonaType | SonaType Nexus | Build fast with centralized components. Manage components, binaries and build artifacts across your entire software supply chain. |
| ASRM | Palo Alto Networks | Cortex XPANSE | The Cortex Xpanse Security Rating represents the overall hygiene of an organization's externally facing attack surface and the risk of a breach originating from those assets, enabling organizations to proactively manage their security posture and mitigate risks in the ever-evolving threat landscape.<br><br>Traditional security rating tools often provide incomplete data and assessments of attack surfaces, leading to difficulties in understanding the real-time security health and asset hygiene of an organization. Additionally, organizations struggle with effectively prioritizing and resolving high-risk incidents that impact their security ratings, which affect their cyber insurance premiums.<br><br>The Cortex Xpanse Security Rating addresses these challenges by offering a real-time security rating driven by exploiting intelligence for the entire attack surface. This allows organizations to assess their security, health and hygiene, track risk trends over time, and compare their ratings with industry peers. By identifying and prioritizing high-risk incidents, organizations can work toward improving their security rating and overall attack surface protection. |
| | Trend Micro | Attack Surface Risk Management | With never-ending technological advancements, enterprises are rapidly expanding, but at a pace that outstrips the traditional controls employed to oversee them. According to ESG1, only 9% of organizations believe they actively monitor their entire attack surface. However, when factoring in dynamic elements such as dispersed teams and organizations, business transformation efforts, hybrid infrastructure environments, supply chain expansion, and even mergers and acquisitions, uncertainty increases.<br><br>In a recent Ponemon Institute report, 69% of the small to medium-sized businesses queried2 stated that they were seeing an increase in targeted cyberattacks. On top of this, threat actors and deployed cyberattacks are only becoming more sophisticated. Through traditional, siloed attack surface |

| Solution | Brand | Product / Service | Description |
|---|---|---|---|
| | | | management (ASM) solutions, organizations tend to have a harder time maintaining proper visibility of their attack surface, let alone properly managing it to effectively reduce risk.<br><br>Introducing Trend Vision One — Attack Surface Risk Management (ASRM) Our ASRM is a next-gen solution that brings enhanced, proactive security to SecOps war rooms all the way up to the executive boardroom. Supported by our industry-leading research, our ASRM empowers security leaders and teams to discover and contextually evaluate overall organizational risk. In addition, it allows you to leverage advanced AI and ML models, which produce remediation recommendations to help you proactively mitigate risks and reduce the attack surface. |
| Asset Discovery | SentinelOne | S1 Singularity Ranger | Singularity Ranger is a real-time network attack surface control solution that finds and fingerprints all IP-enabled devices on your network, for global visibility with zero additional agents, hardware, or network changes. Ranger discovers and recovers unsecured endpoints with configurable, automated peer-to-peer agent deployment, to quickly plug gaps in your attack surface. By transforming Sentinel agents into distributed network sensors, Ranger identifies suspicious or malicious devices that can be isolated with a single click. Policies govern what should and should not be scanned. Create global asset inventories in seconds, investigate suspicious activity, and know with certainty what is connected where and with what protocol. |
| Breach and Attack Simulation | Picus | Picus Security Control Validation (SCV) | Picus Security Control Validation (SCV) is a BAS solution for the enterprises in Thailand.<br><br>Modern enterprises face increasingly sophisticated cyber-attacks. Breach and Attack Simulation (BAS) is now a key capability for security teams that need to continuously validate and improve their security controls, reduce cyber risk, and demonstrate compliance to management and regulators.<br><br>Picus SCV, powered by award-winning Breach and Attack Simulation (BAS) technology, automatically and continuously tests the effectiveness of your existing security controls across network, endpoint, web and email. By simulating real-world attacker techniques in a safe and controlled way, Picus helps security teams in Thailand measure, monitor, and strengthen their cyber resilience.<br><br>Why enterprises in Thailand choose Picus SCV<br>• Extensive Library of Real-World Threats: Continuously updated library of malware, exploits, and attacker techniques based on global and regional threat intelligence relevant to organizations in Thailand.<br>• Actionable Mitigation Recommendations: Detailed, vendor-specific prevention signatures and detection |

| Solution | Brand | Product / Service | Description |
|---|---|---|---|
| | | | rules to improve the effectiveness of your firewalls, IPS, EDR, Email, Web Security and SIEM.<br>• Customizable Threats and Attack Scenarios: This powerful feature enables security professionals to chain together attack actions and upload custom payloads.<br>• MITRE ATT&CK Mapping: All simulations mapped to MITRE ATT&CK, helping blue teams understand gaps across the full attack lifecycle.<br>• Executive Reports and Dashboards: High-level risk and readiness scores for CISOs and management, plus detailed technical views for SOC and security engineers.<br>• Benchmarking Capability: Compare your security scores with industry peers. Gain insights into the most simulated threats, threat templates, and popular ATT&CK tactics within your region, industry, and Picus community.<br><br>*"Do you want to see how Breach and Attack Simulation can help organization in Thailand validate security controls and reduce cyber risk?"*<br>*Contact DCS team for a consultation or request a Picus SCV demo.* |
| Cloud Security | Check Point | CloudGuard AppSec | CloudGuard for Application Security automates your application security and API protection with AppSec powered by contextual AI.<br><br>Stop attacks against your web applications with a fully automated, cloud native application security solution. |
| | | CloudGuard Intelligence | CloudGuard Cloud Intelligence and Threat Hunting, part of the CloudGuard Cloud Native Security platform, provides cloud native threat security forensics through rich, machine learning visualization, giving real-time context of threats and anomalies across your multi-cloud environment. |
| | | CloudGuard Network | CloudGuard Cloud Network Security, part of the CloudGuard Cloud Native Security platform, provides advanced threat prevention and automated cloud network security through a virtual security gateway, with unified security management across all your multi-cloud and on-premises environments. |
| | | CloudGuard Posture Management | CloudGuard Cloud Security Posture Management, part of the CloudGuard Cloud Native Security platform, automates governance across multi-cloud assets and services including visualization and assessment of security posture, misconfiguration detection, and enforcement of security best practices and compliance frameworks. |
| | | CloudGuard Spectral | CloudGuard Spectral is a developer-centric code security platform that seamlessly monitors, classifies, and protects codes, assets, and infrastructure; simply. |

| Solution | Brand | Product / Service | Description |
|---|---|---|---|
| | | CloudGuard Workload | CloudGuard provides the first comprehensive, fully automated, cloud-native workload security solution. It provides unified visibility, compliance and threat prevention across applications, APIs and microservices (K8s containers & serverless functions), from development through runtime. |
| | Palo Alto Networks | Prisma Cloud | **Protect Applications from Code to Cloud**<br>Prisma® Cloud is a cloud-native application protection platform (CNAPP) designed to protect applications across any public, private, hybrid, or multicloud environment. Unlike a collection of point products, Prisma Cloud integrates a broad set of security capabilities into a single platform to deliver unified, best-in-class security. The benefits of our approach include reduced risk, fewer breaches, better Dev-Sec collaboration, increased efficiency, and improved compliance and security posture.<br>**Risk Prevention :** Prevent risks and misconfigurations from entering production.<br>**Visibility and Control :** Establish continuous visibility and control across your cloud environment.<br>**Runtime Protection :** Enable real-time protection for cloud workloads, web applications, and APIs. |
| Data Security | Forcepoint | Forcepoint Data Classification | Data security is complex. Protecting data across cloud, endpoint, email, network, and web is an exhausting challenge. Forcepoint Data Classification leverages Artificial Intelligence (AI) and Large Language Models (LLMs) to increase the accuracy of data classification for unstructured data to improve your team's efficiency, reduce false alerts, and better prevent data loss. |
| | | Forcepoint Data Visibility | Actionable Visibility of Your Data At Rest Fast discovery of data using AI and ML delivers a highly accurate view of your unstructured data. Forcepoint Data Visibility provides uniquely valuable insights by:<br>• Continuous self-learning AI model pre-trained on hundreds of millions of files from diverse companies and industries for enhanced personalization and accuracy.<br>• Viewing who exactly has permission to your sensitive data to secure all data with least privilege access.<br>• Reducing redundant, obsolete, and trivial data to simplify management and minimize loss of sensitive data.<br>• Understanding risk for each file to maintain regulatory compliance more easily.<br>• Providing location of your data by IP address and file paths. Grouping data assets and cataloging to gain a bird's-eye view into how best to organize your data. |
| | | Forcepoint Enterprise DLP | Data security everywhere your people work, and data resides Data security is a major problem for organizations of all types and sizes today. On one hand, IT organizations are required to keep up with regulations and protect personal identifiable information (PII), protected health information (PHI), and other types of regulated information from targeted malicious attacks as well as accidental data loss. On the other hand, they must adapt to macro-IT movements, such as the adoption of |

| Solution | Brand | Product / Service | Description |
|---|---|---|---|
| | | | cloud applications, hybrid cloud environments, and BYOD trends, all of which increase the ways data can leave your organization.<br><br>This expanding attack surface poses the most significant challenge to protecting critical data. Data security teams must consider the explosion of data movement from "inside" the organization to all the places and channels that data now resides and moves. Visibility must be gained across all data in the cloud as well as on-prem. Data security teams must also have visibility and control across all channels (endpoint, web traffic, network, email, cloud applications, and private applications) with a single point of management.<br><br>Forcepoint DLP is the industry's most trusted solution, giving you the tools to easily manage global policies across every major channel, whether its endpoint, network, cloud, web, private applications, or email. We can simplify your work with the most pre-defined templates, policies, and classifiers of any DLP provider in the industry. This can dramatically streamline your incident management so you can focus on what's most important, eliminating risk so that your people can be increasingly productive. Forcepoint DLP addresses risk by bringing you visibility and control everywhere your people work and anywhere your data resides |
| | | Forcepoint ONE Cloud Access Security Broker (CASB) | The Forcepoint ONE Cloud Access Security Broker (CASB) is one of the three foundational gateways of the Forcepoint ONE all-in-one cloud platform. It controls access to managed SaaS applications and shadow IT applications while providing Data Loss Prevention (DLP) and malware protection. |
| | | Forcepoint Risk-Adaptive Protection | Risk-Adaptive Protection (RAP) is an integral part of the Forcepoint Data Loss Prevention (DLP) solution that is designed to alert organizations of risky behavior, so they can protect critical data and reduce the risk associated with insiders. The solution collects user behavior and Forcepoint DLP incidents then computes the user's risk using Forcepoint's Indicator of Behavior (IOB) analytic models. This risk score is actively communicated to DLP to automate policy enforcement based on the risk level. |
| | Thales | Thales CipherTrust Data Security Platform | The CipherTrust Data Security Platform (CDSP) significantly reduces risk across your business. CDSP integrates centralized key management with data discovery, classification, data protection and granular access controls. CDSP decreases resources required for data security operations and compliance controls by simplifying data security, accelerating time to compliance, and securing cloud migration.<br><br>The CDSP platform offers capabilities for discovering, protecting and controlling access to databases and files—and can secure assets residing in cloud, virtual, and physical environments. This scalable, efficient data security platform enables you to address your urgent requirements and prepares your organization to respond nimbly when the next security challenge or compliance requirement arises. |

| Solution | Brand | Product / Service | Description |
|---|---|---|---|
| Database Security | Imperva | Cloud Database Security | Managed database services platforms like Amazon and Azure secure their infrastructure, but not your data. Every DBaaS customer must have their own security and compliance controls. Imperva(™) Cloud Data Security can help you to find and resolve issues before they become data breaches or compliance failures |
| | | Imperva Database Security Fabric | Imperva Data Security Fabric provides data-centric protection enterprise-wide to fill the gaps left by traditional perimeter security, native data repository access controls, and data encryption solutions, which are powerless against numerous data breach threats such as data handling mistakes, malicious insiders, and attack exploits that leverage compromised account credentials. |
| DDoS Protection | Cloudflare | Network Services | **Modern security and performance**<br>Protect & accelerate networks!<br>Traditional solutions just aren't designed to fulfill the Internet's basic needs: security, performance, and reliability. Modernize your network approach. |
| | Imperva | DDoS Protection | Imperva DDoS Protection is a cloud-based service that protects your assets at the edge 24/7, ensuring business continuity with guaranteed uptime. It offers transparent mitigation for website, network, and individual IP protection against any size or duration of DDoS attacks. |
| Deception Protection | SentinelOne | S1 Singularity Hologram | Singularity Hologram, a component of the SentinelOne Singularity XDR platform, leverages advanced, high-interaction deception and decoy technology to lure in-network attackers and insider threat actors into engaging and revealing themselves. By mimicking production OSes, applications, data, and more, Singularity Hologram uncovers covert adversary activity, collects high-fidelity telemetry, and garners actionable intelligence to help you build your defenses |
| Digital Certificate | Entrust | Digital Certificate | The Entrust Certificate Services (ECS) platform greatly reduces security issues associated with certificate lifecycle management. Increased visibility into security loopholes helps you stay in compliance and prevent threats. The greatest benefit is the peace of mind you get with more service uptime and maintaining brand reputation.<br><br>ECS takes the guesswork out of certificate lifecycle management and is included with digital certificates purchased from Entrust.<br><br>A centralized dashboard makes it easy for you to consolidate and manage all your digital certificates from one location – regardless of issuing certification authority (CA). Accessible from any web browser, it delivers critical insight via real-time reporting to help you avoid security lapse and maintain regulatory compliance. |
| DNS Security | Infoblox | Infoblox Advanced DNS Protection | SAFEGUARD YOUR BUSINESS FROM DISRUPTIONS CAUSED BY DNS-BASED ATTACKS<br>With Infoblox Advanced DNS Protection (ADP), your business is always up and running, even under a DNS-based attack. Infoblox blocks the widest range of attacks, such as volumetric |

| Solution | Brand | Product / Service | Description |
|---|---|---|---|
| | | | attacks, NXDOMAIN, exploits and DNS hijacking. Unlike approaches that rely on infrastructure overprovisioning or simple response-rate limiting, Advanced DNS Protection intelligently detects and mitigates DNS attacks while responding only to legitimate queries by using constantly updated threat intelligence, without the need to deploy security patches. With Infoblox, you can take network reliability to the next level by ensuring that your critical infrastructure—and your business—keep working at all times. |
| | | Infoblox BloxOne Threat Defenses | INFOBLOX PROVIDES A SCALABLE PLATFORM THAT MAXIMIZES YOUR EXISTING THREAT DEFENSE INVESTMENT<br>Infoblox BloxOne Threat Defense Advanced strengthens and optimizes your security posture from the foundation up. It maximizes brand protection by securing your existing networks as well as digital imperatives like SD-WAN, IoT and the cloud. It uses a hybrid architecture for pervasive, inside-out protection, powers security orchestration, automation, and response (SOAR) solutions by providing rich network and threat context, optimizes the performance of the entire security ecosystem and reduces your total cost of enterprise threat defense.<br><br>KEY CAPABILITIES<br>• Detect and block exploits, phishing, ransomware and other modern malware that other solutions miss<br>• Protect users and devices regardless of platform or OS, at the DNS layer, including BYOD, IoT, and ICS<br>• Defend mobile devices from emerging threats like those that abuse photos taken of malicious QR codes<br>• Discover high-risk applications and manage your Shadow IT, Insider, Compliance and other risks<br>• Prevent data exfiltration techniques with machine learning/AI analytics including DNS-based data exfiltration, DGA, and DNS Messenger<br>• Restrict user access to inappropriate or unwanted web content and track activity<br>• Protect your brand with Lookalike Domain Monitoring for your most valuable internet properties<br>• Accelerate investigations 3X and streamline threat response and threat hunting activities<br>• Enhance visibility: Get precise visibility “and rich network context” by integrating with IPAM asset metadata for optimum event understanding and correlation<br>• Control the risks of rising DoH use: block DoH (DNS over HTTPS) domain access and gracefully revert DoH requests to existing, trusted DNS |
| Email Security | Check Point | Harmony Email and Collaboration | Harmony Email & Collaboration provides complete protection for Microsoft 365, Google Workspace and all your collaboration and file-sharing apps. Email & Collaboration is designed specifically for cloud email environments and is the ONLY solution that prevents, not just detects or responds to, threats from entering the inbox. |
| | Cisco | Cisco Secure Email | Cisco Secure Email includes advanced threat protection capabilities to detect, block, and remediate threats faster, prevent data loss, and secure important information in transit |

| Solution | Brand | Product / Service | Description |
|---|---|---|---|
| | | | with end-to-end encryption.<br>With Cisco Secure Email customers can:<br>• Detect and block more threats with superior threat intelligence from Talos™, our threat research team.<br>• Combat ransomware hidden in attachments that evade initial detection with Cisco Secure Email Malware Defense and Cisco Threat Grid.<br>• Drop emails with risky links automatically or block access to newly infected sites with real-time URL analysis to protect against phishing and BEC.<br>• Prevent brand abuse and sophisticated identity-based email attacks with Cisco Secure Email Domain Protection and Cisco Secure Email Phishing Defense services.<br>• Protect sensitive content in outgoing emails with Data Loss Prevention (DLP) and easy-to-use email encryption, all in one solution.<br>• Provide user behavior training with Cisco Secure Awareness Training to help users work smarter and safer.<br>• Maximize deployment flexibility with a cloud, virtual, on-premises, or hybrid deployment or move to the cloud in phases.<br>• Integrate across a growing number of Cisco Security products and accelerate key security operations functions like visibility, detection, automation, investigation, and remediation with SecureX. |
| | Trend Micro | Cloud App Security | Trend Micro Cloud App Security enables you to embrace the efficiency of cloud services while maintaining security. It protects incoming and internal emails from Microsoft 365 and Gmail against advanced malware and other threats. It also enforces compliance on other cloud file- sharing and collaboration services, including Box, Dropbox, Google Drive, Microsoft SharePoint online, Microsoft OneDrive for business, and Microsoft Teams. Cloud App Security integrates directly with Microsoft 365, Google Workspace, and other services using APIs, maintaining all user functionality without changing the MX record to reroute email traffic or setting up a web proxy. This second layer of defense caught 39.9 million high-risk threats beyond those detected by the cloud email services' built-in security. |
| | | Email Security | Email is mission critical, but email-based threats, including ransomware and business email compromise (BEC), are growing exponentially—and it's difficult to keep up. Even your savviest employees can mistakenly click on a malicious link and expose your enterprise to a cyberattack.<br><br>Trend Micro Email Security stops more phishing, ransomware, and BEC attacks. Our solution uses an optimum blend of cross-generational threat techniques, like machine learning, sandbox analysis, data loss prevention (DLP), and other methods to stop all types of email threats. This solution minimizes management overhead and integrates with other Trend Micro security layers to share threat intelligence and provide central visibility of threats across your organization. Email Security protects Microsoft Exchange, Microsoft 365, Gmail, and other hosted and on-premises email solutions. |

| Solution | Brand | Product / Service | Description |
|---|---|---|---|
| Endpoint Security | CrowdStrike | Falcon | CrowdStrike Falcon® Endpoint Protection Enterprise sets the new standard in endpoint security with the first and only cloud-native security platform proven to stop breaches by unifying next-gen antivirus (NGAV), endpoint detection and response (EDR), managed threat hunting and integrated threat intelligence, in a single cloud-delivered agent. |
| | Palo Alto Networks | Cortex XDR | **Prevent, Detect, and Respond to the Stealthiest Threats**<br>You can now stop modern attacks with Cortex XDR – the industry's first endpoint-based extended detection and response platform that integrates data from any source. Your SOC team can cut through the noise and focus on what matters most with intelligent alert grouping and incident scoring. Cross-data insights accelerate investigations so that you can streamline incident response and recovery. Finally, by harnessing the power of AI, analytics, and rich data, XDR allows you to detect stealthy threats.<br><br>Cortex XDR delivers peace of mind with industry-leading endpoint security that achieved the highest combined protection and detection scores in the 2022 MITRE ATT&CK Evaluations. The Cortex XDR platform collects and analyzes all data, so you can gain complete visibility and holistic protection to secure what's next.<br><br>Block Attacks with Best-in-Class Endpoint Detection and Response<br>The Cortex XDR agent offers unparalleled protection for exploits, malware, ransomware, and fileless attacks. It includes the broadest set of exploit protection modules available to block malware infections. It enables sharp detection with AI-powered analytics and threat insights. Finally, it allows you to remediate quickly and take control of affected machines. |
| | SentinelOne | S1 Singularity Endpoint | Singularity Complete provides best-in-breed EPP & EDR capabilities in one platform, management console, and agent. Designed for organizations seeking enterprise-grade prevention, detection, and response scalable across the enterprise, coupled with custom automations, Singularity Complete empowers security teams to easily identify and secure every user endpoint on their network.<br>• Patented Storyline™ for fast RCA and easy pivots<br>• Complete visibility of both benign and malicious data<br>• Data retention options to suit every need, upgradeable up to 3 years<br>• Hunt by MITRE ATT&CK® Technique<br>• Mark benign Storylines as threats for enforcement by the EPP functions<br>• Custom detections and automated hunting rules with Storyline Active Response (STAR™)<br>• Built-in data collection scripts to enhance visibility and incident investigation<br>• Timelines, remote shell, file fetch, sandbox integrations, and more |
| | Trend Micro | Apex One | Eliminate security gaps across any user activity and endpoint with a blend of advanced threat protection techniques |

| Solution | Brand | Product / Service | Description |
|---|---|---|---|
| | | | combined with detection and response, delivered through a single-agent portfolio.<br>• Automated: Stop attackers sooner with the most effective protection against zero-day threats: a blend of next-gen anti-malware techniques and the industry's most timely virtual patching.<br>• Insightful: Get exceptional visibility and control across your environment. Integrated extended detection and response (XDR) capabilities for cross-layer detection, investigation, and threat hunting.<br>• Connected: Quickly respond to attacks with real-time and local threat intelligence updates and a broad API set for integration with third-party security tools. Flexible deployment options fit perfectly with your environment. You can have it all.<br>• Malware and ransomware protection: Defends endpoints against threats like malware, ransomware, and malicious scripts. Advanced protection capabilities adapt to protect against unknown and stealthy new threats.<br>• Extensive detection and response capabilities in one console: XDR goes beyond EDR with cross-layer detection and threat hunting and investigation across email, endpoints, servers, cloud workloads, and networks.<br>• The industry's most timely virtual patching: Vulnerability protection applies virtual patches for protection before a patch is available or deployable.<br>• Ransomware rollback: Detects ransomware with runtime machine learning and expert rules to block encryption processes in milliseconds. Rollback restores any files encrypted before the detection.<br>• Connected threat defense: Trend Micro Apex One integrates with other security products via our global cloud threat intelligence, delivering sandbox rapid response updates to endpoints.<br>• Flexible deployment: Trend Micro Apex One as a Service saves time, money, and is always up to date with the latest protection. On-premises and hybrid deployments are also fully supported. |
| Firewall Management | Check Point | Quantum Smart-1 | Quantum Smart-1 security management appliances consolidate security management in an all-in-one scalable appliance for full threat visibility and greater system resiliency to handle any network growth and log capacity across your entire infrastructure. |
| | Fortinet | FortiManager | FortiManager delivers unified management for consistent security across complex hybrid environments resulting in protection against security threats. Key benefits include accelerated zero-touch provisioning with best-practice templates for deployment at scale of SD-WAN and streamlined workflows between the Fortinet Security Fabric and integrations with 500+ ecosystem partners. |
| | Palo Alto Networks | Panorama | Security deployments can overload IT teams with complex security rules and data from multiple sources. Panorama™ network security management empowers you with easy-to-implement, consolidated policy creation and centralized management features. You can provision firewalls centrally and use industry- leading functionality to create effective |

