The Future of Secure Network Connectivity

The Future of Secure Network Connectivity

Connecting and securing hybrid, work-from-anywhere environments

The pandemic proved to be transformational for networking and security technologies. From the beginning, organizations rapidly moved employees home to work, which simultaneously impacted broadband usage. Where it had been climbing in previous years, a 2020 report showed that broadband usage sharply increased by 40% over 2019.[1]

But that was only the beginning. In addition to sending employees home to work, organizations quickly scaled operations to accommodate this massive business disruption and continue business operations. As a result, they undertook three key initiatives that have forever changed networking and security:

- **IoT –** As organizations sought to generate value and return on investment, IoT initiatives exploded. One report showed more than 46% of IoT projects were in full deployment in 2020 compared to only 7% the previous year.[1]
- **Cloud –** Once a "nice to have" for many businesses, cloud projects quickly moved into the "must-have" column. In its May 2020 report, Flexera reported that "the majority (57%) of organizations had changed their cloud usage plans to be slightly or significantly higher than originally planned."[1] Organizations also began adopting multi-cloud strategies to ensure the best price for each workload. Today, 87% report having a multi-cloud strategy in place.[2]
- **Security –** Even as their distributed environments—and security needs—grew, CISOs had to quickly pivot to support them, while supporting business operations. In fact, 85% admitted that "they sacrificed cybersecurity in the effort to enable employees to work remotely." As a result, 63% conceded that there was a corresponding rise in cyberattacks.[3]

Clearly, the pandemic not only changed the ways that we work, but it also shifted business priorities, technology roadmaps, and digital transformation plans. Today's organizations are distributing applications across on prem data centers, public clouds, edge and work-from-anywhere locations, creating management complexity and blind spots for networking teams—and prompting a major rethinking of networking and security models.

And now it's leading us into a new future, driven by cloud-based networking, perimeter-less zero-trust security and AI-everything.

This playbook shows you how you can help your customer transition to a post-disruption world that's more connected, more automated, more intelligent, more secure and more efficient.

Networks are changing.....

- 50% of organizations currently using network automation technology report these solutions do not leverage AI/ ML capabilities.[4]
- 58% of organizations would immediately switch to a nonincumbent vendor that offered robust unified end-to-end network management software.[4]
- 65% of organizations identify improving IT team productivity as a business driver behind their purchases of joint vendor technology solutions.[5]
- 84% currently use, are experimenting with, or plan to use AI/machine learning as a public cloud service.[6]

Security is changing.....

- 51% and 39% of IT professionals cite identifying cloud security risks and the increase in remote workers, respectively, as major challenges.[2]
- 41% of networking professionals say that providing secure access to applications distributed across multiple clouds is the top challenge.[6]
- 37% of networking professionals report that gaining end-to-end visibility into network performance and security as more traffic originates or terminates beyond the boundaries of the corporate network is the second biggest challenge.[6]
- 61% of organizations are using managed services extensively to support their cyberthreat intelligence program.[7]
- 64% of organizations believe that their cyberthreat intelligence sources are not always accurate.[7]
- 82% of organizations believe that cyberthreat intelligence programs are often treated as an academic exercise.[7]
- 46% of organizations use their cyberthreat intelligence program to help pinpoint security

The new "normal"....

- "Cloud is the new data center, Internet is the new network, and cloud offerings dominate applications."[7]

Considerations for Long-Term Work-from-Home (WFH) and Hybrid Environments

The Shift to Work-From-Home Employees

The rise of work-from-home employees continues to fundamentally change both how we work and live. Employees benefit from less commute time and a better work-life balance – and most employees say they want to work from home at least some of the time.

The challenge for organizations is that work-from-home employees create a growing attack surface that's difficult to secure, due to a plethora of personal devices and a patchwork of home networks. Will employees use their corporate-issued device or the tablet that's conveniently sitting nearby? Will they connect through an onerous corporate VPN—or a bullet-fast home network?