| Solution | Brand | Product / Service | Description |
|---|---|---|---|
| | | | security rules as well as gain insight into network traffic and threats. |
| HSM | Thales | Thales Luna General Purpose HSM | Thales is the leading provider of general-purpose hardware security modules (HSMs) worldwide. Our Thales Luna HSM product family represents the highest-performing, most secure, and easiest-to-integrate HSM solution available on the market today.<br><br>Luna HSMs is purposefully designed to provide a balance of security, high performance, and usability that makes them an ideal choice for enterprise, financial, and government organizations. |
| Identity and Access Management | BeyondTrust | Active Directory Bridge | Active Directory Bridge streamlines authentication across Windows, Unix, and Linux environments by extending Microsoft AD's Kerberos authentication and single sign-on. Users can use their AD credentials to access Unix and Linux systems for a seamless experience. Organizations can achieve consistency by extending native group policy management tools to include Unix and Linux settings and transitioning users. |
| | | Cloud Privilege Broker | Cloud Privilege Broker enables organizations to identify and manage risks related to cloud access permissions and entitlements across multiple environments. It provides complete visibility and management of entitlements across cloud platforms, as well as a recommended path for fast mitigation to enhance security and meet compliance goals. Additionally, it centralizes management and reporting of privilege-related risk. |
| | | Identity Security Insights | Identify Security Insights is an analytics solution that detects anomalous activity and threats from compromised identities and privileged access misuse. It correlates data from BeyondTrust products and third-party solutions, providing a single view of human and non-human identities, accounts, and privileged access. It also provides risk ratings. |
| | | Password Safe | Password Safe combines privileged password and session management to discover, manage, and audit all privileged credential activity. It scans, identifies, and profiles all assets for automated onboarding, ensuring no credentials are left unmanaged. It also controls privileged user accounts, applications, SSH keys, cloud admin accounts, RPA accounts, and more. Additionally, it vaults and generates employee passwords for enterprise applications. Adaptive access control is used for automated evaluation. |
| | | Privilege Management for Unix & Linux | Privilege Management for Unix & Linux is an enterprise-class, gold-standard privilege management solution that helps organizations control privileged access, achieve compliance, and reduce cyber risk. It uses factors like time, day, location, application, and asset vulnerability status to make better privilege elevation decisions. Users can securely run specific commands and sessions remotely without logging in as admin or root. |
| | | Privilege Management for Windows & Mac | Enforce Least Privilege and Control Applications for Windows & Mac combines powerful least privilege management and |

| Solution | Brand | Product / Service | Description |
|---|---|---|---|
| | | | application control capabilities, delivering fast, unmatched preventative endpoint security. Grant the right privilege to the right application- not the user- only when needed and create a single audit trail. Prebuilt policy templates stop attacks involving trusted apps, instantly addressing bad scripts and infected email attachments. |
| | | Privileged Remote Access | With a VPN-less solution, IT teams can control, manage, and audit remote privileged access by authorized employees, contractors, and vendors without compromising security. Connect securely from anywhere, no VPN required. Extend privileged access to cloud assets and limit network traffic and ports to only authorized sources and applications. Monitor sessions and confidently meet compliance requirements. |
| | CyberArk | Access Management | Businesses use access management solutions to authenticate, authorize, and audit access to applications and IT systems. Often delivered as a component of an identity and access management (IAM) solution, access management solutions help strengthen security and reduce risk by tightly controlling access to on-premises and cloud-based applications, services, and IT infrastructure. They help ensure the right users have access to the right resources at the right times for the right reasons. |
| | | Privilege Cloud | Privileged access is used in almost every cyber assault. Bad actors, whether foreign attackers or malevolent insiders, may exploit privileged access to deactivate security mechanisms, seize control of vital IT infrastructure and applications, and gain access to sensitive business and personal data.<br><br>CyberArk Privilege Cloud is a SaaS service that allows organizations to securely store, cycle, and isolate credentials (for both human and non-human users), monitor sessions, and provide scalable risk reduction to their businesses.<br><br>Privilege Cloud secures, manages, and monitors privileged access across on-premises, cloud, and hybrid infrastructures. |
| | | Endpoint Privilege Security | Endpoint security protects enterprise networks from threats from on-premises or remote devices. Endpoints include desktops, laptops, servers, workstations, smartphones, and tablets.<br><br>Most organizations have used firewalls, VPNs, endpoint management solutions, and antivirus programs to protect sensitive data, prevent unauthorized access to critical applications and IT systems, and prevent malicious software and other vulnerabilities. However, mobile apps and cloud services are eroding the enterprise network perimeter. |
| | | Identity Governance and Administrator | Identity Governance and Administration (IGA) solutions efficiently manage digital identities and access rights across diverse systems and are used by corporate information security, risk management, compliance teams and IT organizations. IGA solutions help businesses strengthen security, simplify operations, streamline onboarding, and improve compliance with government regulations, industry standards or corporate policies. |

| Solution | Brand | Product / Service | Description |
|---|---|---|---|
| | | | IGA capabilities are just one part of a unified Identity Security platform and work in tandem with Identity and Access Management (IAM) and Privileged Access Management (PAM) services. |
| | | Privileged Access | Privilege access management (PAM) refers to a comprehensive cybersecurity strategy – comprising people, processes, and technology – to control, monitor, secure and audit all human and non-human privileged identities and activities across an enterprise IT environment. Organizations implement privilege access management to protect against the threats posed by credential theft and privilege misuse. |
| | | Secrets Management | Today's digital enterprises rely on commercial, internally developed, and open-source applications to run their businesses and increasingly leverage automated IT infrastructure and DevOps methodologies to speed development and innovation. While application and IT environments vary significantly from organization to organization, one thing remains constant: every application, script, automation tool and other non-human identity relies on some form of privileged credential to access other tools, applications and data. |
| | | Secure Cloud Access | CyberArk Secure Cloud Access, part of the Identity Security Platform, offers zero standing privilege access in multicloud environments, implementing least privilege access to improve security posture. The SaaS solution improves operational efficiency for IAM and Security teams implementing Zero Trust.<br><br>Secure Cloud Access with Just-in-Time elevation and least privilege permissions significantly reduce risk for sensitive public cloud sessions, including configurations. On-demand elevation requests allow on-call engineers to request and receive elevated entitlements in critical situations. |
| IPS | Trellix | Trellix Intrusion Prevention System | Trellix Intrusion Prevention System (IPS) is a next-generation intrusion detection and prevention system (IDPS) that discovers and blocks sophisticated malware threats across the network. It uses advanced detection and emulation techniques, moving beyond traditional pattern matching to defend against stealthy attacks with a high degree of accuracy.<br><br>Trellix IPS combines intelligent threat prevention with intuitive security management to improve detection accuracy and streamline security operations. Your network faces advanced attacks that can evade traditional detection methods—which is why our IPS layers multiple signature and signature-less detection engines to help prevent unwanted malware from wreaking havoc on your network. It performs deep inspection of network traffic using a combination of advanced technologies, including full protocol analysis, threat reputation, and behavior analysis to detect and protect against malware callbacks, denial-of-service (DoS), zero-day attacks, and other advanced threats. |
| | Trend Micro | TippingPoint Threat Protection System (IPS) | Trend Micro™ TippingPoint™ Threat Protection System (TPS) is a powerful network security platform that delivers |

| Solution | Brand | Product / Service | Description |
|---|---|---|---|
| | | | comprehensive threat protection against known and undisclosed vulnerabilities with high accuracy. TippingPoint TPS provides your organization with industry-leading coverage across different threat vectors with extreme flexibility and high performance, keeping you resilient against advanced threats like malware and phishing. The TippingPoint TPS uses a combination of technologies--including deep packet inspection, threat reputation, URL reputation, and advanced malware analysis on a flow-by-flow basis— to detect and prevent attacks on your network. The TippingPoint TPS enables your teams to take a proactive approach to security, providing you with comprehensive contextual awareness and deeper analysis of network traffic. This complete contextual awareness, combined with the threat intelligence from Trend Micro™ TippingPoint™ Digital Vaccine™ (DV) threat intelligence provides the visibility and agility necessary to keep pace with today's dynamic, evolving enterprise and data center networks. |
| Load Balancer | F5 | F5 Distributed Cloud Services | F5 Distributed Cloud Services are SaaS-based security, networking, and application management services that enable customers to deploy, secure, and operate their applications in a cloud-native environment wherever needed– data center, multi-cloud, or the network or enterprise edge. |
| | | F5 Big-IP | Keep your apps secure, up and running with F5 application delivery controllers. Along with application, API protection and access control services, BIG-IP application delivery and security software scales your application traffic and secures your infrastructure. You'll get built-in security, traffic management, and performance application services, whether your applications live in a private data center or in the cloud. |
| | NetScaler | NetScaler load balancing | NetScaler load balancing for layer 4 and layer 7 distributes incoming network traffic across multiple servers or resources to prevent bottlenecks and ensure that each resource is being used to its fullest capacity. This results in improved application performance and faster response times.<br><br>To ensure that no server or resource fails, NetScaler automatically redirects traffic to a backup server or resource so that services remain available to your application end users. To meet both predictable and unpredictable application demand, NetScaler load balancing automatically scales to handle demand by distributing traffic across additional servers or resources.<br><br>By distributing traffic across multiple servers or resources, NetScaler load balancing reduces the risk of a single point of failure or attack, effectively providing an additional layer of security. And it's cost effective: NetScaler load balancing optimizes resource utilization, so you can make the most of your existing infrastructure and reduce the need to invest in additional hardware or resources. |
| Log Management | Fortinet | FortiAnalyzer | FortiAnalyzer delivers unparalleled visibility across IT and OT infrastructures. Seamlessly integrating with devices and applications throughout the Security Fabric, it turns raw data into actionable intelligence. This consolidated view helps eliminate operational bottlenecks, bolstering defenses with |

| Solution | Brand | Product / Service | Description |
|---|---|---|---|
| | | | historical and real-time insights and empowering security teams to be consistently proactive. |
| Multi Factor Authentication | Cisco | Cisco Duo | Duo is a two-factor authentication solution that helps organizations boost security by verifying user identity, establishing device trust, and providing a secure connection to company networks and applications. Duo multi-factor authentication protects your organization's data at every access attempt, from any device, and from any location. It verifies user trust, establishes device trust, and provides secure access to company apps and networks—from wherever users are logging in.<br><br>When a user logs in, whether from their home office, the corporate office, or another remote location—Duo uses two-factor authentication and a zero-trust approach to security. Before granting access, Duo will:<br>• Verify user trust. Duo uses a second form of validation, such as a smartphone, to verify that a user is who they say they are before granting them access.<br>• Establish device trust. Once access is granted, Duo enables your organization to see every device that is connected to your network and applications and easily monitor device health and compliance.<br>• Enforce adaptive policies. You can set access levels based on role, device, location, and other relevant factors.<br>• Grant secure access to users. Get even more secure access, beyond what a VPN can provide, and verify the identities of users from wherever they choose to log in.<br>• Grant secure access to apps. Provide users with single sign-on (SSO) for a consistently easy login experience. A user-friendly dashboard provides streamlined access to company apps. |
| | Entrust | Identity as a Service (IDAAS) | Cloud-based Identity and Access Management (IAM) Entrust Identity as a Service (IDaaS) enables trusted identities for workforces, consumers, and citizens so they can engage securely and seamlessly with your organization. Our intelligent IAM platform lets you implement a Zero Trust approach, providing user authentication, authorization, and access control to the right resources anytime anywhere. |
| | Fortinet | FortiAuthenticator | FortiAuthenticator provides identity and access management (IAM) services to prevent breaches resulting from unauthorized users gaining access to a network or inappropriate levels of access granted to valid users. FortiAuthenticator ensures only the right person can access your sensitive resources and data at the right time. |
| | | FortiToken | FortiToken helps prevent breaches that occur due to compromised user accounts and passwords by increasing the certainty of the identity of users attempting to access resources. To achieve multi-factor authentication (MFA), FortiToken integrates with FortiAuthenticator and FortiGate Next-Generation Firewalls and is part of the Fortinet Identity and Access Management (IAM) solution. |
| | OneSpan | OneSpan Authentication Server | OneSpan Authentication Server is a centralized authentication server offering strong authentication and validation of |

| Solution | Brand | Product / Service | Description |
|---|---|---|---|
| | | | transaction signatures. It verifies authentication requests from individuals trying to access the corporate network or business applications.<br><br>The solution adds additional security measures to standard username/password logins across a wide range of servers and services. This stops unauthorized logins, "even when passwords have been compromised. OneSpan Authentication Server is ideally suited for large and small enterprise network security implementations, application security and online banking security.<br>• Can be used out of the box or integrated with existing infrastructure<br>• Designed to fit the needs of organizations of any size<br>• Easy to install, manage and support<br>• Easy to integrate in existing infrastructure<br>• Efficient tools for helpdesk staff<br>• Robust and easy expandable with users and applications<br>• Cronto technology ensures an easy and convenient user experience<br>• Smooth migration, updates, and maintenance<br><br>Strong, two factor authentication : The combination of OneSpan Authentication Server and Digipass® provides strong user authentication and greater security than static passwords, which expose the organization to data breaches. OneSpan Authentication Server provides a turnkey solution that can be rapidly implemented and operational. |
| | | OneSpan Mobile Authenticator | OneSpan Mobile Authenticator is a mobile, two factor authentication app that enables users to securely login to applications, via their mobile device, with biometrics (on devices that support them) or PIN along with a onetime password (OTP). OneSpan Mobile Authenticator is the easiest way to deploy strong mobile authentication within your company and/or customer base. A modern user interface, flexible licensing options and expanded support translate into the best overall user experience. |
| | RSA | RSA SecureID | For many decades, customers have trusted the one-time passcode (OTP) technology delivered by SecurID authenticators available in a broad range of easy-to-use form factors. Now, RSA is making the choice easier than ever by supporting new and emerging standards and offering the broadest portfolio of authentication methods for any use case, on-premises or in the cloud. To suit a wide variety of organization and application requirements, RSA offers the following SecurID authentication methods:<br><br>Mobile app<br><br>Quickly set up advanced mobile MFA options and give users a single authenticator to access both on-premises and cloud applications on all the major mobile platforms (iOS, Android, Microsoft Windows). The SecurID mobile app provides convenient authentication methods, such as push notification, device biometrics, FIDO and OTP, to seamlessly access on-premises applications such as virtual private networks (VPNs) or cloud applications like Microsoft 365.<br><br>Fast IDentity Online (FIDO) authentication |

| Solution | Brand | Product / Service | Description |
|---|---|---|---|
| | | | As a U2F and FIDO2 certified vendor, RSA enables a passwordless experience with the broadest support for FIDO authentication, including hardware, software, wearable and embedded options.<br><br>Software authenticators<br><br>Deploy SecurID software tokens on mobile devices, desktops and laptops, and make strong authentication a convenient part of doing business. SecurID authenticators are available for the following platforms: Microsoft Windows, macOS, iOS, Android, and more.<br><br>Hardware authenticators<br><br>Protect sensitive data and mission-critical systems with the industry's highest-quality two-factor authentication device, the SecurID Hardware Token Authenticator. Gain two-factor authentication, hard disk encryption, email and transaction signing capabilities with a single hardware token.<br><br>On-demand: SMS text/voice/email<br><br>On-Demand Authentication (ODA) enables users to receive an OTP as an SMS message delivered to their cell phone or via email. Users are sent an OTP to use as a login to their SMS-enabled mobile device. |
| NAC | Cisco | Cisco ISE | Cisco Identity Services Engine (ISE) is a security policy management platform that provides secure network access to end users and devices. Cisco ISE enables the creation and enforcement of security and access policies for endpoint devices that are connected to an organization's routers, switches and wireless. It is designed to help organizations simplify identity management across devices and applications.<br><br>Cisco Identity Services Engine helps enterprises understand and gain visibility into their network, giving them the ability to see who is connected as well as which applications are installed and running. The product can help with zero-trust strategies by securing the network and everyone and every endpoint connected to it. ISE can also share data like user and device identities as well as threats and vulnerabilities with other integrated Cisco tools to further streamline security policy management.<br><br>Cisco Identity Services Engine (ISE) provides a range of network access control (NAC) capabilities from guest access to security response depending upon the licenses and appliances purchased. ISE is intended for use with guest and employee endpoints, but Cisco also offers separate and specialized NAC solutions for equipment (internet of things (IoT), operational technology (OT), and industrial controls), for medical devices, and specifically for rapid threat containment.<br><br>With an increased number of users and devices accessing networks remotely, protecting an organization's data from network security breaches becomes more complex. Administrators can use Cisco Identity Services Engine to control who has access to their network and ensure authorized policy-compliant devices are being used. IT administrators can use ISE for policy enforcement, visibility, |

| Solution | Brand | Product / Service | Description |
|---|---|---|---|
| | | | granting guest access to the network, threat containment, tool integrations, device administration and bring-your-own-device (BYOD) management. Cisco ISE can authenticate wired, wireless and virtual private network (VPN) users. Authorized and unauthorized users are logged so administrators can view who and which devices are connected to their network at any time. |
| | Forescout | eyeExtend | **Automate Security Workflows Across Disparate Products :** Share device context between the Forescout Platform and other IT and security products, automate policy enforcement across disparate tools and accelerate system-wide response to mitigate risks. |
| | | Forescout eyeControl | Forescout eyeControl provides flexible and frictionless network access control for heterogeneous enterprise networks. It enforces and automates Zero Trust security policies for least-privilege access on all managed and unmanaged assets across your digital terrain. Policy-based controls can continuously enforce asset compliance, proactively reduce your attack surface, and rapidly respond to incidents.<br>Secure Network Access<br>• Enforce network access based on user, device identity and security posture<br>• Deploy with or without 802.1X in heterogeneous networks Enforce Asset Compliance<br>• Automate compliance with security policies, industry standards and government regulations<br>• Initiate remediation and risk mitigation workflows in real-time<br>• Automate Incident Response<br>• Automate response to security incidents<br>• Contain threats to minimize propagation and disruption |
| | | Forescout eyeSegment | Forescout eyeSegment removes the complexity of designing, planning and deploying dynamic segmentation across your digital terrain. Shrink the attack surface, limit the blast radius and mitigate regulatory and business risk by rapidly accelerating your segmentation projects. A core component of Forescout Continuum Platform, eyeSegment enables organizations to embrace zero trust security principles and automate cybersecurity actions across their digital terrain. |
| | | Forscout eyeInspect | Forescout eyeInspect provides in-depth device visibility for OT/ICS networks and enables effective, real-time management of operational and cyber risks.<br>• Fully understanding the cyber-resiliency of your OT network with an Asset Risk Framework<br>• Gain complete device visibility through deep packet inspection of more than 270 industrial network protocols and baseline assets<br>• Defend your network with thousands of OT-specific threat indicators and powerful anomaly detection |
| | | Forescout eyeSight | Forescout eyeSight delivers unparalleled insight into every connected asset through deep integration into your network fabric. |

| Solution | Brand | Product / Service | Description |
|---|---|---|---|
| | | | • Discover your entire asset inventory with over 30 active and passive techniques that reveal coverage gaps across your digital terrain, providing a real-time view of your attack surface<br>• Automate asset classification and build comprehensive profiles that include known risks and vulnerabilities with threat intelligence powered by Vedere Labs<br>• Prepare to face new threats as they emerge by leveraging cloud-based machine learning that continuously improves Forescout's Device Cloud, a proprietary source of device intelligence with over 30 billion unique data points<br>• Continuously assess an asset's status, risk posture, and policy compliance without needing an agent to be installed, which is essential for protecting IoT, IoMT, and OT assets<br>• Multiply your forces while minimizing human error with automated reporting on compliance posture and cyber-risk exposure, letting you focus your efforts on what matters most |
| | HPE | Aruba Clearpass | Aruba ClearPass for Secure Network Access Control<br>From IoT to an always-on mobile workforce, organizations are more exposed to attacks than ever before. With Aruba ClearPass, you get agentless visibility and dynamic role-based access control for seamless security enforcement and response across your wired and wireless networks.<br><br>Agentless policy control and automated response.<br>What's needed beyond visibility, control and response? Real-time policies for how users and devices connect and what they can access is critical, as well as robust guest access and strong enforcement capabilities.<br><br>Enforcing access privileges to effectively reduce risk. In addition to its role as the policy enforcement mechanism for ClearPass, the Aruba Policy Enforcement Firewall (PEF) has been designated "Cyber Catalystsm", based on its ability to effectively reduce risk.<br><br>Secure access for guest, BYOD and corporate devices<br>.There are simple ways to let users securely connect devices to a network – without compromising security. ClearPass includes secure Wi-Fi guest access, device onboarding and health checks, and strong enforcement capabilities.<br>Leverage the ClearPass Security Ecosystem.<br>Integrating disparate tools and technologies is critical in today's security environment. Our Security Exchange Program brings together best-of-breed third-party solutions for end-to-end security – from the campus to the road warrior.<br><br>Key features<br>• Role-based, unified network access enforcement across multi-vendor wireless, wired and VPN networks.<br>• Intuitive policy configuration templates and visibility troubleshooting tools.<br>• Supports multiple authentication/authorization sources (AD, LDAP, SQL). |

| Solution | Brand | Product / Service | Description |
|---|---|---|---|
| | | | • Self-service device onboarding with built-in certificate authority (CA) for BYOD.<br>• Guest access with extensive customization, branding, and sponsor-based approvals.<br>• Integration with key UEM solutions for in-depth device assessments<br>• Comprehensive integration with the HPE Aruba Networking 360 Security Exchange Program.<br>• Single sign-on (SSO) support works with other identity management tools to improve user experience to SAML 2.0-based applications.<br>• FIPS 140-2 and CC certified. |
| Next Generation Firewall | Check Point | Quantum Maestro | Check Point Maestro introduces to the industry a new way to utilize current hardware investment and maximize appliance capacity in an easy-to manage Hyperscale network security solution to bring our networks and data center to the world of hybrid clouds.<br><br>With Maestro, organizations can simplify their data center workflow orchestration and scale up their existing Check Point security gateways on demand — the same way as they can spin up new servers and compute resources in public clouds. |
| | | Quantum NGFW | Check Point gateways provide superior security beyond any Next Generation Firewall (NGFW). Best designed for SandBlast's Zero Day protection, these gateways are the best at preventing the fifth generation of cyber-attacks with more than 60 innovative security services. Based on the Infinity Architecture, the new Quantum Security Gateway™ line up of 15 models can deliver up to 1.5 Tbps of threat prevention performance and can scale on demand. |
| | Cisco | Cisco Secure Firewall Threat Defense | Cisco Secure Firewall Threat Defense combines Cisco's proven network firewall with Snort IPS, URL filtering, and malware defense. It simplifies threat protection with consistent security policies across physical, private, and public cloud environments. Get deep visibility into your network and quickly detect threat origin and activity. Then, stop attacks before they impact on your operations.<br><br>**Features**<br>Cisco Firewall device manager (local management): ESXi, KVM and Openstack: Version 7.0 and above; Azure: Version 6.5 and above; AWS: 6.6 and above, Cisco Hyperflex: Version 7.0 and above; Nutanix AHV: Version 7.0 and above<br><br>**Centralized management:** Centralized configuration, logging, monitoring, and reporting are performed by the Cisco Firewall Management Center (all platforms including on-premises and in AWS, Azure, GCP and OCI(6.7 and above)) or alternatively in the cloud with Cisco Defense Orchestrator (ESXi and KVM; Azure: Version 6.5 and above, Cisco Hyperflex: Version 7.0 and above; Nutanix AHV: Version 7.0 and above)<br><br>**Application Visibility and Control (AVC):** Supporting more than 4000 applications, as well as geolocations, users, and |