Data has consistently shown the security risks that work-from-anywhere employees bring. In one report, some 56% of IT leaders believe employees have adopted bad cybersecurity behaviors while working from home – and 54% are worried remote workers will bring infected devices and malware into the office.[8]

Work-From-Home Employees: A New Perspective

New research suggests that security awareness training may finally be taking hold. Rather than carelessly accessing data from untethered devices, the survey found that work-from-home employees typically feel a much more heightened sense of responsibility for their own cybersecurity. They are more aware of the risks and feel more personally invested in precautions that they can take to prevent a security incident.

Employees working onsite full-time, however, trust their organizations to develop, maintain, and update security systems and practices to mitigate cybersecurity threats and risks on their behalf. These employees tend to become much more complacent and pay less attention to security threats and concerns. It's the notion of "someone is taking care of that."

Security awareness training is just not a checkbox item for remote workers. The study reveals that as they gained greater cybersecurity awareness, work-from-home employees were more likely to take the precautions they learned and apply them. This reinforces the idea that "fostering cybersecurity awareness among remote workers can lead to better protection of organizational information assets against threats."[9]

56%
of IT leaders

believe employees have adopted bad cybersecurity behaviors while working from home.[8]

72%
of organizations

of organizations treat home offices as corporate endpoints that require network visibility and management using centralized enterprise solutions.[4]

Cloud Networking Considerations for Long-Term Work-from-Home (WFH) and Hybrid Environments

Cloud Networking: The "New Normal" in Networking

The cloud model has become the gold standard for today's modern organizations for its ability to drive agility, deliver differentiation, accelerate time-to-market and increase scale. Most turn to the cloud to address their growing infrastructure needs, M&A deals and regional expansions and redundancy plans.

The cloud also enables organizations to choose what resides on premises and what resides on private, public or hybrid clouds and then make the connections between resources. But for many organizations today, on-premises deployments, public/private/hybrid cloud services, legacy applications and systems and emerging technologies have created an increasingly fragmented network environment. The result? Lack of governance and visibility, leading to poor management and weakened security for customers.

Add in leased connections (e.g., colocation) and untethered devices and applications (e.g., shadow IT), and consistently extending network protocols and security policies out into a multi-cloud environment quickly becomes a self-surrendering quagmire.

With cloud networking, your client can drastically improve performance, security and management of their hybrid and multi-cloud environments by enabling connectivity to and between applications and workloads across clouds, cloud services, on-premises data centers and edge networks. They can host network resources—virtual routers, firewalls, bandwidth and network management software, etc.—on a public or private cloud platform and manage them in-house. Or your customer can turn to you, as their MSP or MSSP, to ensure those services are available on demand.

Regardless of where resources are hosted, the defining factor is that they have a cloud-based management plane rather than a control pane on an on-premises device or software stack. At the end of the day, your customer's cloud networking strategy should enable them to:

- Simplify lifecycle management.
- Provide a great user experience.
- Reduce time to market for service rollouts.
- Lower operational costs.
- Reduce risk.

87%
of IT leaders
are embracing multi-cloud environments.[2]

Top cloud challenges across all organizations include managing cloud spend (82%), security (79%), and lack of resources/expertise (78%).[2]

Consider these solutions:

Cisco

- **Cisco Umbrella –** Combine multiple security functions into one cloud-delivered solution that extends data protection to devices, remote users and distributed locations anywhere, enabling you to enforce security and block malicious activity before an internet connection is ever established—no hardware to install or software to manually update.

Fortinet

- **Fortinet FortiSASE –** Empower organizations to consistently apply enterprise-grade security and superior user experience across all edges with a comprehensive single-vendor SASE approach that integrates cloud-delivered SD-WAN connectivity with a cloud-delivered security service edge (SSE) to enable secure access from anywhere to the web, cloud, and applications everywhere.
- **Fortinet Secure SD-WAN –** Get fast, flexible, scalable, and secure SD-WAN—whether on-premises or in the cloud—in one operating system that integrates Fortinet SD-WAN with FortiGate next-generation firewall (NGFW), advanced routing, and zero trust network access (ZTNA) application gateway capabilities.