| Solution | Brand | Product / Service | Description |
|---|---|---|---|
| | | | websites. OpenAppID support for custom, open-source, application detectors.<br><br>**Cisco Security Intelligence:** Standard with IP, URL, and DNS threat intelligence<br><br>IPS license for Cisco Secure Firewall: Snort 3 IPS can passively detect endpoints and infrastructure for threat correlation and Indicators of Compromise (IoC)<br><br>Malware Defense license for Cisco Secure Firewall: Enables detection, blocking, tracking, analysis, and containment of targeted and persistent malware, addressing the attack continuum both during and after attacks. Integrated threat correlation with Cisco Secure Endpoint is also optionally available.<br><br>**Cisco Secure Malware Analytics sandboxing URL filtering**: Support more than 80 categories and 280 million of URLs categorized.<br><br>**Automated threat feed and IPS signature updates**:<br>Third-party and open-source ecosystem: Open API for integrations with third-party products; Snort and OpenAppID community resources for new and specific threats<br><br>**High availability and clustering: Active/standby (ESXi and KVM only) Deployment modes**: Routed, transparent (inline set IPS-only), and passive; AWS, Azure, GCP and OCI: routed mode only |
| | | Meraki MX Cloud-Managed Security | The Cisco Meraki MX is a multifunctional security and SD-WAN enterprise appliance with a wide set of capabilities to address multiple use cases—from an all-in-one device. Organizations of all sizes and across all industries rely on the MX to deliver secure connectivity to hub locations or multicloud environments, as well as application quality of experience (QoE), through advanced analytics with machine learning.<br><br>The MX is 100% cloud managed, so installation and remote management is truly zero touch, making it ideal for distributed branches, campuses, and data center locations. Natively integrated with a comprehensive suite of secure network and assurance capabilities, the MX eliminates the need for multiple appliances. These capabilities include application-based firewalling, content filtering, web search filtering, SNORT®-based intrusion detection and prevention, Cisco Advanced Malware Protection (AMP), site-to-site Auto VPN, client VPN, WAN and cellular failover, dynamic path selection, web application health, VoIP health, and more. SD-WAN can easily be extended to deliver optimized access to resources in public and private cloud environments with virtual MX (vMX) appliances. Public clouds supported with vMX include Amazon Web Services (AWS), Microsoft Azure, Google Cloud Platform, Alibaba Cloud, and private cloud support through Cisco NFVIS.<br><br>Advanced quality of experience (QoE) analytics<br>• Monitor end-to-end health of web applications at-a-glance across the LAN, WAN, and application server |

| Solution | Brand | Product / Service | Description |
|---|---|---|---|
| | | | • Machine-learned smart application thresholds autonomously apply to identify true anomalies based on past behavioral patterns<br>• Monitor the health of all MX WAN links, including cellular, across your entire organization<br>• Get detailed hop-by-hop VoIP performance analysis across all uplinks<br><br>Agile on-premises and cloud security capabilities informed by Cisco Talos<br>• Next-gen layer 7 firewall for identity-based security policies and application management<br>• Advanced Malware Protection with sandboxing; file reputation-based protection engine powered by Cisco AMP<br>• Intrusion prevention: PCI-compliant IPS sensor using industry-leading SNORT® signature database from Cisco<br>• Granular and automatically updated category-based content filtering<br>• Other capabilities: SSL decryption/inspection, data loss prevention (DLP), cloud access security broker (CASB), SaaS tenant restrictions, granular app control, file type control.<br><br>Branch gateway services<br>• Built-in DHCP, NAT, QoS, and VLAN management services<br>• Web caching: accelerates frequently accessed content<br>• Load balancing combines multiple WAN links into a single high-speed interface, with policies for QoS, traffic shaping, and failover<br>• art connection monitoring provides automatic detection of layer 2 and layer 3 outages and fast failover, including the option of integrated LTE Advanced or 3G/4G modems<br><br>Industry-leading cloud management<br>• Unified firewall, switching, wireless LAN, and mobile device management through an intuitive web-based dashboard<br>• Template-based settings scale easily from small deployments to tens of thousands of devices<br>• Role-based administration, configurable email alerts for a variety of important events, and easily auditable change logs<br>• Summary reports with user, device, and application usage details archived in the cloud.<br><br>Intelligent site-to-site VPN with Cisco SD-WAN powered by Meraki<br>• Auto VPN allows automatic VPN route generation using IKE/IKEv2/IPsec setup; runs on physical MX appliances and as a virtual instance in public and private clouds<br>• SD-WAN with active/active VPN, policy-based routing, dynamic VPN path selection, and support for application-layer performance profiles to ensure prioritization of application types that matter<br>• Interoperates with all IPsec VPN devices and services<br>• Automated MPLS to VPN failover within seconds of a connection failure |

| Solution | Brand | Product / Service | Description |
|---|---|---|---|
| | | | • Layer2 TP IPsec remote client VPN included at no extra cost with support for native Windows, Mac OS X, iPad, and Android clients<br>• Support for Cisco AnyConnect remote client VPN (AnyConnect license required) |
| | Fortinet | FortiGate Next Generation Firewall | FortiGate provides flawless convergence that can scale to any location: remote office, branch, campus, data center, and cloud. We've always delivered on the concept of hybrid mesh firewalls with FortiManager for unified management and consistent security across complex hybrid environments. The Fortinet FortiOS operating system provides deep visibility and security across a variety of form factors. |
| | Palo Alto Networks | Palo Alto NGFW | Security capabilities on the Palo Alto Networks ML-Powered NGFW are delivered in an integrated platform that offers application, user and device-based policies, decryption of encrypted traffic, networking capabilities, high availability, and a host of cloud-delivered security subscriptions. Core security capabilities are built into the PAN-OS operating system, which powers all Palo Alto Networks ML-Powered NGFWs. Additional security capabilities are available through the deployment of Cloud-Delivered Security Services on the ML-Powered NGFW.<br><br>With the integrated platform, all Cloud-Delivered Security Services work seamlessly with each other. Also, the ML-Powered NGFWs' single-pass architecture ensures no additional performance overhead when enabling additional features.<br><br>Seamlessly integrated with our industry-leading NGFWs, our Cloud-Delivered Security Services use the network effect of 85,000 customers to instantly coordinate intelligence and protect against all threats across all vectors. Eliminate coverage gaps across your locations and take advantage of best-in-class security delivered consistently in a platform to stay safe from even the most advanced and evasive threats.<br><br>The ML-Powered NGFW is available in hardware (PA-Series), software (VM-Series and CN-Series), and cloud-delivered (Prisma Access) form factors. |
| | Sangfor | Sangfor Network Secure | Sangfor Network Secure (previously known as NGAF) takes Next Generation Firewall technology to the next level to meet the evolving security needs of modern enterprises. Through market foresight and technical prowess, Sangfor Network Secure holds several "world's first" titles.<br><br>Sangfor Network Secure Advantages Advanced Threat Detection<br>Sangfor Network Secure leverages artificial intelligence, machine learning, and real-time threat intelligence to deliver a superior malware detection rate of 99.76%, keeping the vast majority of security threats outside the network perimeter. Cloud Deception<br>Sangfor Network Secure is the first NGFW with built-in deception technology. The cloud deception feature sets up |

| Solution | Brand | Product / Service | Description |
|---|---|---|---|
| | | | decoy systems in the cloud to help administrators locate and stop malicious actors and lateral movement.<br><br>Next-Gen WAF Sangfor Network Secure is the first NGFW integrated with NG-WAF. The groundbreaking WISE Engine utilizes semantic analysis and machine learning techniques to empower NG-WAF to stop known and unknown web attacks.<br><br>SOC Lite<br>SOC (Security Operations Center) Lite is a lifesaver for security administrators of small to mid-size enterprises. Network Secure provides intuitive security visibility with response guidance that allows administrators to quickly determine the threat level of users, servers, and ransomware events.<br><br>Anti-Ransomware<br>Sangfor Network Secure integrates with Sangfor Endpoint Secure (Endpoint Detection and Response- EDR) and Cyber Command (Network Detection and Response – NDR) as part of Sangfor's Anti-Ransomware solution.<br><br>Forensic threat intelligence data, collected from the network and endpoints, visualizes the hidden ransomware process through the GUI and provides "one-click quarantine" to eradicate the encryption-controlling application from all infected hosts.<br><br>Security Integration<br>Sangfor Network Secure integrates seamlessly with endpoint and network security products to create a truly holistic solution. Each product works in tandem to close the gaps between their spheres of influence to deliver a foolproof security system. |
| SASE | Check Point | Quantum SASE | Secure Access Service Edge (SASE) promises a better way to protect hybrid work and cloud networks. But existing solutions are fragmented and frustrating for users.<br><br>Quantum SASE from Check Point is different. Quantum SASE delivers 2x faster internet security combined with full mesh Zero Trust Access and optimized SD-WAN performance—all with an emphasis on ease-of-use and streamlined management. |
| | Cisco | Cisco Umbrella | Cisco Umbrella is cloud-delivered enterprise network security which provides users with a first line of defense against cybersecurity threats. Cisco Umbrella uses the Internet's infrastructure to enforce security and block malicious activity before a connection is ever established. By delivering security from the cloud, there is no hardware to install and no software to manually update.<br><br>DNS-layer security: Simple to deploy, easy to manage DNS is at the heart of every internet connection request. Securing the DNS layer means blocking malicious domains, IP addresses, and cloud applications before a connection is ever established. Join the more than 26,000 organizations that use Umbrella to deliver a fast, safe, and reliable internet experience. |

| Solution | Brand | Product / Service | Description |
|---|---|---|---|
| | | | SSE: Converged security protects users anywhere and everywhere. Cybersecurity is evolving. SSE, or Security Service Edge, consolidates formerly disparate features like secure web gateway, data loss prevention, CASB, ZTNA, and DNS security into one cloud-delivered architecture, so organizations can streamline and improve their security resilience.<br><br>As a leading provider of recursive DNS services, we've helped businesses of all sizes and industries connect to the internet with confidence. We've built a reputation on easy deployment and powerful protection anywhere users work. To help organizations embrace direct internet access, in addition to DNS-layer security and interactive threat intelligence, Cisco Umbrella now includes secure web gateway, firewall, and cloud access security broker (CASB) functionality, plus integration with Cisco SD-WAN, delivered from a single cloud security service. |
| | Forcepoint | Forcepoint ONE | Forcepoint ONE is a cloud service that secures data everywhere for distributed businesses and government agencies that need to adapt quickly to changing remote and hybrid workforces. It gives employees, contractors, and other users safe, controlled access to business information on the web, in the cloud (SaaS and IaaS), and in private applications, while keeping attackers out and sensitive data in. As a result, Forcepoint ONE makes users more productive, whether remote or in the office, and businesses more efficient.<br><br>Forcepoint ONE combines Zero Trust and SASE security technologies, including three secure access gateways and a variety of shared threat protection and data security services, all built on a cloud-native platform. This approach enables organizations to manage one set of policies, in one console, communicating with one endpoint agent.<br>• Secure Web Gateway (SWG). Monitors and controls any interaction with any website, including blocking access to websites based on category and risk score, blocking download of malware, blocking upload of sensitive data or securing use with digital rights management, and detecting and controlling shadow IT.<br>• Cloud Access Security Broker (CASB). Agent-based or agentless solution that enforces granular access controls over company SaaS apps based on identity, location, device, and group that enforces granular access controls for private applications in real time. Scans data at rest in popular SaaS and IaaS for malware and sensitive data and remediates as needed. The agentless option facilitates BYOD and contractor access.<br>• Zero Trust Network Access (ZTNA). Agent-based or agentless solution that allows granular access to private applications without the use of a VPN. Agent based solution required for non-HTTP/S applications. |
| | Palo Alto Networks | Prisma SASE | Palo Alto Networks Prisma SASE is the industry's most complete single vendor secure access service edge (SASE) solution, delivering: |

| Solution | Brand | Product / Service | Description |
|---|---|---|---|
| | | | • Superior ZTNA 2.0 security: Consistently protect the hybrid workforce with the superior, AI-powered security of ZTNA 2.0.<br>• Next-Generation SD-WAN: The industry's first Next-Generation SD-WAN solution that delivers branch transformation with an exceptional user experience while simplifying operations with improved security outcomes.<br>• Exceptional user experience: Integrated Autonomous Digital Experience Management (ADEM) empowers IT to detect, predict, and resolve issues with applications, networks, and the security posture to proactively deliver great user experiences. |
| | | Prisma Access | Prisma Access enables organizations to securely connect all users to the internet, SaaS, and private applications they need, regardless of where they're accessing them from or which device they are using, all while significantly reducing risk. It provides a cloud-native single product to secure hybrid enterprises and workforces, is made up of best-in-class security capabilities, optimizes the user experience with dynamic scalability, and guarantees maximum end-user performance. Prisma Access makes securing today's hybrid workforces and cloud-first organizations easy by offering:<br>• The superior protection of ZTNA 2.0 combines fine-grained, least-privileged access with deep and ongoing security inspection as well as enterprise DLP to protect all users, devices, apps, and data.<br>• A unified security product with comprehensive protections converged into a single unified product, single-pane-of-glass visibility, consistent policy management, and shared data for all users and all apps.<br>• The best user experiences from a truly cloud-native architecture built to secure at cloud scale, providing uncompromised performance—all backed by leading SLAs.<br><br>Prisma Access consolidates best-in-class security in a leading cloud-native security service edge (SSE) platform. When combined with Prisma SD-WAN, businesses are able to transform their networking and security with the most complete secure access service edge (SASE) solution in the industry. |
| SD-WAN | Check Point | Quantum SD-WAN | Unifying the best security with optimized internet and network connectivity.<br><br>Most SD-WAN solutions were not built with security in mind, opening branch networks to increased risk. To bridge this gap, Quantum SD-WAN unifies the best security with optimized internet and network connectivity.<br><br>A software blade activated in Quantum Gateways, Quantum SD-WAN is deployed at the branch level and provides comprehensive prevention against zero-day, phishing, and ransomware attacks, while optimizing routing for users and over 10,000 applications. |
| | Fortinet | Secure SD-WAN | Simplify Your Network Security with One Operating System<br>As the use of business-critical, cloud-based applications continues to increase, organizations with a distributed |

| Solution | Brand | Product / Service | Description |
|---|---|---|---|
| | | | infrastructure of remote offices and an expanding remote workforce need to adapt. The most effective solution is to switch from static, performance-inhibited wide-area networks (WANs) to software-defined WAN (SD-WAN) architectures.<br><br>Traditional WANs may utilize SLA-backed private multiprotocol label switching (MPLS) or leased line links to an organizations' main data centers for all application and security needs. But that comes at a premium price for connectivity. While a legacy hub-and-spoke architecture may provide centralized protection, it increases latency and slows down network performance to distributed cloud services for application access and compute. The result is operational complexity and limited visibility associated with multiple point products. This scenario adds significant management overhead and difficulties, especially when trying to troubleshoot and resolve issues.<br><br>Fortinet's Secure Networking strategy tightly integrates an organization's network infrastructure and security architecture, enabling networks to transform at scale without compromising security. This next-generation approach provides consistent security enforcement across flexible perimeters by combining a next-generation firewall with advanced SD-WAN networking capabilities. |
| Secure Remote Access | Ivanti | Ivanti Connect Secure | The modern workforce is a remote workforce, and the modern workplace has spread beyond the office and the traditional data center to the cloud. With the increased number and complexity of applications users need, the many different types of devices users can connect from, and the constant threat of malicious actors, securing the Everywhere Workplace can be a daunting task.<br><br>Ivanti Connect Secure provides a seamless, cost- effective, SSL VPN solution for remote and mobile users from any web-enabled device to corporate resources — anytime, anywhere. Powerful and easy to use, Ivanti Connect Secure is the most widely deployed SSL VPN for organizations of any size, across every major industry. |
| SIEM | Opentext | ArcSight SIEM Security Open Data Platform | ArcSight Security Open Data Platform (SODP) by OpenText offers a future-ready data solution that enriches data in real time and supports open standards for better threat detection. Using security data connectors, SODP collects data and enriches it in real-time to give analysts organized information that can be acted upon instantly. With an intelligent Transformation Hub, built on a foundation of Apache Kafka, ArcSight Security Open Data Platform can ingest and broker data from any source, anywhere, seamlessly. |
| | SolarWinds | SolarWinds SEM | Thousands of resource-constrained IT and security pros rely on SolarWinds® Security Event Manager (SEM) for affordable and efficient threat detection, automated incident analysis and response, and compliance reporting for their IT infrastructure. Our SIEM solution combines log management, threat detection, normalization and correlation, forwarding, reporting, file integrity monitoring, user activity monitoring, USB detection and prevention, threat intelligence, and active response in a virtual appliance that's easy to deploy, manage, |

| Solution | Brand | Product / Service | Description |
|---|---|---|---|
| | | | and use. We've designed our SIEM to provide the functionality you need without the complexity and cost of most other enterprise SIEM solutions.<br><br>SECURITY EVENT MANAGER AT A GLANCE<br>Easy Collection and Normalization of Network Device and Machine Logs Security Event Manager comes with hundreds of out-of-the-box connectors to simplify the process of collecting, standardizing, and cataloging log and event data generated across your network. Our industry leading log compression rate allows more data to be stored with fewer resources required.<br><br>Customizable Visualizations and Dashboard<br>Quickly identify important or suspicious patterns in machine data with a wide variety of customizable visualizations and a flexible dashboard. Drill into interesting patterns with a click of a button and see the full list of related logs and their details.<br><br>Powerful and Simple Searching for Forensic Analysis and Troubleshooting<br>Security Event Manager is designed to allow users to quickly find important log data using simple keyword searches in both real-time event data as well as historical data at predefined or custom time periods. Out-of-the-box and user-defined filters also provide fast data refinement.<br><br>Real-Time, In-Memory Event Correlation<br>By processing and normalizing log data before it's written to the database, Security Event Manager can deliver true real-time log and event correlation. Predefined and custom correlation rules allow Security Event Manager to automatically alert on possible security breaches and other critical issues.<br><br>Out-of-the-Box Security and Compliance Reporting Templates<br>Security Event Manager makes it easy to generate and schedule compliance reports quickly using over 300 report templates and a console allowing for customizable reports to meet your organization's specific needs.<br><br>Threat Intelligence Feed and Groups<br>Correlation rules are enhanced with a fully integrated, regularly updating threat intelligence feed that automatically identifies and tags malicious activity from known bad IPs. Easily build groups containing values relevant to your environment, such as user and computer names, sensitive file locations, and approved USB devices. These groups can be auto populated via correlation rules and can help simplify searching and reporting.<br><br>Built-in Active Response<br>Security Event Manager can do much more than trigger email alerts. SEM is designed to immediately respond to security, operational, and policy-driven events using predefined responses, such as quarantining infected machines, blocking IP addresses, killing processes, and adjusting Active Directory® settings. |

| Solution | Brand | Product / Service | Description |
|---|---|---|---|
| | | | **Enhanced, Real-Time File Integrity Monitoring**<br>Embedded File Integrity Monitoring (FIM) is designed to deliver broader compliance support and deeper security intelligence for insider threats, zero-day malware, and other advanced attacks. Leverage enhanced filter capabilities for finer tuning and significantly reduced the noise associated with lower priority file changes, increasing productivity and efficiency.<br>USB Detection and Prevention<br>Security Event Manager can help prevent endpoint data loss and protect sensitive data with real-time notifications when USB devices connect, the ability to automatically block their usage, and built-in reporting to audit USB usage.<br><br>**Log Forwarding and Exporting**<br>Security Event Manager forwards raw log data with syslog protocols (RFC 3164 and RFC 524 4) to other applications for further use. Additionally, users can export logs to a CSV file so the data can be shared with other teams and external vendors, uploaded to other tools, or attached to helpdesk tickets. |
| | Splunk | Splunk Enterprise | Do you want to get more value from your data? Splunk Enterprise collects data from any source, including metrics, logs, clickstreams, sensors, stream network traffic, web servers, custom applications, hypervisors, containers, social media and cloud services. It enables you to search, monitor and analyze that data to discover powerful insights across multiple use cases like security, IT operations, application delivery, industrial data and IoT. Additionally, with the power of machine learning baked in, you can make faster, more informed decisions across the organization.<br><br>With Splunk Enterprise, everyone from data and security analysts to business users can gain insights to drive operational performance and business results. Whether you're looking to troubleshoot IT, monitor your security posture and application development, or optimize marketing campaigns, Splunk Enterprise can help get you there. |
| | | Splunk Enterprise Security | Splunk Enterprise Security (ES) is a data-centric, modern security information and event management (SIEM) solution that delivers data-driven insights for full-breadth visibility into your security posture so you can protect your business and mitigate risk at scale. With unparalleled search and reporting, advanced analytics, integrated intelligence, and pre- packaged security content, Splunk ES accelerates threat detection and investigation, letting you determine the scope of high-priority threats to your environment so you can quickly act. Splunk ES is built on an open and scalable data platform that allows you to stay agile in the face of evolving threats and business needs. |
| SOAR | Palo Alto Networks | Cortex XSOAR | Redefining Security Orchestration, Automation, and Response<br>Security teams need more people and scalable processes to keep pace with an overwhelming volume of alerts and endless security tasks. Analysts waste time pivoting across consoles for data collection, determining false positives, and performing repetitive, manual tasks throughout the lifecycle of an incident. Faced with a growing skills shortage, security leaders |

| Solution | Brand | Product / Service | Description |
|---|---|---|---|
| | | | deserve more time to make decisions that matter rather than drown in reactive, fragmented, manual responses. This is not the way.<br><br>Transform Security Operations<br>Your SOC teams can simplify security operations by unifying automation, case management, real-time collaboration, and threat intelligence management. This means you can manage alerts across all sources, standardize processes with playbooks, take action on threat intelligence, and automate response options for virtually any use case, all with the help of Cortex XSOAR.<br><br>Experience Better Performance, Reliability, and Scalability<br>Cortex XSOAR now offers cloud-native SOAR that auto scales to support future growth, with rapid deployment to accelerate your return on investment (ROI). Fully integrated into the Cortex platform, Cortex XSOAR is delivered through a unified user interface for ease of use and consistency in workflow management. |
| Threat Hunting Service | CrowdStrike | Overwatch | Falcon OverWatch™ is CrowdStrike's managed threat hunting service, built on the CrowdStrike Falcon® platform. OverWatch provides deep and continuous human analysis, 24/7, to relentlessly hunt for anomalous or novel attacker tradecraft that is designed to evade standard security technologies.<br><br>OverWatch is comprised of an elite team of cross-disciplinary specialists who harness the massive power of the CrowdStrike Threat Graph®, enriched with CrowdStrike threat intelligence, to continuously hunt, investigate and advise on sophisticated threat activity in customer environments. Armed with cloud-scale telemetry and detailed tradecraft on more than 130 adversary groups, OverWatch provides unparalleled ability to see and stop the most advanced threats. |
| | SentinelOne | Watchtower | As the global threat landscape evolves in complexity and scope, cybersecurity teams protect dynamic and dispersed attack surfaces from threat actors with changing motivations and techniques.<br><br>SentinelOne WatchTower offers security teams the expertise and proactive protection they need, by detecting anomalous and hands-on-keyboard threat activity with behavioral threat hunting, machine learning models backed by global SentinelOne telemetry, and best-in-class threat intelligence.<br><br>Overextended security teams can also dive deeper with WatchTower Pro to uncover and remediate hidden threats and security risks unique to your environment to offer you peace-of-mind with in-depth compromise assessments that enhance your team's agility and mitigate their risks with attack surface mapping, dark web exposure reviews, and externally facing vulnerability risk reviews. |
| Threat Intelligence Service | Recorded Future | Recorded Future Threat Intelligence | Defending against new and emerging cyber threats requires timely, relevant insights updated in real-time. Recorded Future's Threat Intelligence module provides a comprehensive view of your unique threat landscape through a combination of automated analytics, human-finished intelligence, and |

| Solution | Brand | Product / Service | Description |
|---|---|---|---|
| | | | advanced search and analysis capabilities. With our Intelligence Cloud, billions of entities are fused together to deliver original research to dynamically categorize, link, and analyze intelligence with unprecedented speed, arming you with easy-to-consume insights that are easily integrated directly into your existing security tools and workflows.<br><br>The world's most advanced intelligence cloud empowers you to make fast, confident decisions. Features like advanced querying capabilities, real-time alerting, and threat visualization capabilities provide the context you need for advanced threat research and threat hunting.<br><br>Quickly detect critical threats with the Recorded Future Threat Intelligence module – and get ahead of emerging ones to disrupt adversaries before they get to you. |
| Vulnerability Management | Rapid7 | Rapid7 InsightVM | InsightVM lets you stay one step ahead of bad actors by providing clarity into where risk is present across your ecosystem, and visibility into the cross-functional operations needed to prioritize and remediate those vulnerabilities.<br><br>With this deep and accurate understanding of your risk, you can better inform and align technical teams from prioritization through remediation, and track and see shared progress. |
| | | Rapid7 Nexpose | Vulnerabilities pop up every day. You need constant intelligence to discover them, locate them, prioritize them for your business, and confirm your exposure has been reduced. Nexpose, Rapid7's on-premises option for vulnerability management software, monitors exposures in real-time and adapts to new threats with fresh data, ensuring you can always act at the moment of impact. |
| | Tenable | Tenable Nessus | Scarce resources, limited time, a constantly changing attack surface – it's a challenge for security practitioners on the front lines to keep pace with attackers. You need a fast, easy way to proactively find and fix vulnerabilities.<br><br>Nessus® Professional automates point-in-time assessments to help quickly identify and fix vulnerabilities, including software flaws, missing patches, malware, and misconfigurations, across a variety of operating systems, devices, and applications. |
| | | Tenable Vulnerability Management | Discover, Assess and Prioritize Vulnerabilities<br>Tenable Vulnerability Management is available as part of the Tenable One Exposure Management Platform or as a stand-alone product. Tenable Vulnerability Management gives you a risk-based view of your entire attack surface- from IT to cloud to OT and containers- so you can quickly identify, investigate, and prioritize vulnerabilities. You get immediate visibility so you can understand your risk and know which vulnerabilities to fix first.<br><br>Powered by Nessus technology and managed in the cloud, Tenable Vulnerability Management provides the industry's most comprehensive vulnerability coverage with the ability to predict which security issues to remediate first. Using an advanced asset identification algorithm, Tenable Vulnerability |

| Solution | Brand | Product / Service | Description |
|---|---|---|---|
| | | | Management provides the most accurate information about dynamic assets and vulnerabilities in ever-changing environments. As a cloud-delivered solution, its intuitive dashboard visualizations, comprehensive risk-based prioritization, and seamless integration with third-party solutions help security teams maximize efficiency and scale for greater productivity. |
| | | Tenable Security Center | **See Everything. Predict What Matters. Managed On-Prem. With Tenable Security Center Plus.**<br><br>Changing IT landscapes and evolving cyber threats have made periodic scanning and compliance audits ineffective in protecting against modern cyberattacks. To keep your organization safe, you need a vulnerability management solution that gives you complete visibility into your attack surface so you can effectively manage and measure your cyber risk.<br><br>Built on leading Nessus technology, Tenable Security Center Plus is a market leading vulnerability management platform that delivers the next generation of vulnerability management, on prem. Through advanced analytics, customizable dashboards, reports and workflows, Tenable Security Center Plus helps you master vulnerability management and reduce organizational risk.<br><br>Leverage Predictive Prioritization combines data and threat intelligence across multiple sources to anticipate the probability of a vulnerability being exploited, paired with the criticality of your dynamic assets in an ever-changing environment. The result?- a lens to help view and prioritize vulnerabilities tied with their most critical assets giving you actionable insight for protecting your organization against a business impacting breach.<br><br>Tenable Security Center Plus includes over 350 pre-built, highly customizable dashboards and reports to give you immediate insight into your security compliance, effectiveness and risk. You can continuously measure, analyze and visualize the effectiveness of your security program, based on high-level business objectives and underlying customizable policies that executives care about. |
| Middle Ware | Cloudflare | Developer Platform | **Build applications on the connectivity cloud**<br>Build & deploy code at edge Build and deliver powerful, trusted applications on Cloudflare's global network. Write code, test and deploy static and dynamic applications without configurations and manage your web assets and performance. Deploy code instantly across Cloudflare’s global network Save money with generous free tiers Innovate faster when developers are free to focus on code not configs |
| | | Network Services | **Modern security and performance Protect & accelerate networks**<br>Traditional solutions just aren’t designed to fulfill the Internet’s basic needs: security, performance, and reliability. Modernize your network approach. |
| | SonaType | Lifecycle | **Control open-source risk across your SDLC** |

| Solution | Brand | Product / Service | Description |
|---|---|---|---|
| | | | Automatically find and fix open-source vulnerabilities across the SDLC |
| | | Nexus Repository | **Build fast with centralized components**<br>Manage components, binaries and build artifacts across your entire software supply chain. |
| | | Repository Firewall | **Block malicious open source at the door**<br>Your first line of defense against modern software supply chain attacks. |
| **Web Application and API Protection** | Cloudflare | Application Services | Cloudflare's connectivity cloud provides powerful application and API security, allowing for no-gaps security and unified control from a single console. Our global edge network of 300 data centers in over 100 countries ensures exceptional performance, reliability, and scalability.<br><br>Cloudflare enhances web application performance and user experience, providing seamless access to content across all devices and ensuring business continuity during traffic spikes, attacks, and outages. |
| | Imperva | Imperva Cloud WAAP | Imperva Cloud WAAP protects web applications and APIs from application layer hacking attempts and DDoS attacks using an auto-scaling, multitenant cloud environment. It offers bot mitigation, Web Application Firewall (WAF), API protection, and DDoS protection. |
| | | Imperva Runtime Protection | Imperva RASP, a key component of Imperva's market, offers the industry's leading runtime application self-protection solution, providing enterprise-class protection against known and zero-day attacks. It easily integrates with your applications and existing DevOps processes to secure by default, preventing exploits in production and reducing risk. |
| | | Imperva Web App Security | Imperva Web Application Security protects web applications and APIs from application layer hacking attempts and DDoS attacks using an auto-scaling, multitenant cloud. Its security modules include bot mitigation, Web Application Firewall (WAF), API protection, and DDoS protection. |
| **Web Security** | Forcepoint | Forcepoint ONE Secure Web Gateway (SWG) | The Forcepoint ONE Secure Web Gateway (SWG) is one of the three foundational gateways of the Forcepoint ONE all-in-one cloud platform. Forcepoint ONE SWG monitors and controls any interaction with any website, including blocking access to websites based on category and risk score, blocking download of malware, blocking upload of sensitive data to personal file sharing accounts, detecting shadow IT, and optionally providing Remote Browser Isolation (RBI) with Content Disarm and Reconstruction (CDR) |
| | Sangfor | Sangfor Internet Access Gateway | Sangfor IAG enables you to identify, analyze and take immediate action upon user internet access behavior. Gain full visibility to find any bad behavior in encrypted traffic. Uncover user identity with analytics into who is using what applications and when it is used on your network. Take full control to increase user productivity by ensuring internet access compliance. |

| Solution | Brand | Product / Service | Description |
|---|---|---|---|
| | | | Product Advantages<br>Proxy Avoidance Protection:<br>Web filters are commonly used by the organization to restrict user internet access to certain web application content, and it has increasingly become non-effective against proxy avoidance applications. IAG collaborates with Endpoint Secure to enforce Proxy Avoidance Protection on any user attempt to use this application for bypassing the security perimeter more effectively. The R&D team within Sangfor employs a dedicated team of application signatures security experts who are continuously categorizing and adding the latest proxy avoidance applications to ensure that detection rate and blocking capabilities are current and up to date.<br><br>Intelligent Traffic Management<br>Sangfor IAG improves bandwidth utilization by more than 30% using three unique major traffic management solutions. Dynamic Traffic Control automatically adjusts traffic control policies and intelligently allocates idle bandwidth resources. Intelligent Flow Control manages both up-link and down-link P2P traffic and can customize traffic "packages" for different users, allocating specific traffic quotas and limiting bandwidth for heavier users.<br><br>Gateway and Client Decryption to Uncover Encrypted Traffic<br>Typically, most of the internet traffic is protected by SSL/TLS encryption. While encryption helps to keep user and corporate data protected and private, it also creates security challenges when it comes to the rapid growth of malware infections and other malicious content. Sangfor IAG offers both decryption methods including gateway and client decryption to overcome these challenges. This enables an organization to have the flexibility to run either one or both in parallel to uncover encrypted traffic according to your corporate IT strategy and planning.<br><br>Unified Network-wide Management of all Clients<br>Sangfor IAG provides Unified Management and effectively controls both Wired and Wireless networks for the entire network. With intuitive and flexible authentication methods, it fully guarantees the security of access control, supporting a variety of traditional authentication methods such as username/password, IP/MAC binding, and a wide array of value-added marketing authentication methods (QR code, SMS, WeChat, social media, OA account, SAML 2.0, third-party system, etc.). Permissions are controlled based on user, application, location, and client types while using IAG or third-party wireless controller as a unified authentication server, building a faster and more cost-effective wireless network.<br><br>Precise and Accurate Application Control<br>Sangfor IAG manages and controls network applications more comprehensively, accurately, and conveniently with the largest application signature database in Asia, which can identify more than 6,000+ applications in its database including 700+ cloud applications, 1,000+ mobile applications, 300+ web applications, and is updated every 2 weeks. In addition, it precisely controls applications according to their specific functions, such as distinguishing upload, download, |

| Solution | Brand | Product / Service | Description |
|---|---|---|---|
| | | | and other actions in the network. Finally, bulk management mode for large enterprises greatly improves management efficiency.<br><br>**Offloading Performance When Using ICAP Integration with Third-Party System**<br>Sangfor IAG can act as an ICAP client to be used with any ICAP server-enabled network appliance by offloading threat protection or other value-added services. In addition, Sangfor IAG provides request and response inspection mode while enabling the ICAP server group to run on a round-robin or concurrent condition.<br><br>**Secure Onboarding Devices with Endpoint Compliance Check**<br>Sangfor IAG identifies and secures endpoint devices with or without agents, it helps to ensure these devices are connected with compliance and security. You gain visibility and control of what is in your environment without impacting your network performance. |
| | Trend Micro | Web Security | The rising sophistication and complexity of web threats, coupled with the new ways your employees do their work, have eroded the effectiveness of traditional web security solutions. In addition to blocking malicious code, inappropriate websites, and targeted attacks, security managers also need to protect an increasingly mobile workforce who frequently adopt new cloud-based applications.<br><br>Trend Micro Web Security protects against cyber threats before they reach your users. It uses cross-generational defense techniques to catch known and unknown threats, giving you visibility and access control on unsanctioned cloud applications for each of your users. Our unique deployment model provides you with the flexibility to deploy gateways on-premises, in the cloud, or both—protecting your users no matter where they are. One cloud-based management console simplifies your workload, letting you set up policy, manage users, and access reporting across a single pane of glass. |
| | Zscaler | Zscaler Internet Access (ZIA) | Zscaler Internet Access includes a comprehensive suite of AI-powered security and data protection services to help you stop cyberattacks and data loss. As a fully cloud-delivered SaaS solution, you can add new capabilities without any additional hardware or lengthy deployment cycles. The modules available as part of Zscaler Internet Access are:<br>• Cloud Secure Web Gateway (SWG): Deliver a safe, fast web experience that eliminates ransomware, malware, and other advanced attacks with real-time, AI-powered analysis and URL filtering from the only leader in the 2020 Gartner MQ for SWGs.<br>• Cloud Access Security Broker (CASB): Secure cloud apps with integrated CASB to protect data, stop threats, and ensure compliance across your SaaS and IaaS environments.<br>• Cloud Data Loss Prevention (DLP): Protect data in motion with full inline inspection and advanced measures like exact data match (EDM), optical character recognition (OCR), and machine learning. |

| Solution | Brand | Product / Service | Description |
|---|---|---|---|
| | | | • Zscaler Firewall & cloud IPS: Extend industry- leading protection to all ports and protocols and replace edge and branch firewalls with a cloud native platform.<br>• Zscaler Sandbox: Stop never-before-seen and elusive malware across web and file transfer protocols with AI-driven quarantine, sharing consistent and global protection across all users in real time.<br>• AI-Powered Cloud Browser Isolation: Make web-based attacks obsolete and prevent data loss by creating a virtual air gap between users, the web, and SaaS.<br>• Digital Experience Monitoring: Reduce IT operational overhead and speed up ticket resolution with a unified view of application, cloud path, and endpoint performance metrics for analysis and troubleshooting.<br>• Zero Trust Branch Connectivity: Reduce risk and complexity with non-routable branch and data center connectivity for users, servers, and IOT/OT devices.<br>• DNS Security: Optimize DNS security and performance for all users, devices, and applications, on all ports and protocols, anywhere in the world. |
| Workload Protection | Trend Micro | Cloud One Workload Security | The data center is undergoing a tremendous transformation. Organizations are now moving their server workloads to the cloud and even leveraging containers and serverless in their cloud-native application architectures. There are many advantages of hybrid cloud computing, however, it also comes with new risks and threats. Your organization must ensure compliance requirements are met and that you have unified security across all your workloads, such as physical servers, virtual, cloud, or containers.<br>Trend Cloud One™ – Workload Security provides comprehensive detection and protection in a single solution that is purpose-built for server, cloud, and container environments. Workload Security allows for consistent security, regardless of the workload. It also provides a rich set of application programming interfaces (APIs) so security can be automated and won't impact your teams. |
| XDR | Cisco | Cisco XDR | Cisco XDR changes the way security teams look at detection and response. Our cloud-based solution is designed to simplify security operations and empower security teams to detect, prioritize, and respond to the most sophisticated threats. Integrating with the broader Cisco security portfolio and select third-party offerings, Cisco XDR is one of the most comprehensive and flexible solutions on the market today.<br><br>Designed by security practitioners for security practitioners, Cisco XDR helps analysts aggregate and correlate data from multiple sources into a unified view to streamline investigations, reduce false positives, prioritize alerts, and achieve the shortest path from detection to response.<br><br>Built-in automation, orchestration, and guided remediation recommendations help analysts automate repetitive tasks and mitigate threats more effectively, freeing up time and resources to focus on other critical security tasks.<br><br>The data-driven Cisco XDR approach allows SOC teams to define the most impactful events and focus remediation |

| Solution | Brand | Product / Service | Description |
|---|---|---|---|
| | | | strategies there first, strengthening the organization's overall security posture and increasing resilience.<br><br>**Benefits of Cisco XDR**<br>Unify visibility regardless of vendor or vector to avoid blind spots<br>Gain visibility and identify threats across network, cloud, endpoint, email, and applications for effective security across multi-vendor, multi-vector environment.<br><br>By correlating data from multiple disparate detection technologies into a unified view, Cisco XDR enables faster, more simplified investigations to streamline responses.<br><br>**Accelerate threat detection and response to act on what truly matters**<br>Correlate detections across multiple telemetry sources to prioritize threats by greatest risk.<br><br>By leveraging AI and machine learning, Cisco XDR enables high-fidelity correlated detection, reduces clutter, and effectively aligns security risk with business risk.<br><br>**Automate responses with evidence backed recommendations to minimize impact.**<br>Remediate threats confidently using automation and guided response recommendations across all relevant control points.<br><br>By compressing investigation time and accelerating responses, Cisco XDR levels-up SOC teams to build resilience.<br><br>Deliver comprehensive threat detection and response actions with data-backed insights<br><br>**Detect complex threats sooner**<br>• Cisco XDR offers the broadest range of built-in integrations across endpoint, email, network, cloud, firewall and more, as well as select third-party integrations for the most flexible, scalable and effective XDR strategy.<br>• Leverage telemetry from on-prem networks and public and private clouds to detect threats on managed and unmanaged devices and gain critical context when correlating events, including where attacks start and how they spread through the network.<br>• Talos threat intelligence strengthens detection capabilities, so analysts gain an unrivaled collection of actionable information to expose known and emerging threats with deeper context and awareness of real-world threat behavior.<br><br>**Prioritize threats by impact and act on what matters most, faster**<br>• Risk-based prioritization helps SOC analysts focus on the alerts that pose the greatest threat, allowing them to take rapid and effective action. This unique approach provides a unified view of alerts, prioritized by real-world severity.<br>• Reduce the Mean Time to Respond (MTTR) with guided responses for identification, containment, eradication and |

| Solution | Brand | Product / Service | Description |
|---|---|---|---|
| | | | recovery. That, combined with embedded response actions enable consistent, effective decision-making.<br>• Simplify and compress investigation times with unified context and progressive disclosure techniques. Cisco XDR shows analysts the information they need without inundating them with extraneous data leading to analysis paralysis. If needed, more information to enrich investigations is always just a click away<br>• Accelerate response times.<br>• Rapidly remediate threats with built-in response actions and orchestration. With Cisco XDR, SOC teams can leverage a range of pre-built and customizable orchestration workbooks to help shut down threats and mitigate risk with just a few clicks.<br>• Boost limited resources for maximum value by automating repetitive and time-consuming tasks and providing SOC teams with out-of-the-box best practices. When automation is not suitable, Cisco XDR provides guided response suggestions and recommendations to help SOC analysts take effective response actions.<br>• Quickly push response actions across a broad range of security tools through deep integrations with varying security control points, both built-in Cisco solutions and third-party. Take a proactive role in threat hunting by surveying across disparate alert logs as you learn of new tactics, techniques and indicators of compromise. |
| | Palo Alto Networks | Cortex XDR | **Prevent, Detect, and Respond to the Stealthiest Threats**<br>You can now stop modern attacks with Cortex XDR – the industry's first endpoint-based extended detection and response platform that integrates data from any source. Your SOC team can cut through the noise and focus on what matters most with intelligent alert grouping and incident scoring. Cross-data insights accelerate investigations so that you can streamline incident response and recovery. Finally, by harnessing the power of AI, analytics, and rich data, XDR allows you to detect stealthy threats.<br><br>Cortex XDR delivers peace of mind with industry-leading endpoint security that achieved the highest combined protection and detection scores in the 2022 MITRE ATT&CK Evaluations. The Cortex XDR platform collects and analyzes all data, so you can gain complete visibility and holistic protection to secure what's next.<br><br>**Block Attacks with Best-in-Class Endpoint Detection and Response**<br>The Cortex XDR agent offers unparalleled protection for exploits, malware, ransomware, and fileless attacks. It includes the broadest set of exploit protection modules available to block malware infections. It enables sharp detection with AI-powered analytics and threat insights. Finally, it allows you to remediate quickly and take control of affected machines." |
| | SentinelOne | S1 Singularity XDR | The cybersecurity threat landscape is evolving exponentially in both speed and scope. Meanwhile, most security teams struggle to keep pace with emerging threats with the resources they have at hand. These organizations often lack |

| Solution | Brand | Product / Service | Description |
|---|---|---|---|
| | | | global visibility and context across their technology stacks, creating gaps in what they can see and detect. Simultaneously, analysts juggle point tools for each vector, forcing them to analyze data in isolation and manually investigate. Today's security teams need a more proactive solution to identify, contain, and remediate emerging threats.<br><br>SentinelOne Singularity XDR unifies and extends detection and response capabilities across multiple security layers, including endpoint, cloud, identity, network, and mobile, providing security teams with centralized end-to-end enterprise visibility, powerful analytics, and auto- mated response across a large cross-section of the technology stack. |
| | Trend Micro | Vision One | Trend Vision One delivers the broadest native XDR sensor coverage in the cybersecurity market. The platform's native-first, hybrid approach to XDR and ASM benefits your security teams by delivering richer activity telemetry—not just detection data—across security layers with full context and understanding. This results in earlier, more precise risk and threat detection and more efficient investigation. |
| | | Managed XDR (MDR) Service | Expert threat detection, investigation, and hunting<br>Organizations are increasingly facing stealthy targeted attacks, designed to bypass existing security defenses. These attacks can monetize stolen intellectual property, encrypt essential data for ransom, or damage the flow of information in the case of nation state attacks. Advanced threat detection tools, such as extended detection and response (XDR), are effective methods for identifying and responding to attacker behavior. However, even with the right solution, security teams still struggle with constrained resources. They can gain tremendous value by leveraging a service to augment detection capabilities, add threat expertise/intelligence, and ensure proactive threat hunting and regular sweeping for indicators of compromise (IoC).<br><br>Trend Micro is the only vendor that can use its native security stack to offer an integrated managed service across email, endpoints, servers, cloud workloads, and networks. Our managed detection and response service, Trend Micro™ Managed XDR, drives unparalleled improvements in security teams' time-to-detect and time-to-respond, while minimizing the risks and impact of threats." |
| ZTNA | Forcepoint | Forcepoint ONE Zero Trust Network Access (ZTNA) | Forcepoint ONE Zero Trust Network Access (ZTNA) is one of the three foundational gateways of the Forcepoint ONE cloud platform. It controls access to individual applications hosted behind a firewall, without the need for virtual private networks (VPNs), while providing data loss prevention (DLP) and malware protection for private web-based applications. |
| | Trend Micro | Vision One- Zero Trust Secure Access | As the recent transition to a remote or hybrid workforce has widened the digital attack surface, increasing cyber risk significantly across many organizations, the adage of "trust, but verify" is no longer practical. The growing interest and movement toward zero trust architectures in the past few years has shifted this approach to the more accurate "never trust, always verify." |