HPE Aruba Networking

- **Aruba EdgeConnect SD-WAN + SSE –** Improve application performance and dramatically reduce the cost and complexity of building a wide area network (WAN) with a unified secure access service edge (SASE) security platform that enables enterprises to leverage broadband to connect users to applications.
- **Aruba Central –** Leverage a cloud-based networking solution that empowers IT to manage campus, branch, remote, data center and IoT networks from one dashboard with AI-powered insights, intuitive visualizations, workflow automation and edge-to-cloud security.

ZPE Systems

- **Modernized Networking –** Deploy edge virtualization on a platform that utilizes its own and can deploy third-party solutions—such as SD-WAN, User Experience Monitoring, Cloud Access and Hybrid Infrastructure and Platforms and Applications—or make the one you have more resilient with Wireless Backup Networking, ZT Interfaces and recovery systems.

SD-WAN Considerations for Long-Term Work-From-Home (WFH) and Hybrid Environments

SD-WAN Considerations for Long-Term Work-From-Home (WFH) and Hybrid Environments

SD-WAN: Make IoT Work

The Internet of Things (IoT) has revolutionized the way that organizations operate. With 41.76 billion active IoT-connected devices forecasted globally in 2023, Frost & Sullivan expects increased demand for IoT solutions to drive an 18% growth in connections compared to 2022. The main drivers for this expansion include the acceleration of automation, continuing digital transformation initiatives, post-pandemic value chain recovery and 5G connectivity rollouts.[10]

Alongside the growing number of IoT devices is an exponential growth of data and a corresponding increase in network traffic, adding network complexity. Mining a gargantuan lode of IoT data and culling it into intelligent and actionable insights also requires massive processing power.

At the same time, the growing raft of entry points onto the network requires more robust security measures and overall network management to better streamline ongoing operations and policy orchestration. Fortunately, a software-defined wide area network (SD-WAN) answers this growing network complexity.

41.76 BILLION

active IoT-connected devices forecasted globally in 2023[10]

Consider these solutions:

Cisco

- **Cisco Catalyst SD-WAN -** connects any user to any application with integrated capabilities for multi-cloud, security, predictive operations and enhanced network visibility —all on a SASE-enabled architecture. Cisco Catalyst SD-WAN enables you to transform your IT infrastructure by delivering network connectivity that's cloud-agnostic, efficient and simpler to manage, lowers operational costs and increases control and visibility across the entire digital service delivery chain.
- **Cisco Umbrella –** Combine multiple security functions into one cloud-delivered solution that extends data protection to devices, remote users, and distributed locations anywhere, enabling you to enforce security and block malicious activity before an internet connection is ever established—no hardware to install or software to manually update. Cisco Umbrella is fully integrated with Catalyst SD-WAN. The integration between Cisco Catalyst SD-WAN and Umbrella enables networking and security convergence capabilities that accelerate the transition to a SASE architecture in a secure and agile manner.
- **Cisco Duo –** Use multi-factor authentication to protect your organization's data wherever users are logging in—for every access attempt and from any device or location—by verifying user trust, establishing device trust and providing secure access to company apps and networks.

Fortinet

- **Fortinet Secure SD-WAN –** Get fast, flexible, scalable and secure SD-WAN—whether on-premises or in the cloud—in one operating system that integrates Fortinet SD-WAN with FortiGate next-generation firewall (NGFW), advanced routing and ZTNA application gateway capabilities.
- **Fortinet FortiSASE –** Empower organizations to consistently apply enterprise-grade security and superior user experience across all edges with a comprehensive single-vendor SASE approach that integrates cloud-delivered SD-WAN connectivity with a cloud-delivered security service edge (SSE) to enable secure access from anywhere to the web, cloud, and applications everywhere.