| Solution | Brand | Product / Service | Description |
|---|---|---|---|
| | | | And for good reason. The broad implicit-trust methods and practices haven't kept pace with stealthy, more resourceful threat actors. Organizations need to modernize the methods used to securely connect users, devices, and applications no matter where they are or what they need to access.<br><br>Introducing Trend Vision One™ — Zero Trust Secure Access: Secure Access is part of Trend Vision One™. The modern cloud-native platform integrates attack surface risk management (ASRM), extended detection and response (XDR), and Secure Access.<br><br>Through Trend Vision One, organizations can enrich continuous adaptive risk and trust assessment to drive zero-trust architectures that support their business objectives. With Secure Access, no user or device should be inherently trusted.<br><br>In relation to SSE, Secure Access provides secure web gateway (SWG), cloud access security broker (CASB) and zero trust network access to secure access of users and devices across network, web, cloud, and private apps—all in one platform. This strengthens your overall security posture by enforcing strong access control permissions from multiple identity services across the organization. |
| | Zscaler | Zscaler Private Access (ZPA) | ZPA is the world's most deployed ZTNA platform, applying the principle of least privilege to give users secure, direct connectivity to private applications running on-premises or in the public cloud while eliminating unauthorized access and lateral movement. As a cloud native service built on a holistic security service edge (SSE) framework, ZPA can be deployed in a matter of hours to replace legacy VPNs and remote access tools to:<br>• Deliver a superior user experience: Connecting users directly to private apps eliminates slow, costly backhauling over legacy VPNs while continuously monitoring and proactively resolving user experience issues<br>• Minimize the attack surface: Applications are made invisible to the internet preventing unauthorized users and devices from discovering them. The inside-out connections between user and app ensures apps and IPs are never exposed<br>• Enforce least-privileged access: Application access is determined by identity and context— not an IP address—and users are never put on the network for access<br>• Eliminate lateral movement: Applications are segmented so that users can only access a specific app, helping limit lateral movement<br>• Stop cyberattacks with complete inspection: Private app traffic is inspected inline to prevent the most prevalent web attack techniques<br>• Prevent data loss: Integrated DLP for private apps, advanced incident response and data classification to protect crown jewel apps<br>• Detect compromised users and devices: Integrated decoys work to quickly identify and remove malicious users and devices |

| Solution | Brand | Product / Service | Description |
|---|---|---|---|
| IT Managed Service | DCS | ITMS Security Managed Service | Security managed services' responsibilities managed security infrastructure (Monitor, Admin's functional) |
| **Digital Transformation** | | | |
| Application Development | DCS | Application Development | Tailor-Made Software Solution Services<br>We develop systems for customers with various options through Tailor-Made Solutions, which involve system development from the beginning based on the customer's requirements. This is suitable for organizations with their own specific work characteristics that cannot adapt packaged software. The advantage is the flexibility to customize according to the customer's needs.<br><br>We have experts involved in collecting requirements, then analyze and design systems to develop projects successfully. Additionally, we have a support team to provide fast and excellent post-sales services to help organizations smoothly operate their businesses.<br><br>We develop systems using various technologies suitable for the nature of the work, cost considerations, and in line with current technology. This includes Web Application, Native Mobile Application, and APIs, such as .Net, Java, Nodejs, React, Angular, Flutter, Ionic, Swift, and others. |
| Cloud Solution | Amazon | Amazon Web Service | Amazon web service (Public Cloud Service) is an online platform that provides cloud computing solutions and others solution as SaaS. |
| | DCS | DCS Cloud Service<br>Cloud Virtual Server<br>Cloud Computing Service | DCS Cloud Service (Local Cloud Service) is an online platform that provides cloud computing solutions with security environment |
| Digital Process Automation | NICE | NICE RPA | The NICE Virtual workforce comprises software robots that are installed on back-end servers, with the capabilities to take over all the repetitive, admin driven processes facing the human workforce every day. A variety of tasks can be executed independently without human intervention, freeing up employees to focus their attention on more valuable business priorities. RPA is fast becoming the technology of choice across for a wide variety of organizations spanning any vertical market. Enterprises who embrace RPA, across the front office, back office, and shared services divisions, are experiencing dramatic increases in business performance and ROI.<br><br>Unattended Versus Attended Automation<br>• Unattended robots completely free the human employee from performing very tedious tasks.<br>• Attended robots takes place on the employee's desktop, where the attended robots work collaboratively with human employees, for processes that require human intervention.<br><br>The combination of both attended and unattended automations can enable greater process efficiencies. For |

| Solution | Brand | Product / Service | Description |
|---|---|---|---|
| | | | example, there is no need for attended bots process automation to stop when encountering an exception, instead, can step in and seamlessly alert a human to intervene and resolve a process error or complication, in real-time. The automated flow can then resume without any down time. |
| | UiPath | UiPath RPA | Robotic process automation (RPA) is a software technology that makes it easy to build, deploy, and manage software robots that emulate humans' actions interacting with digital systems and software. |
| OCR | N2N Solution Provider | ABBYY | OCR software that allows for the conversion of images of text documents and tables into editable, machine-readable text formats. |
| **Innovative Workplace** | | | |
| Meeting room & Classroom solution | Aver Media | Aver Vision Video Conference | USB video conference peripheral for online meeting, support various size of meeting room |
| | BenQ | BenQ Interactive Display | Interactive display that transforms your meeting room or classroom into collaboration fully support google service EDLA enable user to work seamlessly and protect user health with germ resistant screen |
| | | BenQ Conference Camera | BenQ conference camera to support online meeting |
| | | BenQ DLP Laser Projector | DLP Laser projector for meeting room, quick turn on & off with high durability. |
| | Elmo | Elmo Visualizer | Document camera for presentations or meetings ideal for office and classroom |
| | Epson | Epson LCD Laser Projector | Trusted projector for your business, from education solutions to conference room projectors. After sales service by DCS professional technician |
| | Grandview | Grandview Projection Screen | High quality projector screen available from 100" - 300" suitable for different size of room |
| | Hikvision | Hikvision LED | Global LED display available for both indoor & outdoor in any use case scenario |
| | LG | LG LCD/LED/Plasma TV & Monitor | Professional display for digital signage and meeting room available with various size suitable for any meeting room |
| | Newline | Newline Interactive Display | Interactive display from USA, with no.1 market share, available from 65" - 98" inches support wireless screen sharing, whiteboarding, support online meeting application such as Zoom, MS Team and google meet. |
| | Panasonic | DLP Laser Projector | World leading DLP projector empowered by laser technology to ensure business continuity suitable for large auditorium hall and immersive mapping event |
| | | LCD Laser Projector | Mid to high brightness LCD laser projector for meeting room, classroom, and auditorium |

| Solution | Brand | Product / Service | Description |
|---|---|---|---|
| | Razr | Razr Projection Screen | Projector screen for fix installation and portable |
| | ScreenBeam (Barbados) Inc. | ScreenBeam | Easy to use wireless presentation solution support all OS and device, windows, android, iOS, MacOS, no need to install any application and don't require USB dongle, mostly use in business meeting room and classroom |
| | Vertex | Vertex Projection Screen | Projector screen for fix installation and portable |
| | Zoom | Zoom one | Solution from Zoom that transform your office into smart workplace fully support hybrid working with zoom online meeting and zoom workspace to utilize office space with more efficiency |
| **IT Infrastructure** | | | |
| Active Directory | Microsoft | Microsoft Windows Server | Active Directory (AD) is a directory service created by Microsoft for Windows domain networks. It's a set of services and database that connects users to network resources. Active Directory stores information about user accounts, such as names, passwords, phone numbers, and so on, and enables other authorized users on the same network to access this information. |
| Backup & Recovery | Commvault | Commvault Backup and recovery | Commvault Backup and Recovery provides powerful backup, verifiable recovery, helping to ensure data availability. Our simplified backup and recovery solution allows you to manage all your workloads - cloud, VMs, containers, applications, databases, and endpoints from a single platform, while flexible copy data management allows you to backed-up data for DevOps, replication, and more, across your entire infrastructure. |
| | IBM | IBM Spectrum Protect | IBM Spectrum Protect is the next generation of IBM Tivoli Storage Manager (TSM). IBM Spectrum Protect provides centralized, automated data protection that helps to reduce data loss and manage compliance with data retention and availability requirements. The data protection solutions that IBM Spectrum Protect provides consist of a server, client systems and applications, and storage media. IBM Spectrum Protect provides management interfaces for monitoring and reporting the data protection status. |
| | Veeam | Veeam Data Platform | Veeam is a software that provides data protection, backup, and disaster recovery solutions. Veeam Backup & Replication is a data protection solution that provides backup and recovery for virtual, physical, NAS, and cloud-native environments. It offers security for critical business data. |
| | Veritas | Veritas Backup Exec | Veritas Backup Exec is a data protection software product that protects business-critical data from being lost, stolen, or corrupted. It's designed for customers with mixed physical and virtual environments, and who are moving to public cloud services. |

| Solution | Brand | Product / Service | Description |
|---|---|---|---|
| | | Veritas Desktop and Laptop Option | Veritas Desktop and Laptop Option (DLO) is a backup solution that protects Windows and Mac machines. It offers automated file protection for desktops and laptops, whether they are connected to a network or offline. DLO is intended to provide file-level protection for desktop user data, not a full system backup. |
| | | Veritas NetBackup | NetBackup is a complete and flexible data protection solution for a variety of platforms. NetBackup combines data management, automation, artificial intelligence, and elastic architecture to improve agility and data security. NetBackup Resiliency Platform is a solution that protects workloads in the cloud or on-premises. It offers a unified approach for visibility and control of IT service continuity for applications, virtual machines, and complex, multi-tier business services. |
| | | Veritas System Recovery | Veritas System Recovery is a backup and disaster recovery solution for servers, desktops, and laptops. It can quickly restore physical and virtual systems, even to different hardware, remote locations, or virtual environments. |
| Cabling Systems | DCS | UTP, Fiber Optic Cabling Systems and Rack Enclosures | Cabling Systems is the important foundation for Information and Communication Technology (ICT). Our services cover the design, installation, consulting, maintenance, as well as the distribution of products.<br><br>Wired network system LAN cabling services including site survey services system design, installation so that every computer and peripheral device can connect to the internet smoothly without interruption.<br>- UTP Cabling<br>- Fiber Optic |
| Container Platform | Broadcom | VMWare Tanzu | VMware Tanzu is a modular, cloud native application platform that enables development and operations teams to deliver business value faster and more securely to any cloud and manage apps at scale across clouds. Using VMware Tanzu, customer can reduce the complexity of building, delivering, and operating cloud native apps in a multi-cloud world |
| | RedHat | Red Hat OpenShift | Red Hat OpenShift, the industry's leading hybrid cloud application platform powered by Kubernetes, brings together tested and trusted services to reduce the friction of developing, modernizing, deploying, running, and managing applications. OpenShift delivers a consistent experience across public cloud, on-premise, hybrid cloud, or edge architecture. |
| Data Archiving | Veritas | Veritas Enterprise Vault | Veritas Enterprise Vault is a solution for automated data retention that can be used on-premise or in the cloud. It can capture information from all communication platforms and migrate it to the cloud. It can also automatically identify relevant content to ensure compliance.<br><br>Archiving is the process of storing inactive information securely for long periods of time. This information may or may not be used again in the future, but it should be stored until the end of its retention schedule. |

| Solution | Brand | Product / Service | Description |
|---|---|---|---|
| Data Center Monitoring | Delta | Delta Environment Monitoring Systems | EnviroProbe monitors temperature, humidity in a single cabinet or area and transmits signals from environment sensor devices in the data center— such as door sensors, smoke detectors, fire detectors, water-leakage detectors, and others—to management. |
| | Schneider | NetBotz Environment Monitoring Systems | Explore physical threat monitoring solutions from network closets to data centers. |
| Data Center Solution | Delta | Delta Cooling System | The most reliable and efficient cooling solutions In order to offer the best possible space utilization, and to accommodate the potentially rapid expansion of new IT equipment, modern data centers have implemented a high-density model, based primarily on blade server technology. This model requires a higher power supply density and can thereby create more significant problems with heat dissipation. To address these issues, round-the-clock air conditioning is sometimes deployed as a cooling system solution. |
| | | Delta Rack & Accessories | The Delta InfraSuite modular server rack is a simple parallel rack design with a refined and solid exterior that maintains a uniform appearance for the data center. Set-up and maintenance could not be simpler, thanks to tool-less installation. |
| | | Delta UPS- Uninterruptible Power Supplies | Industry-leading energy efficient power solutions with its wide range of Uninterruptible Power Supplies (UPS), Delta offers a competitive edge to businesses in need of first-rate power solutions. |
| | Schneider | APC Rack & Accessories | "Schneider Electric, our Data Center Physical Infrastructure options provide a strong, secure framework that is able to grow and adjust with your needs. Data Center Infrastructure Management software (DCIM) is installed, and your data center is operational, you can collect and analyze data, and control power and processes system-wide or on individual devices.<br><br>APC rack systems offer standard and custom full, half and wall rack enclosures designed to house critical IT infrastructure in IT. The rack systems are built to last, are highly secure and simple to configure.<br><br>UPSs deliver highly efficient, simple-to-deploy, compact 3-phase UPS power protection. With innovative eConversion mode, Li-ion options and a range of 10 kW to 1500 kW.<br><br>The modular cooling solutions includes room and InRow air conditioners, air handlers and chillers. Designed to be easy to maintain, efficient and to maximize ROI they deliver precise temperature and humidity control for critical IT and Infrastructure environments." |
| | | APC UPS Systems | Discover power availability and management for entry-level to high-performance servers, storage and business networking systems. |
| | | Micro Data Centers | Complete IT infrastructure within a stand-alone, secure enclosure for protection of critical business applications. |

| Solution | Brand | Product / Service | Description |
|---|---|---|---|
| | | | Include: power distribution, UPS, and environmental monitoring |
| | | NetShelter SX Enclosures | Feature-rich rack enclosure optimized for easy installation, managing cables, integrating power distribution, and maximizing airflow. |
| | | Uniflair Cooling System | The Uniflair Cooling solutions by Schneider Electric are designed for precision and efficiency in cooling data centers and critical IT environments. These solutions range from room cooling for small IT spaces to large data center cooling systems, focusing on sustainability and energy efficiency. Uniflair products include precision air conditioners, chillers, and modular cooling units, tailored to meet the specific needs of various installations. |
| Data Replication | Oracle | Data Guard | Oracle Data Guard is a feature of the Oracle database that provides data protection and disaster recovery. It ensures high availability, data protection, and disaster recovery for enterprise data. Oracle Data Guard maintains one or more standby databases that are synchronized with the primary database. These standby databases are transactionally consistent copies of the production database. |
| | | GoldenGate | Oracle GoldenGate is a software product that allows users to replicate, filter, and transform data from one database to another. It is a tool for capturing and replicating real-time change data. Oracle GoldenGate is used for data integration, high availability, and online migrations.<br><br>Oracle GoldenGate supports an active-active replication mode, which allows both systems to work simultaneously while maintaining data integrity. |
| | Precisely | Assure MIMIX | Assure MIMIX is the leader in IBM i high availability (HA) and disaster recovery (DR). It provides full-featured, scalable real-time replication with extensive options for automating administration, comprehensive monitoring and alerting, customizable switch automation, and an easy graphical interface.<br><br>Assure MIMIX leverages IBM's Remote Journaling technology to ensure fast, efficient, and accurate replication between any combination of IBM i servers or storage hardware, even when they are running different versions of iOS. It also takes the hard work and complexity out of setting up and managing replication using exclusive, flexible, and highly automated Journal Centric Data Group technology. Journal-centric replication intelligently monitors and responds to changes in journaling for system objects and data, as well as configures and starts replication for newly created journals.<br><br>The Assure MIMIX HA solution has helped reduce downtime and has improved our response to branches and customers. Assure MIMIX has helped us maximize customer satisfaction by ensuring the continuous availability of systems responsible for their transactions. |

| Solution | Brand | Product / Service | Description |
|---|---|---|---|
| DNS DHCP and IPAM | Infoblox | BloxOne DDI | Infoblox, the industry leader in DNS, DHCP, and IP address management (DDI), is the first to market with a cloud-managed solution for these critical network services. BloxOne DDI centralizes the provisioning, management, and administration of DDI for enterprises with distributed environments.<br><br>Mobile, IoT, and cloud solutions are highly sensitive to latency and heavily depend on reliable DDI infrastructures. BloxOne DDI consolidates the visibility, administration, and control of distributed locations into a single interface, directs traffic to the closest SaaS entry point to improve application performance, and ensures the survivability of distributed locations in the event of lost connections to data centers.<br><br>BloxOne DDI also utilizes DNS server group and access control list (ACL) templates and leverages an extensible microservices and container-based platform to simplify deployments, streamline operations, and minimize overall total cost of ownership. A full complement of APIs is also available for secure, programmatic access to supported features throughout the solution. |
| Email | Microsoft | Microsoft Exchange | Microsoft Exchange Server is Microsoft's email, calendaring, contact, scheduling, and collaboration platform. Microsoft Exchange is a highly scalable solution that can support a huge number of users. It's designed from the ground up to keep email in sync between the server and end-user clients. |
| High Availability | HPE | HPE Serviceguard | HPE Serviceguard is a high availability (HA) and disaster recovery (DR) clustering solution that increases uptime for your critical applications by protecting them from a application faults across physical or virtual environments over any distance. |
| | IBM | IBM PowerHA | IBM PowerHA is IBM's solution for high-availability clusters on the AIX Unix, IBM i and Linux. IBM PowerHA provides end-to-end integrated clustering solutions for high availability (HA) and disaster recovery (DR) with one integrated configuration, with a simplified user interface. |
| | Oracle | Oracle RAC | Oracle Real Application Clusters (RAC) is a solution for distributing databases across multiple nodes. It allows customers to run a single Oracle Database across multiple servers. Oracle RAC enables organizations to enhance availability and scalability by providing fault tolerance and load balancing, while also improving performance. |
| | Veritas | Veritas InfoScale | Veritas InfoScale is a software-defined infrastructure solution that provides high availability and disaster recovery. InfoScale Availability utilizes intelligent monitoring to identify risks to availability and automatically recovers applications as needed. It also detects site outages and initiates application recovery at a disaster recovery site. |
| IT Automation | Red Hat | Red Hat Ansible | Red Hat Ansible Automation Platform is an enterprise IT automation solution that helps with configuring systems, deploying software, and managing workflows. It can be used |

| Solution | Brand | Product / Service | Description |
|---|---|---|---|
| | | | across multiple IT domains, including networking, security, operations, and development. |
| Load Balancer | F5 | F5 NGINX | As enterprises adopt a DevOps approach to application development and delivery, the tools, stack, and interoperability of it all can become very complex. F5 NGINX solutions help reduce this complexity by consolidating standard functions into fewer components, making application infrastructure more scalable and manageable. |
| Log Management | SolarWinds | SolarWinds Log Analyzer | SolarWinds Log Analyzer is a powerful log management and analysis tool designed to fully integrate with the Orion Platform and provide users with a mechanism to realize the potential of their log data. With real-time log collection, analysis, and visualization, you can gain out-of-the-box visibility into the performance and availability of your IT infrastructure and applications.<br>• Easily view log data alongside network and systems performance to speed full context troubleshooting with full integration of log and event data into the Orion Platform console.<br>• Use the Orion intelligent alert engine to build customizable alerts in a single pane of glass, define notification criteria, trigger external scripts, and integrate with helpdesk ticketing systems.<br>• Collect, consolidate, and analyze network, systems, Windows, and VMware events alongside availability and performance data from SolarWinds Network Performance Monitor, NetFlow Traffic Analyzer, Server & Application Monitor, and Virtualization Manager. |
| Remote Support | BeyondTrust | BeyondTrust Remote Support | BeyondTrust's Remote Support solution allows help desk teams to securely access and fix any remote device on any platform with a single solution. It supports both attended and unattended remote support, has robust built-in security features, and unlocks powerful synergies through key service desk integrations. Additionally, it provides complete visibility and control over internal and external resources. |
| Resource Management | IBM | Turbonomic | Turbonomic is a performance and cost optimization platform for public, private, and hybrid clouds. It's used by cloud, infrastructure operations, and architecture to ensure application performance.<br><br>Turbonomic uses artificial intelligence technology to manage resources in an application-based and dynamic manner. It simulates supply and demand forces to efficiently allocate resources such as computing, database, memory, and storage. |
| SD-Access | Cisco | Cisco DNA | Software-Defined Networking (SDN) is a technology for automating network control and management, which is a great help to improve and automate network deployment and services. To implement SDN on an enterprise network, we need a controller to manage dynamic controls on the network devices. Cisco released a powerful controller to centralize the network management and control using a Cisco DNA Center dashboard.<br><br>Cisco DNA Center (also called Cisco Digital Network |

| Solution | Brand | Product / Service | Description |
|---|---|---|---|
| | | | Architecture) is a powerful SDN controller and management dashboard that allows you to take control of your network, optimize your network, secure your remote workforce, and lower your IT spending. It is used as a management platform for both SD Access, Intent-Based Networks (IBN) and existing traditional networks. Cisco DNA Center is the recent Network Management Platform of Cisco for Enterprise Networks.<br><br>IBN is the latest SDN technology that allows all manual and hardware-related tasks and operations to be designed into a fully automated or software-based system. It transforms a traditional manual network into a controller-based network that translates the business needs into policies that can be automated and enforced consistently throughout the network. Cisco DNA center uses the technology of Intent-Based Networking.<br><br>With its efficient dashboard, Cisco DNA Center is very easy to use for network engineers. With reusable templates, efficient workflows, policies etc. It simplifies network operations, configurations and troubleshooting. With DNA Center, your network feels Network Automation convenience. Your network is managed easily, network operations are done efficiently and your network down times decrease.<br><br>DNA Center uses recent technologies like Artificial Intelligence (AI), Machine Learning (ML) for this new type of network management. With these systems, network management become more proactive, network operations are more effective and troubleshooting activities are faster. |
| SD-Data Center | Broadcom | VMWare Cloud Foundation | VMware Cloud Foundation is the next generation VMware hybrid cloud platform by extending the core hypervisor with integrated software-defined storage, networking and security capabilities that can be consumed flexibly on premises or as a service in the public cloud. With the integrated cloud management capabilities, the end result is a hybrid cloud platform than can span private and public environments, offering a consistent operational model based on well-known vSphere tools and processes. |
| | | VMWare vSphere Foundation | VMware's core virtualization stack that adds the power of the enterprise platform with integrated management and analytics. Accelerate Innovation for DevOps, customer can deploy DevOps services to run workloads with VMs and containers. |
| | Cisco | Cisco ACI | Cisco Application Centric Infrastructure (ACI) is a software-defined networking (SDN) solution designed for data centers. Cisco ACI allows network infrastructure to be defined based upon network policies – simplifying, optimizing, and accelerating the application deployment lifecycle. To make this possible Cisco has created the ACI Fabric OS, which is run by all systems within the ACI network. This shared OS makes it possible for the various switches within the ACI network to translate policies into infrastructure designs.<br><br>A Cisco ACI environment is built with two main components: |

| Solution | Brand | Product / Service | Description |
|---|---|---|---|
| | | | • Cisco Application Policy Infrastructure Controller (APIC): APIC is the SDN controller for Cisco ACI. It creates the policies that define the data center's network infrastructure.<br>• Nexus 9000 Switches: Nexus 9000 switches use the ACI Fabric OS to communicate with APIC and create infrastructure based on policies. They can be either Spine (distribution) or Leaf (access) switches. All endpoints, including APICs, connect to the network via Leaf switches. These Leaf switches are connected using Spine switches in the backend.<br>• Using these components, ACI can be deployed under a variety of different models. This includes support for on-site, cloud-based (including public, private, and hybrid clouds), and SD-WAN edge environments. This enables organizations to use policy-based network management throughout their corporate WANs.<br><br>Key Features and Benefits of ACI : Cisco ACI enables organizations to easily create a software-defined data center, which provides several benefits, including:<br><br>• Flexibility: With a SDN solution like Cisco ACI, all of an organization's network infrastructure is implemented as code. This makes it easy to update configurations to meet evolving business needs.<br>• Consistent Infrastructure: Cisco ACI abstracts away the details of the underlying infrastructure. This makes it easier to design and configure network environments.<br>• Automation and Orchestration: Cisco ACI makes heavy use of automation to develop network infrastructure based on network policies. This makes changes easy to make and increases scalability.<br>• Support for Hybrid Environments: Cisco ACI supports both on-prem and cloud-based infrastructure, making it possible to deploy ACI environments across multiple different environments. |
| SD-Storage | IBM | IBM Spectrum Scale | IBM Storage Scale is software-defined file, object storage and clustered filesystem for AI and data intensive workloads creating a high performance, globally connected, cost-optimized and enterprise-resilient information supply chain and global data platform. |
| SD-WAN | Broadcom | VeloCloud | Cloud-delivered Software-defined WAN from VeloCloud assures enterprise and cloud application performance over Internet and hybrid WAN while simplifying deployments and reducing costs. |
| | Cisco | Cisco Catalyst SD-WAN | Catalyst SD-WAN's secure architecture has evolved to meet these changing security paradigms by providing a scalable and secure solution that can protect your network from anywhere. Catalyst SD-WAN offers engineering leadership in both networking and security, including full-stack multilayer security capabilities on the premises and in the cloud. The integrated security arms IT with advanced threat defense where and when it is needed — for branches connecting to |

| Solution | Brand | Product / Service | Description |
|---|---|---|---|
| | | | multiple Software-as-a-Service (SaaS) or Infrastructure-as-a-Service (IaaS) clouds, to data centers, or to everything on the internet — and accelerates the transition to a Secure Access Service Edge (SASE) architecture in a secure and agile manner.<br><br>Secure direct internet access<br>Catalyst SD-WAN security delivers full protection and control against all major web attacks arising from SaaS and internet access. The integrated security solutions provide the best balance of security and user experience for direct internet access.<br><br>End-to-end micro segmentation and identity-based policy management, at scale Catalyst SD-WAN enables you to extend micro segmentation and identity-based policy management across Cisco Software-Defined Access (SD-Access) and non-SD-Access branches, driving consistent multidomain policy enforcement, all from a single pane of glass.<br><br>Branch security<br>Catalyst SD-WAN provides constant protection against all cyberthreats, from branches to multicloud SaaS environments. It also meets comprehensive data compliance requirements in every major industry sector, including highly regulated industries such as financial services, healthcare, utilities, and government.<br><br>Application performance optimization<br>Design a global network where critical enterprise applications always maintain the highest service-level agreements (SLAs) and optimal performance, even if problems occur in the network.<br><br>Multicloud access<br>Connect branches and a remote workforce to multicloud applications seamlessly with unified visibility and management.<br><br>Enforce regulatory compliance<br>Catalyst SD-WAN addresses compliance in a holistic way by offering a comprehensive set of security controls. |
| | | Meraki SD-WAN | Meraki MX appliances are natively part of a unified SD-branch cloud platform that removes complexity and maximizes security protection with automatic software updates capable of reaching every customer site globally in a matter of hours. The Meraki SD-WAN implementation is comprised of several key features, built atop our AutoVPN technology.<br><br>Dual-Active VPN Uplinks:<br>Prior to the SD-WAN release, Auto VPN tunnels would only form only over a single interface. With the SD-WAN release, it is now possible to form concurrent AutoVPN tunnels over both Internet interfaces of the WAN Appliance.<br><br>The ability to form and send traffic over VPN tunnels on both interfaces significantly increases the flexibility of traffic path and routing decisions in AutoVPN deployments. In addition to providing administrators with the ability to load balance VPN traffic across multiple links, it also allows them to leverage the |

| Solution | Brand | Product / Service | Description |
|---|---|---|---|
| | | | additional path to the datacenter in a variety of ways using the built-in Policy-based Routing and dynamic path selection capabilities of the WAN Appliance.<br><br>**Policy-Based Routing (PbR):** Policy-based Routing allows an administrator to configure preferred VPN paths for different traffic flows based on their source and destination IPs and ports.<br><br>**Dynamic Path Selection:** Dynamic path selection allows a network administrator to configure performance criteria for different types of traffic. Path decisions are then made on a per-flow basis based on which of the available VPN tunnels meet these criteria, determined by using packet loss, latency, and jitter metrics that are automatically gathered by the WAN Appliance.<br><br>**Performance Probes:** Performance-based decisions rely on an accurate and consistent stream of information about current WAN conditions to ensure that the optimal path is used for each traffic flow. This information is collected via the use of performance probes.<br><br>The performance probe is a small payload (approximately 100 bytes) of UDP data sent by spokes to hubs or by hubs to other hubs over all established AutoVPN tunnels every 1 second. WAN Appliances track the rate of successful responses and the time that elapses before receiving a response. This data allows the WAN Appliance to determine the packet loss, latency, and jitter over each AutoVPN tunnel to make the necessary performance-based decisions. |
| | HPE | Aruba Edge Connect | The EdgeConnect SD-WAN platform secures and powers a self-driving wide area network for cloud-first enterprises. EdgeConnect SD-WAN provides a secure network foundation for Zero Trust and SASE. It includes a first-class SD-WAN paired with a next-generation firewall delivering unmatched quality of experience and advanced security.<br><br>**Unified SASE**<br>EdgeConnect SD-WAN tightly integrates with HPE Aruba Networking SSE to form a unified SASE platform and meet the security requirements of today's digital organizations.<br><br>**Designed for cloud-first organizations**<br>Increase SaaS application performance and enforce security policies with intelligent traffic steering to the cloud and real-time monitoring of network. Deploy EdgeConnect in leading cloud providers and exchanges such as AWS, Azure, Google Cloud, and Equinix.<br><br>**Network and security simplification**<br>EdgeConnect SD-WAN provides comprehensive security services including next-generation firewall, fine-grained segmentation, IDS/IPS as well as routing, and WAN Optimization capabilities—enabling you to consolidate branch network and security functions by eliminating legacy firewalls and routers in branches. |

| Solution | Brand | Product / Service | Description |
|---|---|---|---|
| | | | **Highest quality of experience**<br>Experience consistent application performance including high quality voice and video over broadband connections. Real-time monitoring, continuous adaptation, and automated response assure the highest performance and availability, whether applications reside in the data center or the cloud.<br><br>**Easily add primary/backup high speed LTE Links**<br>By using a plug-and-play HPE Aruba Networking USB LTE modem with EdgeConnect SD-WAN, enterprises can fully manage their LTE equipment through Aruba Orchestrator, while ensuring optimal connections to critical applications and resources, even if primary connections fail or become unreliable. |
| Virtualization | Broadcom | VMWare vSphere Essential Plus | VMware vSphere Essentials Plus are designed for small businesses that are getting started with virtualization. by providing virtualization and centralized management for up to three server hosts. Customer can ensure business continuity by using features such as vSphere High Availability (automatic restart of applications when server failures are detected) and vSphere vMotion® (elimination of planned downtime during server maintenance) |
| | | VMWare vSphere Standard | Industry leading server virtualization solution for data center consolidation and enhanced application availability. |
| | Microsoft | Microsoft Hyper V | Hyper-V is a virtualization product from Microsoft that allows users to create and run virtual machines (VMs) on a physical host. Hyper-V is a hypervisor, which is a virtualization platform that allows administrators to run multiple operating systems simultaneously on the same physical server.<br><br>In general, an operating system that uses an x86 architecture will run on a Hyper-V virtual machine. |
| | Proxmox | Proxmox VE | Proxmox VE is a server virtualization platform that combines the powerful KVM hypervisor and LXC containers with integrated software-defined storage and networking capabilities, enabling enterprise-grade performance and flexibility. Designed for modern data centers, allowing IT teams to efficiently orchestrate virtual machines, containers, storage, and network configurations. With built-in backup tools, high availability clustering, and integrated firewall and security.<br><br>Proxmox VE delivers a unified platform for private cloud deployments, offering a consistent and streamlined operational model for both small businesses and large enterprises. |
| **IT Managed Service** | | | |
| DR Managed Service | DCS | DR Support Service | Provide service to recover IT infrastructure environment at DR site |
| | | DR Managed Service | |

| Solution | Brand | Product / Service | Description |
|---|---|---|---|
| IT Call Center Service | DCS | ITMS IT Call Center | Provide a single point of contact to handle queries, incidents, or requests for IT services from end user |
| IT Managed Service | DCS | IT Consulting Service | Provide IT process consulting (review, analysts, and recommend the customer IT processes) |
| | | ITMS System Operation Service | System Operation Service is focusing on the operational of IT system which task defined with customer |
| | | ITMS System Managed Service | System managed services' responsibilities managed system infrastructure and operation system (Monitor, Admin's functional) |
| | | ITMS Security Managed Service | Security managed services' responsibilities managed security infrastructure (Monitor, Admin's functional) |
| | | ITMS Network Managed Service | Network managed services' responsibilities managed network infrastructure (Monitor, Admin's functional) |
| | | ITMS Monitoring Service | Monitoring Service monitors the performance of IT equipment |
| | | ITMS Local Cloud Managed Services | System managed services' responsibilities managed system infrastructure and operation system (Monitor, Admin's functional) |
| | | ITMS Backup Managed Service | Provides managed data backup service as remote administration to manage backup task |
| | | ITMS Administrator Service | Provides an administrative for customer system and services to help administrators to manage administrator tasks |
| ServiceDesk Support Service | DCS | Deskside Support | Provide online end user assistance service with incident determination and incident resolution or fulfill service request |
| | | ITMS Field Support | Provide deskside end user assistance service with incident determination and incident resolution or fulfill service request |
| | | ITMS End user Professional Service | Provide service to implementation end user equipment and solution |
| **IT Service Solution** | | | |
| Data Center Service | DCS | DR Rack Co-location Service | Provide rack space for store customer's own server equipment in data center, with physical monitoring service |
| | | DR Dedicated Room Co-location Service | Provide dedicated room & rack space for store customer's own server equipment in data center |
| | | Data Center Co-location service | Provide rack space for store customer's own server equipment in data center, with physical monitoring service |
| | | Data Center Rack Co-Location Services | Provide rack space for store customer's own server equipment in data center, with physical monitoring service |
| | | Data Center-Dedicated Room Co-location Service | Provide dedicated room & rack space for store customer's own server equipment in data center |

| Solution | Brand | Product / Service | Description |
|---|---|---|---|
| Data Center Solution | BMC | BMC TrueSight Infrastructure Management | TrueSight Automation for monitoring and event management to Detect, analyze, and act on events impacting the business |
| Disaster Recovery | DCS | DRC Hot Site | A disaster recovery hot site is a fully functional backup site, a backup facility that replicates the primary production facility. It includes the software, hardware, and network connectivity as the primary center, and enables real-time backup (data replication) of important data.<br>• Recovery Time Objective (RTO) is near-zero.<br>• Recovery Point Objective (RPO) is near-zero<br><br>Hot-Site summary:<br>- fully redundant equipment<br>- network connectivity is enabled<br>- failover occurs within hours or days<br>- near real-time data synchronization<br>- zero data loss" |
| | | DRC Warm Site | A disaster recovery warm site is to prepare the standby hardware ready to be used, but backup data must be sent to the site to install.<br>• Recovery Time Objective (RTO) can be 24-48 hours or more than depend on the amount of data.<br>• Recovery Point Objective (RPO) is based on the most recent backup available. The data lost may be more than 24 hours.<br><br>Warm-Site summary:<br>- partially redundant equipment<br>- network connectivity is enabled<br>- failover occurs within hours or days<br>- schedule of data synchronization<br>- minimum data loss" |
| | | DRC Cold Site | A disaster recovery cold site is a backup facility with little or no hardware equipment installed. Using a cold site is very limiting to a business since before it can be used, hardware needs to be set up and backup data must be sent to the site to install.<br>• Recovery Time Objective (RTO) can be 48 hours to a week. This is because hardware preparation and data installation are required, which depends on the amount of data.<br>• Recovery Point Objective (RPO) is based on the most recent backup available. The data lost may be more than 24 hours.<br><br>Cold-Site Summary:<br>- little or no equipment<br>- no network connectivity<br>- not ready for automatic failover<br>- no data synchronization<br>- high risk of data loss" |
| | | Office Continuity-Dedicated | We offer dedicated office space to ensure your staff can stay productive while working off site. Enable businesses to continue their normal activities in a disaster situation.<br><br>Office Facilities and equipment are dedicated and prepared to be used for each customer which include: |

| Solution | Brand | Product / Service | Description |
|---|---|---|---|
| | | | - dedicated room (office space)<br>- table and chair<br>- computer and printer<br>- telephone and internet access<br>- etc.<br><br>Computers can be setup and prepared for use, whether it's the OS or application according to the version you want to use. |
| | | Office Continuity-Shared | We offer the office space to ensure your staff can stay productive while working off site. Enable businesses to continue their normal activities in a disaster situation.<br><br>**Office Facilities and equipment are prepared to be used which include:**<br>- room (office space)<br>- table and chair<br>- computer and printer<br>- telephone and internet access<br>- etc.<br><br>Computers require a deployment image before they are ready to use. |
| IT Infrastructure Service | DCS | IT Infrastructure Service | Provide IT Infrastructure environment, which bundle IT managed service together as monthly service fee model |
| | | IT equipment as a Service | Provide IT hardware equipment, which bundle IT managed service together as monthly service fee model |
| | | Shared Infrastructure Service | Provide shared IT Infrastructure environment, which bundle IT managed service together at DCS environment as monthly service fee model |
| IT Operation Management | ServiceNow | ServiceNow ITOM | Software for monitoring and event management to Detect, analyze, and act on events impacting the IT operation |
| IT Service Management | BMC | BMC Helix ITSM | BMC Helix IT Service Management (ITSM) is an ITIL® 4-certified SaaS solution that modernizes and transforms the IT service desk by leveraging intelligence to automate everywhere, reduce risk, and prevent points of failure. |
| | ServiceNow | ServiceNow ITSM | IT Service Management (ITSM) is an ITIL® 4-certified SaaS solution that modernizes and transforms the IT service desk by leveraging intelligence to automate everywhere, reduce risk, and prevent points of failure. |
| IT Service Solution | BMC | BMC TrueSight Infrastructure Management | TrueSight Automation for monitoring and event management to Detect, analyze, and act on events impacting the business |
| | ManageEngine | ManageEngine Patch Software | Patch Management software for managing the process of detecting, downloading, testing, approving and installing new/missing patches for all the Operating Systems, applications and clients |
| | | ManageEngine ITSM Software | IT Service Management (ITSM) software is an ITIL® 4-certified SaaS solution that modernizes and transforms the IT service desk by leveraging intelligence to automate everywhere, reduce risk, and prevent points of failure. |

| Solution | Brand | Product / Service | Description |
|---|---|---|---|
| | Microsoft | MS Office365 | Office 365's cloud-based nature ensures that your business stays at the forefront of technology with automatic updates and cutting-edge security features. Our Microsoft Office 365 services are designed to transform the way businesses operate, fostering a more connected and productive workplace. |
| | | Microsoft SPLA | DCS is at the forefront of facilitating seamless access to Microsoft technologies through comprehensive license subscription services. |
| | | Microsoft SQL | Our Microsoft SQL Server subscription services are designed to provide businesses with cutting-edge database management solutions. By choosing our subscription services, clients gain access to the latest SQL Server capabilities. You will also benefit from expert support for installation, configuration, and optimization of SQL Server environments, maximizing performance and reliability. |
| Mainframe Solution | BMC | BMC Automated Mainframe Intelligence (BMC AMI) | BMC AMI is software to automatically manage, diagnose, heal, and optimize mainframe systems without manual intervention. |
| Workload Orchestration | BMC | BMC Helix Control-M | BMC Helix Control-M is an application to orchestrate data workflow to build, define, schedule, manage and monitor production workflows ensuring visibility, reliability and improving service level agreements. |
| **Media & Broadcasting** | | | |
| Broadcasting Solution | ADT | Aveco Hardware | Broadcast automation platform provide to run on a mission-critical real time operating system |
| | | Vantage Hardware | It's transcoded products for media conversion, the multi-format, multivendor video environments (Video and audio), into the right file format. |
| | | Vantage Software | It's transcoded products for media conversion, the multi-format, multivendor video environments (Video and audio), into the right file format. |
| | DCS | I-Gateway | Digital Advertising Content Delivery & broadcast platform |
| | | Live Broadcast | Broadcast service is the live sessions of the program for training or seminar event |
| | VIZRT | Media Solution | VIZRT offers broadcasters the tools to create captivating and informative content. Their solutions empower producers to deliver high-quality visuals across various platforms. |
| Digital Signage Solution | Dahua | Dahua digital signage | Global brand for digital signage provides easy content management using cloud service, full line up for display from indoor and outdoor with multiple size for customer need. |
| | | Kiosk | Ready to use kiosk with digital signage and built in software to manage content via cloud, available from 55"- 65" inches |

| Solution | Brand | Product / Service | Description |
|---|---|---|---|
| Smart Multimedia | Dicolor | Dicolor LED | One of Global top ten LED supplier with cutting edge technology and advance innovation can provide full line up of LED from indoor to Outdoor |
| | Epson | Epson LCD Laser Projector | Trusted projector for your business, from education solutions to conference room projectors. After sales service by DCS professional technician |
| | Fonestar | Fonestar Audio System | User friendly Audio Solution originate from Spain, offering high-quality speakers, amplifiers, and accessories designed for a versatile range of applications, ensuring clear and immersive sound experiences for everyone, from home entertainment enthusiasts to business professionals. |
| | Panasonic | Panasonic LCD Laser Projector | Mid to high brightness LCD laser projector for meeting room, classroom and auditorium |
| **Middleware** | | | |
| Middle Ware | IBM | WebSphere MQ | **Make every message count.**<br>Connect applications and microservices in private data centers, across hybrid or multicloud environments, and at the edge of your enterprise.<br><br>Tap into the value of your existing mission-critical data to gain near-real-time insights. Only IBM® MQ protects your business from incorrect data and application errors with exactly-once message delivery. |
| | Oracle | WebLogic | Oracle WebLogic Server is a unified and extensible platform for developing, deploying and running enterprise applications, such as Java, for on-premises and in the cloud. WebLogic Server offers a robust, mature, and scalable implementation of Java Enterprise Edition (EE) and Jakarta EE. |
| | Red Hat | Red Hat JBoss EAP | Red Hat® JBoss® Enterprise Application Platform (JBoss EAP) delivers enterprise-grade security, performance, and scalability in any environment. Whether on-premises; virtual; or in private, public, or hybrid clouds, JBoss EAP can help you deliver apps faster, everywhere. |
| **Monitoring/Observability** | | | |
| Application Performance Monitoring | Cisco | Cisco ThousandEyes | ThousandEyes is a software-as-a-service (SaaS) product that uses synthetic monitoring probes to measure network and application performance. A combination of active and passive monitoring techniques plus real-time internet outage detection gives deep insight into user experience across the applications and services you deliver and consume.<br><br>The product includes elements of network and application tomography for loss and latency, route analytics to visualize BGP advertisements, DNS monitoring, VoIP monitoring, website monitoring for HTTP and HTTPS and SNMP device polling.<br><br>Explore the platform |

| Solution | Brand | Product / Service | Description |
|---|---|---|---|
| | | | Network & Application Synthetics: See hop-by-hop and layer-by-layer across your entire digital supply chain, so you can deliver a high-performance network and reliable application experience.<br>• Path Visualization<br>• BGP Monitoring<br>• DNS Performance<br>• Web Performance<br>Internet Insights: Stay on top of the Internet and application outages as they happen so you can react quickly to protect your users' digital experience.<br>• Collective Intelligence<br>• Network Outages<br>• Application Outages<br>• Internet Monitoring<br><br>End User Monitoring: Gain on-demand and real-time visibility into each employee's experience of SaaS and internally hosted applications to instantly identify issues that are hindering their productivity.<br>• Browser-based RUM<br>• Network Synthetics<br>• Wireless Networks<br>• Automated Session Tests<br><br>WAN Insights: ITOps teams can greatly benefit from the preventative approach of WAN Insights by lessening the need to react and instead leverage ThousandEyes to enable customers to proactively prevent bigger problems from developing across their networks.<br>• Forecast-based Recommendations<br>• Proactive SD-WAN Monitoring<br>• Easy App Onboarding<br>• Continuous Assurance |
| | IBM | Instana | IBM Instana Observability is a fully automated application performance management (APM) solution designed for the challenges of managing microservice and cloud-native applications. Instana automatically makes your applications and services visible, provides context to that observed information, and then enables you to take intelligent action based on that information. Instana monitors and analyzes your applications, services, infrastructure, and more for over 200 domain-specific technologies. In addition, Instana displays real-time data through distributed tracing and 1-second metrics. |
| | SolarWinds | SolarWinds Observability | A SaaS offering built to extend visibility across the cloud-native, on-prem, and hybrid technology stack, enabling DevOps, IT ops, and Cloud Ops teams to spend more time developing new modern applications and infrastructures, fuel innovation while continuing to meet SLAs, and exceed customer expectations in legacy on-prem and hybrid IT via a single, unified offering.<br><br>Application observability<br>Comprehensive application observability for both internally written and commercial applications, to go beyond basic metrics, traces, and logs offerings. It combines application |

| Solution | Brand | Product / Service | Description |
|---|---|---|---|
| | | | performance metrics with distributed tracing and leverages log monitoring capabilities along with AIOps-driven notifications—and supports cloud-native open-source frameworks and third-party integrations. Application observability helps ensure the availability and performance of cloud-native custom applications and microservices while also observing your commercially acquired packaged applications and databases.<br>**Infrastructure Observability** helps ensure the health and performance of on-premises, and cloud-based resources, including physical servers, VMs, hosts, containers, serverless, and cloud service providers. Integration with AI-powered analytics and application and log observability combine to deliver context-rich intelligence to help you proactively identify and resolve performance issues.<br><br>**Log observability** provides scalable, full-stack, multi-source log management, combining wide support, powerful search, AI-driven analytics, and built-in integration with application and infrastructure observability to deliver context-rich intelligence to help teams troubleshoot smarter and faster.<br><br>**Database observability** provides deep performance monitoring to diagnose and analyze issues, using sophisticated root cause analysis. Get comprehensive visibility into your database instances to help increase system performance and team efficiency while helping ensure infrastructure cost savings.<br><br>ML-based AIOps and health scores based on golden metrics quickly highlight issues. Get full-stack observability by correlating database metrics with the application performance, distributed tracing, and log monitoring capabilities of SolarWinds Observability.<br><br>**Database observability** simplifies the complexity of managing multi-vendor environments by providing support for databases such as MySQL, PostgreSQL, Microsoft SQL Server, AWS Aurora (PostgreSQL, MySQL), AWS RDS (PostgreSQL, MySQL), MongoDB, MongoDB Atlas, and Redis<br><br>**Digital experience observability** enables DevOps teams to optimize web application customer experience. Granular, real-time performance data, combined with AI-powered analytics, delivers deep insights into application performance impacts on the end user experience. Armed with this intelligence, DevOps and IT ops teams can experience the application the way the customer does—and make better design and implementation choices.<br><br>**Network observability** helps enable troubleshooting of the availability, health, and performance of on-premises networks and end-to-end connections to public cloud networks through the collection and analysis of diverse network metrics and logs. With network observability, organizations can more easily understand and visualize the overall picture of how the network is impacting the services and experiences depending on it. |