HPE Aruba Networking

- **Aruba EdgeConnect SD-WAN + SSE –** Improve application performance and dramatically reduce the cost and complexity of building a wide area network (WAN) with a unified secure access service edge (SASE) security platform that enables enterprises to leverage broadband to connect users to applications.
- **Aruba Central –** Leverage a cloud-based networking solution that empowers IT to manage campus, branch, remote, data center and IoT networks from one dashboard with AI-powered insights, intuitive visualizations, workflow automation and edge-to-cloud security.

ZPE Systems

- **Modernized Networking –** Deploy edge virtualization on a platform that utilizes its own and can deploy third-party solutions—such as SD-WAN, User Experience Monitoring, Cloud Access and Hybrid Infrastructure and Platforms and Applications—or make the one you have more resilient with Wireless Backup Networking,
ZT Interfaces and recovery systems.

Cloud Networking: The "New Normal" in Networking

SD-WAN Considerations for Long-Term Work-From-Home (WFH) and Hybrid Environments

SD-WAN: Make IoT Work

Cloud Networking: The "New Normal" in Networking

Having the right network architecture to manage the unique scalability and connectivity challenges that IoT presents is critical to your customer's success. As organizations continue to embrace IoT, SD-WAN can play a foundational role with cost-effective, secure, and easily manageable network connectivity. Software-based SD-WANs reduce the number of network devices and connections required at each site, simplifying network complexity and reducing costs. You can also use software to remotely configure and customize SD-WANs to quickly adapt to changing business needs and perform ongoing system updates. Here are three reasons why SD-WANs make it easier for your customer to scale their IoT initiatives—and what your customer should seek in a platform:

1 **Visibility –** With multiple locations connecting potentially thousands of IoT devices, real-time visibility into the network is critical. SD-WAN provides single-pane-of-glass management with real-time visibility into network performance, simplifying network management and enabling more accurate issue resolution. And with centralized, cloud-based policy administration, your customer can better address dynamic traffic flows and orchestrate policies to ensure network resilience.

2 **Security –** Connecting IoT devices to the Internet opens the door to potential security vulnerabilities; yet, ensuring end-to-end security can quickly tax resource-constrained IT teams. SD-WAN typically provides unified threat management that includes SASE and SSE technologies (firewall, ZTNA, SWG) as well as CASB and MDR, dynamic AES-encrypted tunnels, web and app filtering, SIEM, SSL and intrusion detection/prevention, and antivirus/antimalware/antispyware software. Your customer can also usesegmentation to isolate IoT traffic from other application traffic to limit the attack surface and use role-based access control for stronger security policy enforcement.

3 **Agility –** Your customer needs to quickly deploy IoT devices and SD-WAN makes it easy with zero-touch provisioning, which automates device connection and management. Plus, as a cloud-managed service, SD-WAN simplifies enterprise-wide deployments by eliminating the need to manage and maintain centralized SD-WAN data centers.

It's important to note that SD WAN is only one component of your customer's security architecture. Although leading SD-WAN solutions have been designed with zero trust in mind, it's important to make sure that the following security best practices have been implemented into your customer's environment:

- Strongest possible end-to-end encryption.
- Secure web gateways integrated with next-generation firewalls.
- Network threat intrusion detection and real-time monitoring.
- Regular vulnerability assessments and penetration tests.
- Regular architecture reviews with comparison to reference architectures.

Consider these solutions:

Cisco

- **Cisco Catalyst SD-WAN -** connects any user to any application with integrated capabilities for multi-cloud, security, predictive operations and enhanced network visibility —all on a SASE-enabled architecture. Cisco Catalyst SD-WAN enables you to transform your IT infrastructure by delivering network connectivity that's cloud-agnostic, efficient and simpler to manage, lowers operational costs and increases control and visibility across the entire digital service delivery chain.
- **Cisco Umbrella –** Combine multiple security functions into one cloud-delivered solution that extends data protection to devices, remote users, and distributed locations anywhere, enabling you to enforce security and block malicious activity before an internet connection is ever established—no hardware to install or software to manually update. Cisco Umbrella is fully integrated with Catalyst SD-WAN. The integration between Cisco Catalyst SD-WAN and Umbrella enables networking and security convergence capabilities that accelerate the transition to a SASE architecture in a secure and agile manner.
- **Cisco Duo –** Use multi-factor authentication to protect your organization's data wherever users are logging in—for every access attempt and from any device or location—by verifying user trust, establishing device trust and providing secure access to company apps and networks.