| Solution | Brand | Product / Service | Description |
|---|---|---|---|
| Infrastructure Monitoring | Cisco | Cisco Nexus Dashboard | Cisco Nexus Dashboard is a single-pane-of-glass console that streamlines data center network operations and management.<br><br>Cisco Nexus Dashboard Services<br>Cisco Nexus Dashboard Orchestrator, Cisco Nexus Dashboard Insights, and Cisco Nexus Dashboard Fabric Controller services are being integrated into the Cisco Nexus Dashboard as native services as part of simplifying the overall consumption experience for our customers.<br>• Cisco Nexus Dashboard Orchestrator allows operators to easily interconnect fabrics and/or clouds over any routed network, facilitating datacenter and cloud migrations, as well as network extension across fabrics. Organizations can also centralize network and policy configurations and set up connectivity at a scale. Besides rendering configurations defined in the template(s) to the local data center or cloud controller, it enables separation of fault domains, federation of datacenter and cloud networks, and business resiliency at a global scale. Nexus Dashboard Orchestrator also enables end-to-end change-management workflows, centralized fabric management and upgrades, multi-cloud/hybrid-cloud connectivity, normalized segmentation, and security policies across the data center, SD-WAN, and enterprise branch and campus networks.<br>• Cisco Nexus Dashboard Insights allows operators to minimize downtime by turning hardware and software telemetry (including anomalies and advisories) into insights to identify potential issues and recommendations to fix them, gathering years of experience under a single network-operations platform. It can also take advantage of its analytics to learn more about sustainability, compliance, changes, and traffic behavior (including flow records, drop, congestion, latency, AI/ML RoCEv2, and more). It also minimizes risk by providing pre- and post-upgrade assistance and can enhance visibility by integrating tools from vendors such as VMware, Splunk, ServiceNow, Panduit, Vertiv, and many more. It incorporates a set of advanced alerting, baselining, correlation, and forecasting algorithms to provide a deep understanding into the behavior of the network. The Insights service and AppDynamics are tightly integrated to pinpoint exactly where and when an application issue originated from a network perspective.<br>• Cisco Nexus Dashboard Fabric Controller (NDFC) consolidates management for multiple NX-OS-based switches, bringing automation and monitoring for LAN, EVPN VXLAN, and SAN fabrics. Simply choose an operational mode (LAN, SAN), discover new and/or existing switches, and leverage the benefits of Zero-Touch Provisioning (ZTP), fabric monitoring, backup, faster provisioning and upgrades, and much more. NDFC supports Cisco (including Nexus, Catalyst®, and ASR routers) and third-party devices. |
| | Netka Systems | NetkaView Network Manager | A network management solution designed specifically for large and complex networks. Its main goal is to ensure that the network performs at its best and is always available for use. It |

| Solution | Brand | Product / Service | Description |
|---|---|---|---|
| | | | offers a wide range of features to achieve this. It also provides intuitive dashboards and reports that make troubleshooting and decision-making quicker and easier. Furthermore, it can seamlessly integrate with various systems, vendors, and technologies.<br><br>Revolutionize Your IT Infrastructure Operations for Efficiency, Proactivity, and Availability<br>NetkaView Network Manager (NNM) is designed and developed to support the 4 pillars of IT infrastructure operations including planning, provisioning, monitoring, and analytics. NNM is the ultimate tool to help you for building IT infrastructure, configuring devices, monitoring fault and performance, logging events and alarms, accounting traffic and usage, discovering and recording inventory, alerting for incident or degradation, and providing ton of reports. It's the perfect tool for traffic engineering to continually improve your network performance for the best customer experience in digital era.<br>• Real-time monitoring resources and provide insight into your IT infrastructure with rich interactive data visualizations e.g., network diagram, weather map and dashboards.<br>• Single pane of view for your IT which comes with hundreds of out-of-the-box reports. Help you to troubleshoot your IT incidents faster than ever.<br>• Detect and proactively alert before interruption. Ensure your IT infrastructure is reliable for all business processes.<br>• Friendly user interface with responsive web design. Support cross-browser compatibility and work across all devices.<br>• High speed distributed polling engine, supports polling large network, support automatic discovery and polling new devices and elements with zero effort.<br>• Scalable to manage IT infrastructure from SME to service provider at high performance and fast response.<br><br>Key Features<br>NNM is a carrier-grade IT Infrastructure Management solution that offers comprehensive FCAPS (Fault, Configuration, Accounting, Performance, and Security) capabilities. It allows for the management of multi-vendor IP networking devices, servers, VMs, and various networking technologies. This includes IP, MPLS, QoS, IP SLA, RPM, NetFlow, sFlow, jFlow, IPFIX, NetStream, NBAR, AVC, DPI, xDSL, FTTx, microwave, wireless technology, IP Surveillance, IoT, site environment monitoring, and advanced features such as Big Data Analytics, Predictive Analytics, AI Chatbot, and Anomaly Detection.<br><br>Centralized Network Monitoring<br>NNMX provides a centralized platform to monitor your entire network infrastructure, whether it spans multiple locations or is distributed across various environments. Gain real-time insights into your network's health, traffic, and performance, enabling you to identify and resolve issues promptly.<br><br>Network Visualization<br>Our solution offers a comprehensive visual representation of your network topology, allowing you to understand the |

| Solution | Brand | Product / Service | Description |
|---|---|---|---|
| | | | interconnectedness of your devices, switches, routers, wireless access points, servers, or IP cameras. Simplify complex network relationships and make informed decisions for network optimization.<br><br>Automated Discovery and Polling<br>Save time and effort with our automated network discovery and polling feature. NNMX seamlessly discovers and maps your network, polling devices, providing you with a comprehensive inventory. Keep track of hardware and software information, ensuring efficient network asset management.<br><br>Network Performance Monitoring<br>Our solution offers extensive network performance monitoring capabilities, empowering you to measure and analyze network bandwidth, latency, and utilization. Set thresholds and receive notifications for anomalies, enabling you to proactively address potential bottlenecks and maintain optimal network performance.<br><br>Configuration Management<br>NNMX allows you to manage network configurations effectively and efficiently. Ensure consistency across your network devices, track configuration changes, and easily revert to previous configurations when needed. Achieve network stability and minimize downtime with streamlined configuration management.<br><br>Security and Compliance<br>Protect your network from potential threats with robust security features. Monitor network security events, detect anomalies or suspicious activities, and ensure compliance with industry standards and regulations. |
| | SolarWinds | Solarwinds Orion Platform | The SolarWinds® Orion® Platform is a powerful, scalable infrastructure monitoring and management platform designed to simplify IT administration for on-premises, hybrid, and software as a service (SaaS) environment in a single pane of glass. There's no need to struggle with multiple incompatible point monitoring products, as the Orion Platform consolidates the full suite of monitoring capabilities into one platform with cross-stack integrated functionality.<br><br>ADVANTAGES:<br>• Reduce tool sprawl<br>• Monitor and manage from a single pane of glass<br>• Accelerate root cause discovery<br>• Connected use cases for connected problems<br>• See the big picture with intelligent mapping<br>• Monitor multivendor, on- premises, hybrid, and cloud infrastructure<br><br>PRODUCT INTEGRATIONS:<br>The Orion Platform and its associated ecosystem is a key foundation of the broader SolarWinds IT operations management (ITOM) offering. This ecosystem involves the following SolarWinds products or modules, which are installed directly onto the Orion Platform: |

| Solution | Brand | Product / Service | Description |
|---|---|---|---|
| | | | • Network Performance Monitor<br>• NetFlow Traffic Analyzer<br>• Network Configuration Manager<br>• Log Analyzer<br>• Server & Application Monitor<br>• Server Configuration Monitor<br>• Virtualization Manager<br>• Storage Resource Monitor<br>• Web Performance Monitor<br>• VoIP & Network Quality Manager<br>• IP Address Manager<br>• User Device Tracker<br><br>This ecosystem also involves the following SolarWinds products or modules, which are integrated with the Orion Platform:<br>• Database Performance Analyzer (DPA)<br>• Patch Manager<br>• Service Desk<br>• Engineer's Toolset<br><br>Orion Platform offers integrations with third-party applications/platforms such as ServiceNow and interoperability with third-party infrastructure, such as switches, cloud platforms, hypervisors, and storage arrays. |
| **Networking Products** | | | |
| Switch | Broadcom | Brocade SAN Switch | A SAN switch, or storage area network switch, is a device that connects servers and storage devices to move storage traffic. SAN switches are the core of storage area networks. |
| | Cisco | Cisco Catalyst Switch | Cisco network switches deliver performance, flexibility, and security. Cisco switches are scalable and cost-efficient and meet the demands of hybrid work. Cisco delivers a comprehensive portfolio of switching solutions for Enterprise Networks, data centers, and smaller businesses. These solutions are optimized for a wide range of industries, including service providers, financial services, and the public sector.<br><br>Built to reimagine connections, reinforce security, and redefine experience, the Catalyst 9000 family, including the new Catalyst 9000X models, offers versatile design for more flexible operations. The Catalyst 9000 family also assures a more secure experience and brings exceptional speed and scale to the table.<br><br>Catalyst 9000 switches lead the industry with the first 400G interfaces in Enterprise, first Silicon One ASICs for campus, full mGig and UPOE+ ports, converged switching and routing, and continuous zero-trust security.<br>Transform the workspace for hybrid work with a powerful platform that provides the broadest range of bandwidth, speed, scale, and power required for today's more immersive experiences, big and small. |

| Solution | Brand | Product / Service | Description |
|---|---|---|---|
| | | | Secure the network from inside to outside by leveraging enhanced computational power and advanced AI/ML to apply continuous zero trust security anywhere it's needed.<br><br>Future proof design so IT can work smarter not harder, with converged switching/routing capabilities, enhanced app-hosting and more config automations for a smarter, more agile campus and branch.<br><br>Benefits<br>• Twice the density at a lower cost. New features packed into Cisco IOS XE Software.<br>• End to end integrated security solution. Detect and stop threats, even with encrypted traffic.<br>• Simplified automation and assurance: goal-based policies are created once centrally, applied network-wide.<br>• Accelerate changes with programmability, supporting open standards and APIs.<br><br>The Catalyst 9300 Series is the next generation of the industry's most widely deployed stackable switching platform. Built for security, IoT, and the cloud, these network switches form the foundation for Cisco's Software-Defined Access, our leading enterprise architecture. |
| | | Cisco Nexus Switch | The Cisco Nexus series switches are modular and fixed port network switches designed for the data center. All switches in the Nexus range run the modular NX-OS firmware/operating system on the fabric. NX-OS has some high-availability features compared to the well-known Cisco IOS. This platform is optimized for high-density 10 Gigabit Ethernet.<br><br>Digital transformation is having a dramatic effect on enterprises, particularly in three areas: application evolution, application location, and infrastructure management. Modern data centers now must accommodate highly distributed workloads intensifying communications across hundreds or thousands of servers and even different clouds. Application development is also experiencing major shifts, with DevOps and with the associated growth in the use of Linux containers, microservices, and IPstorage. With these trends, network latency, throughput, scale, and visibility are extremely important in helping ensure high application performance and effective IT operations.<br><br>Cisco Nexus Switches offer an exceptional portfolio of networking solutions and integrated, converged, and hyperconverged platforms to help customer meet these challenges. The capabilities of the next-generation Cisco Nexus Series with Cisco Cloud Scale technology provide a multiyear advantage and sustained differentiation between Cisco and point-product network providers and providers of proprietary, single-vendor public clouds. A key component of The Cisco Data Center Series delivers a foundation that analyzes, simplifies, automates, and protects your entire modern data center like no other solution available.<br><br>Cloud-Scale Technology |

| Solution | Brand | Product / Service | Description |
|---|---|---|---|
| | | | As challenges become more diverse, Cisco offers customers a choice of custom application-specific integrated circuit (ASIC) and merchant silicon options in both modular and fixed form factors with flexible 1, 10, 25, 40, 50, and 100 Gigabit Ethernet port configurations. This flexibility offers investment protection and helps customers optimize their price-to-performance targets in their networking solutions for specific use cases and environments.<br><br>However, to address rapidly changing and increasingly complex hybrid data centers, customers should choose the Cisco Cloud Scale ASIC that powers the Cisco Nexus Series. This ASIC gives customers at least a two-year advantage in the functions they get compared to off-the-shelf silicon products, providing greater scalability, deeper analytics and visibility, and greater performance.<br><br>Cloud Scale ASICs offer significantly greater scale and more features at an optimized price with capabilities that include segment routing, group-based security policy, network service headers, and full-featured Virtual Extensible LAN (VXLAN) overlays.<br><br>Open and Extensible Programmability<br>Open Cisco NX-OS Software is the industry's most extensible, open, and programmable network operating system. It enables customers to programmatically provision and configure Cisco Nexus 9000 Series Switches through well-documented, comprehensive APIs offered by both Cisco and third parties. Customers can provision their switches using familiar tool integrations (such as Puppet, Chef, and Ansible) and have access to a robust API and community support. This innovation is essential for application developers, DevOps professionals, and other users who prefer self-service infrastructure models to complete their projects, such as application onboarding, more quickly and efficiently. Using NX-OS, IT staff can meet these requirements by provisioning the network more quickly, reducing the time to recovery after a failure, and gaining flexibility in an environment that is familiar to server administrators.<br><br>Full-Stack Automation and Security<br>IT organizations are expected to operate at the speed of business and deliver services with the agility of the public cloud. In this environment, capabilities such as rapid configuration on a consistent basis are not just desirable—they're essential. But speed needs to be coupled with accuracy. Many security problems are the result of user errors or misconfigurations, and they put your company at risk.<br><br>Cisco Application Centric Infrastructure (Cisco ACI) is the industry's number one Software Defined Networking (SDN) solution, delivering the most comprehensive automation capability. It enhances business agility, reduces total cost of ownership (TCO), automates IT tasks, and accelerates application deployment.<br><br>Real-Time Analytics and Deep Telemetry<br>The Cisco Nexus Series with the Cloud Scale ASIC come configured with support for the Cisco Tetration Analytics and |

| Solution | Brand | Product / Service | Description |
|---|---|---|---|
| | | | Cisco Nexus Data Broker solutions, providing customers with real-time visibility into application performance as well as enhanced security. IT can better understand the current system, helping prepare IT for whatever the future may bring.<br><br>Advanced Centralized Management<br>The Cisco Nexus Series offers tools such as Cisco Data Center Network Manager (DCNM) that enable customers to deploy switches efficiently and optimize the fabric through automatable capabilities. It automatically provisions Cisco Nexus switches and configures switch fabric virtual machine management (VMM) tools for the network manager. It also unifies LAN and SAN management software into a single platform, allowing both storage and network teams to manage their respective domains through a single system while being aware of each other's activities. The Cisco Nexus Series also uses the Cisco Nexus Fabric Manager to simplify the process of building and managing a Cisco Nexus fabric with a point-and-click web interface. After Cisco Nexus Series Switches are cabled in a leaf-and-spine topology, the fabric manager builds and self-manages a VXLAN-based fabric, dynamically configuring switches based on their roles and user-based actions. |
| | | Cisco SAN Switch | A SAN switch, or storage area network switch, is a device that connects servers and storage devices to move storage traffic. SAN switches are the core of storage area networks. |
| | | Meraki MS Series Switch | Cisco Meraki offers a broad range of switches built from the ground up that are designed to be easy to manage without compromising any of the power and flexibility traditionally found in enterprise-class switches.<br><br>Meraki access and aggregation switches are all managed through an elegant, intuitive cloud interface, freeing administrators to spend less time on configuration and more time on meeting business needs.<br><br>To set up a Meraki switch, just plug it in; there's no need for repetitive, command-based configuration. Switches can be up and running within minutes of connecting them to the network.<br><br>A powerful centralized management interface gives administrators deep visibility into the network and how it is used. See which switches are near capacity across hundreds of sites. Quickly provision and reconfigure switch ports with security, quality of service (QoS), and more. The Meraki dashboard provides unified policies, event logs, and monitoring, making switch management efficient and scalable.<br><br>Product highlights<br>• Range of enterprise switching options built on proven Cisco hardware technologies for traditional indoor environments and ruggedized environments<br>• Basic layer 2 to high-performance layer 3 switches with up to 40 GbE uplinks on access and up to 100 GbE on aggregation switches, suitable for deployments of all sizes |

| Solution | Brand | Product / Service | Description |
|---|---|---|---|
| | | | • True zero-touch configuration model that scales with organization needs and requirements<br>• Integrated troubleshooting tools, logging, and alerting help reduce operational costs<br>• Energy-efficient design with low acoustics and fanless options<br>• Flexible stacking for scaled configuration and high performance in one<br>• Cloud management reduces costs, overhead, and time to resolution<br>• Industry-standard features allow for simple integration into existing and mixed infrastructures<br>• Role-based administration and automatic, secure firmware updates delivered via the web<br>• StackPower, improved physical stacking, and multigigabit options on select models |
| | HPE | Aruba CX Switch | Simplify the complexities of deploying and managing modern enterprise networks with AI-powered automation and built-in security delivered by network switches that scale from edge to the cloud. Create a modern enterprise network that connects, protects, and simplifies. Take advantage of intuitive management tools and built-in analytics to meet the ever-growing needs of your users, devices, and applications.<br><br>Operational power<br>Intelligent automation and analytics for flawless configurations and actionable built-in diagnostics with unified management.<br><br>Always-on reliability<br>Highly resilient scalable architecture with visibility and control that eliminates downtime for business continuity – even during upgrades – across campus and data center networks.<br><br>End-to-end security<br>Role-based policy driven Dynamic Segmentation for automated enterprise-wide fabric to secure users and IoT. |
| | | HPE SAN Switch | A SAN switch, or storage area network switch, is a device that connects servers and storage devices to move storage traffic. SAN switches are the core of storage area networks. |
| | IBM | IBM SAN Switch | A SAN switch, or storage area network switch, is a device that connects servers and storage devices to move storage traffic. SAN switches are the core of storage area networks. |
| | Lenovo | Lenovo SAN Switch | A SAN switch, or storage area network switch, is a device that connects servers and storage devices to move storage traffic. SAN switches are the core of storage area networks. |
| Router | Cisco | Cisco Router | Cisco routing provides intent-based networking for the WAN, LAN, and cloud. Our network routers include advanced analytics, application optimization, automated provisioning, and integrated security to deliver a complete, proven solution.<br><br>With Cisco SD-WAN and Cisco Catalyst Center, businesses can automate the provisioning of multiple branch offices. You can also provide intelligent path selection and application control |

| Solution | Brand | Product / Service | Description |
|---|---|---|---|
| | | | using minimal programming and customization. Our high-performance routers streamline network operations. They can reduce costs, speed up deployment for your branch, and make your network architecture more agile.<br><br>Whether you need a small business, branch, edge, enterprise, industrial, or virtual router, Cisco's extensive portfolio of network routers offers end-to-end management and flexibility for your WAN, LAN, and cloud network.<br><br>Benefits<br>Stronger security across your WAN connection Highly secure authentication, strong encryption, and segmentation help protect your users, data, and applications, from the WAN edge to the cloud.<br>• Improve efficiency with on-demand network services Respond to business needs faster and increase IT efficiency by deploying integrated network services on demand, wherever you need them.<br>• Improve your user experience Increase productivity by using real-time analytics, visibility, and control to optimize cloud and on-premises application performance.<br>Experience the benefits of intent-based networking Centralize management for easier deployment of SD-WAN and security while maintaining policy across thousands of sites. |
| Wifi | Cisco | Cisco Catalyst WiFi | Through the evolution of Cisco's wireless portfolio comes the next generation of 6GHz Wi-Fi. Cisco access points give you the flexibility to manage your wireless network on premises or in the cloud. With reliability, security, and applied AI with the choice to network your way with on-prem and cloud options, the Cisco Catalyst Wi-Fi 6E access points provide the best of both worlds while delivering flexibility and performance to meet your most critical network requirements.<br>Cisco understands that selecting your next platform is not an easy choice. With the Cisco Catalyst Wi-Fi 6E access points, you don't need to make the decision now. Keep the operational mode you use today, whether on premises or cloud management. If your needs change-either way-it's an easy switch. No new hardware required. That's investment protection for your network that you can count on.<br><br>Hybrid Work<br>The Cisco Catalyst Wi-Fi 6E access points are the perfect fit for your hybrid work deployment. Hybrid work is all about creating safe, immersive work experiences that foster collaboration, ideation, and innovation. The Cisco Catalyst Wi-Fi 6E access points deliver the performance and features to optimize the hybrid work experience.<br>Cisco Catalyst Wi-Fi 6E access points deliver connectivity in the 2.4- and 5-GHz bands as well as 6 GHz for compatible devices. Wi-Fi 6E offers greater capacity for more devices with more reliable connections, plus more robust security thanks to stronger Wi-Fi Protected Access 3 (WPA3) encryption.<br>With the Cisco Catalyst Wi-Fi 6E access points, you get capabilities based on decades of experience and innovation. This includes long-standing industry leadership with standards bodies and work with ecosystem partners to deliver next-generation features for your modern network needs. |

| Solution | Brand | Product / Service | Description |
|---|---|---|---|
| | | | • Intelligence: Through data from tens of millions of cloud-managed devices, Cisco's platforms are continuously evolving and extending intelligence (AI/ML) to automate identification and, when necessary, resolution of access networking issues.<br>• Any operational model: A unified access networking portfolio with built-in security that brings together the broadest wireless portfolio (Wi-Fi 6E) under any operational model, on-premises or cloud.<br>• Ecosystem partners: Cisco has the industry's most extensive ecosystem of technology partners to address emerging use cases such as location analytics, extended reality, industrial IoT, and more.<br><br>The Cisco Catalyst Wi-Fi 6E access points use the power of access network automation platforms like the Meraki dashboard and Cisco DNA Center to radically simplify operations, making it easier to embrace change and optimize user experiences.<br><br>Additionally, features such as Band Steering make the most of your Wi-Fi 6E network by intelligently steering devices to the high-performance 6-GHz band. And Cisco CleanAir Pro protects your network from the impact of wireless interference.<br><br>Either way you chose, on-premises with Cisco DNA or in the cloud with Meraki Dashboard, the Cisco Catalyst Wi-Fi 6E access points deliver the performance of Wi-Fi 6E and the capabilities and flexibility to support your network now and into the future. |
| | | Meraki MR Cloud-Managed WiFi | The Cisco Meraki MR series is an enterprise-grade line of cloud-managed WLAN access points that leverage the award-winning Cisco Meraki cloud-managed architecture to provide powerful and intuitive centralized management while eliminating the cost and complexity of traditional on-site wireless controllers. Meraki MR series APs are designed for challenging enterprise environments characterized by high-performance hardware, multiple radios, and advanced software features with proven scale and reliability (99.9 cloud SLA) to support the most demanding use cases.<br><br>Product highlights<br>Meraki MR wireless access points come equipped with industry-leading features that make them ideal for demanding enterprise deployments:<br>• Self-configuring plug-and-play deployment<br>• 802.11ax MU-MIMO with up to eight spatial streams built for voice and video<br>• Dedicated radio for security and RF optimization with integrated spectrum analysis (indoor models)<br>• Advanced security to protect against malware, ransomware, and C2 callbacks with Umbrella integration<br>• Integrated intrusion detection and prevention system (WIDS/WIPS)<br>• Intelligent firmware upgrades that minimize downtime<br>• AI/ML-powered analytics for root cause analysis and Wi-Fi troubleshooting |

| Solution | Brand | Product / Service | Description |
|---|---|---|---|
| | | | • Advanced application visibility with Cisco Network-Based Application Recognition (NBAR)<br>• Flexible group policy engine for creating and applying application-aware policies by network, device type, and end user<br>• Wi-Fi personal network (WPN) on any shared network (dorms, senior living, hotel rooms, etc.)<br>• Integrated Bluetooth IoT radio<br>• IoT ready (ESL integration)<br>• Self-healing, zero-configuration mesh<br>• Intelligent firmware upgrades that minimize client downtime<br>• Role-based administration and automatic, scheduled firmware upgrades delivered over the web<br>• Email and text message alerts upon power loss, downtime, or configuration changes<br>• FIPS-140-2 compliant, IPv6 compatible, WFA-certified APs |
| | HPE | Aruba Wifi | High-performance, secure enterprise wireless LAN with support for Wi-Fi 6 and Wi-Fi 6E. Wi-Fi access points and controllers for seamless connectivity. With secure, reliable Wi-Fi that has built-in intelligence.<br><br>Ease of cloud-managed networking<br>Improve efficiency, scalability, and reliability using Aruba ESP and Aruba Central. With cloud-native, centralized management, IT gains visibility across wired, wireless, and WAN architectures using a single pane of glass.<br><br>AI-powered network operations<br>Increase the efficiency and effectiveness of network operations with AIOps. Aruba AIOps applies machine learning to proactively identify issues, recommend corrective actions, and provide service assurance.<br><br>Security for the Intelligent Edge<br>Aruba's Zero Trust Security model reduces risk with role-based policy enforcement firewalls and dynamic segmentation. Support for Wi-Fi 6 standards provides better user and guest encryption. |
| **Notebook/PC/Printer** | | | |
| Notebook/PC/ Printer | Canon | Large Format Printer | Reliable printer for high quality CAD drawing with water resistant ink |
| | Dell | Notebook/PC | Dell's laptop portfolio includes options for a range of computing needs.<br>- Inspiron is for mass-market consumers.<br>- The Vostro line is for low-end business.<br>- The Latitude line is for business-class.<br>- The XPS line is for high-end consumers and creators.<br>- The Precision line is computer workstations for professionals in computer-aided design and computer graphics. |
| | HP | HP Printer | |
| | | Notebook/PC | HP's laptop portfolio includes options for a range of computing needs. |

| Solution | Brand | Product / Service | Description |
|---|---|---|---|
| | | | - The ProBook is for entry-level and mid-range business laptops<br>- The EliteBook is for high-end business laptops<br>- The Zbook is for mobile workstations who need maximum performance while traveling. |
| **OS & Database** | | | |
| OS & Database | IBM | IBM DB2 | IBM Db2 is the database to run your mission-critical workloads. Low-latency transactions and real-time analytics across any cloud, hybrid, or on-prem. |
| | Microsoft | Microsoft SQL | Microsoft SQL Server is a relational database management system developed by Microsoft.<br>As a database server, it is a software product with the primary function of storing and retrieving data as requested by other software applications. There is choice and flexibility across languages and platforms, including Linux, Windows, and Kubernetes. |
| | | Microsoft Windows | Microsoft Windows is a group of operating systems (OS).<br>Windows Server is a series of enterprise-class server operating systems. It's designed to share services with multiple users and provide administrative control of data storage, applications, and corporate networks. Windows Server is typically installed on heavy-use servers that serve as the backbone for most IT companies, applications, and services. A client operating system can be run on a desktop or workstation. |
| | Oracle | Oracle Database | Oracle Database (Oracle DB) is a relational database management system (RDBMS) that stores, organizes, and retrieves data. Oracle Database offers market-leading performance, scalability, reliability, and security, both on-premises and in the cloud. |
| | Red Hat | Red Hat Enterprise | Red Hat Enterprise Linux (RHEL) is a Linux operating system developed by Red Hat for the business market.<br><br>It is a commercial open-source Linux distribution that is mainly used in commercial data centers. RHEL is certified with thousands of vendors and across hundreds of clouds. |
| | SUSE | Linux SUSE | SUSE Linux is a Linux operating system developed by SUSE. It is built on the Linux kernel and is distributed with system and application software from other open-source projects. SUSE Linux is similar to Red Hat, assembling the Linux kernel and other open-source components into a stable, full-featured Linux operating system. |
| **People & Organization** | | | |
| HR Solution | D-Work | D-Work | D-Work streamlines HR management as a from-hire-to-retire solution. |
| **Risk & Compliance** | | | |

| Solution | Brand | Product / Service | Description |
|---|---|---|---|
| Integrated Risk Management | ServiceNow | ServiceNow IRM | ServiceNow IRM, or Integrated Risk Management, is a suite of applications designed to help organizations manage risk, compliance, policy, and audit processes in a unified and integrated manner |
| Audit Tools | Wolters Kluwer | TeamMate+ | A comprehensive solution supports auditors throughout the entire audit process, including planning, execution, collaboration, reporting, and follow-up, ensuring an efficient and effective approach to auditing. It's built with a focus on risk-focused planning and execution, offering data-driven insights and stakeholder engagement through an open ecosystem that is compatible with various infrastructures. |
| ESG | Wolters Kluwer | TeamMate+ ESG | The solution helps leaders understand and address ESG-related risks and supports transparent reporting on climate change, equity, inclusion, and other critical ESG issues. TeamMate+ ESG is recognized for its contribution to promoting transparency and accountability in ESG practices. |
| Finance, Risk and Regulatory Reporting | Wolters Kluwer | OneSumX FRR | A unified platform that simplifies compliance with regulatory requirements, optimizes processes, and provides a real-time and accurate view of an organization's financial position. Manage the complexities of finance, risk, and regulatory compliance by enabling them to connect critical data across the enterprise, thus facilitating better strategic decisions and ensuring compliance under the pressure of rapid regulatory changes. |
| **Server & Storage** | | | |
| Server & Storage | Cisco | Cisco UCS | Cisco UCS is a versatile general-purpose infrastructure and application server. It can deliver industry-leading performance and efficiency for a wide range of workloads, including virtualization, collaboration, and bare-metal applications. |
| | Dell | Dell Intel Server | PowerEdge rack servers are purpose built to address your most challenging workloads, working autonomously and collaboratively across all your IT environments. Paired with our OpenManage integrated IT management system. |
| | | Dell Storage | Dell's storage portfolio is designed to meet the storage needs of organizations of all sizes.<br>• PowerMax: World's most secure mission-critical storage PowerStore: Intelligent all-flash storage for the digital enterprise<br>• Unity XT: Flexible hybrid storage for cost-sensitve enterprises<br>• PowerFlex: Unbounded software-defined infrastructure<br>• PowerScale: Secure and efficient scale-out NAS purpose-built for AI<br>• PowerVault: Affordable entry block storage<br>• ECS: World's most secure enterprise object storage<br>• VxRail: Proven, turnkey hyperconverged infrastructure<br>• Power Protect: Designed to meet backup, archive, disaster and cyber recovery needs for organizations of all sizes |
| | | Dell Tape Device | Tape drives are devices that store computer data on magnetic tape for backup and archiving. |

| Solution | Brand | Product / Service | Description |
|---|---|---|---|
| | | Dell Tape Media | Magnetic-tape data storage is typically used for offline, archival data storage. |
| | HPE | HPE Intel Server | HPE ProLiant servers are designed for small and midsize businesses, with a cloud operating experience, built-in security, and optimized performance |
| | | HPE Storage | Simplify data management with HPE Storage.<br>• MSA: Flash-enabled storage array<br>• Alletra 5000: simple, reliable, and cost-efficient scale-to-fit hybrid storage<br>• Alletra 6000: Designed for business-critical workloads with strict availability and performance SLAs<br>• Alletra 9000: Optimized for workloads with extreme latency and availability requirements. Delivers mission-critical reliability<br>• StoreEasy: network-attached storage purpose-built to affordably a store and protect file<br>• Simplivity: an intelligent, hyper-efficient HCI solution that's optimized for your edge, VDI, and general virtualization workloads.<br>• HPE StoreOnce: Secure your data with greater simplicity, higher performance, and built-in ransomware protection |
| | | HPE Tape Device | Tape drives are devices that store computer data on magnetic tape for backup and archiving. |
| | | HPE Tape Media | Magnetic-tape data storage is typically used for offline, archival data storage. |
| | IBM | IBM Storage | The IBM FlashSystem family is a portfolio of cloud-enabled storage systems:<br>• IBM FlashSystem 5000 are designed to provide enterprise-grade functionalities without compromising affordability or performance.<br>• IBM FlashSystem 5200 is a compact, cost-efficient, security-rich with the power of NVMe in only 1U.<br>• IBM FlashSystem 7000 offers the advantages of robust NVMe, the innovation of IBM FlashCore technology and SCM for ultra-low latency.<br>• IBM FlashSystem 9000 is built for growing enterprises needing the highest capability and resilience. It offers twice the maximum performance, connectivity, and capacity of IBM FlashSystem family. |
| | | IBM System i | IBM i is a fully integrated operating system, meaning the database, middleware, security, runtime and hypervisor are integrated into the stack and licensed as one solution.<br><br>IBM i provides continuous availability, enhanced security, simplified systems management and integration with new technologies- making it the trusted platform to run businesses |
| | | IBM System p | IBM AIX is IBM's proprietary Unix operating system designed to run on IBM Power servers. For over three decades, organizations have trusted IBM AIX to run their most mission-critical applications. |

| Solution | Brand | Product / Service | Description |
|---|---|---|---|
| | | | AIX on Power drives innovation with hybrid-cloud and open-source capabilities that help you build and deploy modern applications within a secure and resilient environment. |
| | | IBM Tape Device | Tape drives are devices that store computer data on magnetic tape for backup and archiving. |
| | | IBM Tape Media | Magnetic-tape data storage is typically used for offline, archival data storage. |
| | Imation | Imation Tape Media | Magnetic-tape data storage is typically used for offline, archival data storage. |
| | Lenovo | Lenovo Intel Server | From small businesses to enterprise workloads, Lenovo servers offer the industry-leading scalable processors designed for AI to meet mission-critical demands with legendary quality and reliability. |
| | | Lenovo Storage | Lenovo ThinkSystem DE Series Storage Arrays are designed to provide performance, simplicity, capacity, security, and high availability for medium to large businesses. ThinkSystem DE Series Storage Arrays deliver hybrid and all flash storage with enterprise-class storage management capabilities and a wide choice of host connectivity options, flexible drive configurations, and enhanced data management features. |
| | Nutanix | Nutanix Server | Nutanix is a software stack that unifies hybrid cloud infrastructure, including computing, storage and network, hypervisors, and containers. It has built-in resilience, self-healing, disaster recovery capabilities, and security. Nutanix can support workloads across public and private clouds, multiple hypervisors and containers, and varied computer, storage, and network requirements.<br>• The native Nutanix hypervisor, AHV, represents a fresh approach to virtualization that brings substantial benefits to enterprise IT administrators by simplifying every step of the infrastructure life cycle, from buying and deploying to managing, scaling, and supporting.<br>• Nutanix Flow delivers advanced networking and security services, providing visibility into the virtual network, application-centric protection from network threats and automation of common networking operations.<br>• Nutanix Calm provides advanced application-level orchestration that transforms how IT teams manage applications and support the business. Calm delivers a powerful, common management framework that can be simultaneously leveraged by multiple IT teams to rapidly create and deliver applications.<br>• Nutanix Karbon is a enterprise-grade Kubernetes service offering that simplifies the provisioning, operations, and lifecycle management of Kubernetes. |
| Software Tools | Adobe | Creative Cloud | Adobe Creative Cloud is a software application for creative projects in photography, graphic design, video editing, UX design, drawing and painting, social media, and more. |
| | IBM | WebSphere Application Server | IBM® WebSphere® Application Server accelerates application delivery with a highly reliable Java Enterprise Edition-based |

| Solution | Brand | Product / Service | Description |
|---|---|---|---|
| | | | runtime environment and is now a part of IBM WebSphere Hybrid Edition. Today's agile businesses depend on IT leaders to deliver high-performing applications to support rapid change while saving costs and improving time to value. But achieving these results in complex, heterogeneous IT environments can be a challenge. WebSphere Hybrid Edition empowers your development teams to deliver new cloud-native apps and modernize existing apps, all while maintaining your traditional WebSphere estate. |
| | Microsoft | Microsoft Office | Microsoft Office is a family of client software developed by Microsoft. It contains a word processor (Word), a spreadsheet program (Excel) and a presentation program (PowerPoint), an email client (Outlook), a database management system (Access). |

## DCS Services

| Solution | Service | Service Description |
|---|---|---|
| Application Development | Application Development | Tailor-Made Software Solution Services<br>We develop systems for customers with various options through Tailor-Made Solutions, which involve system development from the beginning based on the customer's requirements. This is suitable for organizations with their own specific work characteristics that cannot adapt packaged software. The advantage is the flexibility to customize according to the customer's needs.<br><br>We have experts involved in collecting requirements, then analyze and design systems to develop projects successfully. Additionally, we have a support team to provide fast and excellent post-sales services to help organizations smoothly operate their businesses.<br><br>We develop systems using various technologies suitable for the nature of the work, cost considerations, and in line with current technology. This includes Web Application, Native Mobile Application, and APIs, such as .Net, Java, Nodejs, React, Angular, Flutter, Ionic, Swift, and others. |
| | Application Performance Monitoring | Cisco AppDynamics is an application performance monitoring and application intelligence platform that helps businesses gain real-time insights into the performance, availability, and user experience of their applications and IT infrastructure, enabling proactive problem resolution and optimization. |
| Contact Center | Chat Bot Systems | Rule-based chatbot with workflow and productivity tracking. Integration with Cisco Webex to enable logging task progress step-by-step with state transition. Productivity and provides guideline for work optimization as benefit. |
| | Contact Center Chat Integration | Chat channel queue distributed system for handling customer chat request and assign to designated agents by given conditions, similar to telephony channel. Integrates with multiple popular social platforms and simplified chat experience to agents. |
| | Contact Center Customization | Unified smart agent platform integrates various customer channels into the single application.<br><br>Enable agents to work with less distraction by less windows switching and more productivity by improved on information focusing. |

| Solution | Service | Service Description |
|---|---|---|
| | Knowledge Base Management | Provides resources, documents, training manuals and/or frequently asked questions as shared information between users in the organization to enable self-service. Features with rich-content editor and file uploading. Able to integrate with external services and/or tailor-made customized pages. |
| Disaster Recovery | DRC Hot Site | "A disaster recovery hot site is a fully functional backup site, a backup facility that replicates the primary production facility. It includes the software, hardware, and network connectivity as the primary center, and enables real-time backup (data replication) of important data.<br>• Recovery Time Objective (RTO) is near-zero.<br>• Recovery Point Objective (RPO) is near-zero<br><br>Hot-Site summary:<br>- fully redundant equipment<br>- network connectivity is enabled<br>- failover occurs within hours or days<br>- near real-time data synchronization<br>- zero data loss" |
| | DRC Warm Site | "A disaster recovery warm site is to prepare the standby hardware ready to be used, but backup data must be sent to the site to install.<br>• Recovery Time Objective (RTO) can be 24-48 hours or more depend on the amount of data.<br>• Recovery Point Objective (RPO) is based on the most recent backup available. The data lost may be more than 24 hours.<br><br>Warm-Site summary:<br>- partially redundant equipment<br>- network connectivity is enabled<br>- failover occurs within hours or days<br>- schedule of data synchronization<br>- minimum data loss" |
| | DRC Cold Site | "A disaster recovery cold site is a backup facility with little or no hardware equipment installed. Using a cold site is very limited to a business since before it can be used, hardware needs to be set up and backup data must be sent to the site to install.<br>• Recovery Time Objective (RTO) can be 48 hours a week. This is because hardware preparation and data installation are required, which depends on the amount of data.<br>• Recovery Point Objective (RPO) is based on the most recent backup available. The data lost may be more than 24 hours.<br><br>Cold-Site Summary:<br>- little or no equipment<br>- no network connectivity<br>- not ready for automatic failover<br>- no data synchronization<br>- high risk of data loss" |
| | DR Rack Co-location Service | Provide rack space for store customer's own server equipment in data center, with physical monitoring service |
| | Office Continuity-Dedicated | "We offer dedicated office space to ensure your staff can stay productive while working off site. Enable businesses to continue their normal activities in a disaster situation.<br><br>Office Facilities and equipment are dedicated and prepared to be used for each customer which include: |

| Solution | Service | Service Description |
|---|---|---|
| | | - dedicated room (office space)<br>- table and chair<br>- computer and printer<br>- telephone and internet access<br>- etc.<br><br>Computers can be setup and prepared for use, whether it's the OS or application according to the version you want to use." |
| | Office Continuity-Shared | "We offer the office space to ensure your staff can stay productive while working off site. Enable businesses to continue their normal activities in a disaster situation.<br><br>Office Facilities and equipment are prepared to be used which include:<br>- room (office space)<br>- table and chair<br>- computer and printer<br>- telephone and internet access<br>- etc.<br><br>Computers require a deployment image before they are ready to use." |
| IT Services | IT Infrastructure Service | Provide IT Infrastructure environment, which bundle IT managed service together as monthly service fee model |
| | IT equipment as a Service | |
| | DR Managed Service | Provide service to recover IT infrastructure environment at DR site |
| | Managed Service and Outsourcing | Provision services focused on monitoring and troubleshooting of networks. That has evolved from a break/fix service to a proactive approach that includes patch management and predictive maintenance etc.<br><br>Provision of various skillset right from admin, network engineer to network consultant. Additionally, we provide resources to cater for short term project requirements about networking.<br><br>The primary tasks performed by managed IT service can be categorized into the following:<br>• Monitoring: Real-time monitoring of business environment that is related with network devices and issues.<br>• Proactive service: Preventative maintenance, which includes software upgrades, security software updates, patch updating, and alerts for thresholds reached that could lead to network downtime issues.<br>• Scheduled maintenance: This can be done remotely or on-site in coordination with the in-house IT staff.<br>• Infrastructure-as-a-Service (IaaS): The Managed Service provides the hardware and software access to allow a business to create an entire IT infrastructure without owning it or installing the hardware on-site.<br>• Software-as-a-service (SaaS): The subscription model is used for 'software-as-a-service' (SaaS) agreements where the software is centrally hosted by the provider and accessed by the client. |
| | Network Assessment Services | DCS undertakes a range of site network and connectivity assessments to meet audit, security, planning, performance, quotation and due diligence business drivers.<br><br>Our assessment will typically focus on five areas for examination: |

| Solution | Service | Service Description |
|---|---|---|
| | | • Infrastructure<br>• Performance<br>• Availability<br>• Management<br>• Security<br><br>Network Assessment Report<br>One of the key benefits of a network assessment is to have a complete documented summary of the current set-up, along with an analysis of threats/opportunities, and recommendations to the business.<br><br>DCS provides a comprehensive report that can include the following modules as relevant and selected by the customer:<br>• Discovery<br>• Issues summary<br>• Infrastructure design summary<br>• Performance and Availability summary<br>• Security summary<br>• Recommendation summary |
| | Network Professional Service | We provide network consulting services ranging from consultation, design, assessment, right to the implementation services. Offering a full range of Network Consulting Services, we transform and improve the performance of your infrastructure, while optimizing your spending.<br><br>Specifically, we can:<br>• Advise on adopting new technologies and services, designing your hybrid IT environments.<br>• Develop various technology services to support your strategy.<br>• Design a solution to either transform, or increase the longevity of and integrate into, your existing environment, with our multivendor and cross technology capabilities.<br>• Partner with you to deploy the solution; or operationalize it through our managed services capability.<br><br>Our technical network consulting ability offers expert advice in networking. Our capabilities help you from business availability, security and compliance, infrastructure lifecycle management and full automation to analytics in wired and wireless areas, our capabilities help you. |
| | Oracle Database Admin (DBA) | DCS provides DBA database services that can help to build, update, or troubleshoot Oracle database. DCS also offers advanced services including:<br>• Installing Oracle software<br>• Configuring the database file system storage with Automatic Storage Management (ASM)<br>• Configuring database high availability with Real Application Clusters (RAC)<br>• Configuring replication with Data Guard<br>• Configuring Oracle Recovery Manager (RMAN) to backup and restore databases.<br>• Upgrading the database and software to new releases<br>• Oracle Database Migration |
| | Preventive Maintenance | Preventive maintenance is regularly and routinely performed on physical assets to reduce the chances of equipment failure and unplanned machine downtime. Effective preventive maintenance is planned and scheduled based on real-time data insights. A preventive maintenance task is performed while the equipment is still working to prevent unexpected breakdowns.<br><br>Maintenance reports : |

| Solution | Service | Service Description |
|---|---|---|
| | | Depend entirely on what you are making the report for. In general, an official maintenance report might include:<br>• Information about the organization (name, logo, address, contact information<br>• Name/type of the report<br>• Timeframe for which the report was generated<br>• Report details (the main part of the report that outlines all the data<br>- Design<br>- Connectivity<br>- Performance and Availability<br>- Issues<br>- Etc.<br>• Any additional information that might be useful (considered on a case-to-case basis) |
| | Project Management | Project management services specialize in planning, coordinating, and executing projects according to specific requirements and constraints. They perform some or all the activities related to project work, from conceptualization to completion. Emphasis is placed on creating and maintaining project milestones and the project schedule. The end goal is to complete the project on time and within budget.<br><br>Here's where we get down to the process of building that scope statement. Six major scope management processes involved in managing and defining a project's parameters. These are:<br>• Planning scope management: A scope management plan is created based on input from the project plan, the project charter, and consultation with stakeholders.<br>• Collecting requirements: A requirements management plan is created based on the scope management plan plus stakeholder input. Interviews, focus group discussions, surveys, and more will be used to understand requirements. This will all be documented.<br>• Defining scope: A project scope statement is produced based on all the requirements documentation plus the project charter and the scope management plan. This definition will be the basis for all project activity.<br>• Creating the Work Breakdown Structure: A Work Breakdown Structure (WBS) is built after analyzing the project scope statement and the requirements documentation. The WBS is basically the entire project broken down into individual tasks, and deliverables are clearly defined.<br>• Validating scope: Here, deliverables are inspected and reviewed. Either they're accepted as complete or further revisions are requested.<br>• Controlling scope: As the project is executed, scope must be controlled. Performance reports are compared against project requirements to see where gaps exist, which may result in changes to the project plan.<br><br>Communication is an important aspect of project management that cannot be forgotten throughout the course of the project. All project's stakeholders should receive regular updates via email, meetings, conference calls, or by viewing a project's dashboard. Communication during all phases of the project can help avoid costly rework later. |
| Rental Services | Network Equipment Rental | Rental offers a cost-effective solution to companies that require equipment on a short-term basis |
| | Security Equipment Rental | |

| Solution | Service | Service Description |
|---|---|---|
| | Server & Storage Equipment Rental | |
| | Multimedia Products Rental | Projector long term rental service provide worry fee for equipment maintenance with DCS |
| Training Services | System Training | DCS can provide a flexible System training that is created to meet the customer needs. |
| Multimedia Product Service Center | Projector | DCS is authorized service center for Panasonic & Epson projector with well trained and experienced technician to support customer |

Datapro Computer Systems

*www.datapro.co.th*

# DATAPRO COMPUTER SYSTEMS CO., LTD.

## CALL: 02-684-8408


**Head office: Premier Place Bldg.**
2 Premier Place, Soi Premier 2,
Srinakarin Road, Nongbon,Prawet,
Bangkok 10250, Thailand.
Tel : 66-(0)2714-5995

**Branch I: Bangkok Insurance Bldg.**
25 Bangkok Insurance/Y.W.C.A. Bldg.,
12th fl. South Sathorn Road, Thungmahamek,
Sathorn, Bangkok 10120, Thailand.
Tel : 66-(0) 2684-8484


**www.datapro.co.th**