Fortinet

- **Fortinet Secure SD-WAN –** Get fast, flexible, scalable and secure SD-WAN—whether on-premises or in the cloud—in one operating system that integrates Fortinet SD-WAN with FortiGate next-generation firewall (NGFW), advanced routing and ZTNA application gateway capabilities.
- **Fortinet FortiSASE –** Empower organizations to consistently apply enterprise-grade security and superior user experience across all edges with a comprehensive single-vendor SASE approach that integrates cloud-delivered SD-WAN connectivity with a cloud-delivered security service edge (SSE) to enable secure access from anywhere to the web, cloud, and applications everywhere.

HPE Aruba Networking

- **Aruba EdgeConnect SD-WAN + SSE –** Improve application performance and dramatically reduce the cost and complexity of building a wide area network (WAN) with a unified secure access service edge (SASE) security platform that enables enterprises to leverage broadband to connect users to applications.
- **Aruba Central –** Leverage a cloud-based networking solution that empowers IT to manage campus, branch, remote, data center and IoT networks from one dashboard with AI-powered insights, intuitive visualizations, workflow automation and edge-to-cloud security.

ZPE Systems

- **Modernized Networking –** Deploy edge virtualization on a platform that utilizes its own and can deploy third-party solutions—such as SD-WAN, User Experience Monitoring, Cloud Access and Hybrid Infrastructure and Platforms and Applications—or make the one you have more resilient with Wireless Backup Networking,
ZT Interfaces and recovery systems.

AI & Cybersecurity: Fight Fire With Fire

AI & Cybersecurity: Fight Fire With Fire

AI Power at Your Fingertips

The attack surface in today's organizations is massive and fast-growing. Cybercriminals are launching new and more sophisticated attacks every day. Human intervention is no longer enough (was it ever?). AI and machine learning are becoming essential weapons in the fight against cybercrime. New research suggests that 82% of IT leaders plan to invest in AI-driven cybersecurity in the next two years and almost half plan to invest before the end of 2023.[11]

Help your customer fight AI-based attacks with AI-powered tools that can quickly analyze millions of data sets and detect a variety of threats with attack potential. These technologies draw on past experiences to continually learn and, leveraging present-day data, pinpoint new varieties of attacks seeking a crack in your customer's wall.

Here are some use cases12 for your customer:

- **Detect New Threats –** Compared to traditional software systems, AI leverages sophisticated algorithms to spot cyber threats and potentially malicious activities. These systems "learn" to detect malware, run pattern recognition and find even the most insignificant behaviors of malware or ransomware attacks before they enter your customer's system.

- **Battle Bots –** Bots make up a large portion of internet traffic today with some engaging in potentially dangerous activities—from account takeovers with stolen credentials to bogus account creation and data fraud.

  AI and machine learning help build a thorough understanding of website traffic, enabling it to distinguish between good bots, bad bots and humans. By analyzing a vast amount of data, your customer can adapt their strategy to a fast-changing landscape. For example, your customer can intervene in a bad bots' intentions by assessing behavioral patterns and answering questions like "what does an average user journey look like?" or "what does an unusual journey look like?"

- **Protect Against Breaches –** AI can combine your customer's IT asset inventory—devices, users and applications—with their levels of access to predict how and where they are most likely to be compromised. With this information, they can allocate resources toward areas of greatest vulnerability. Prescriptive insights from AI-based analysis allow your customer to configure and improve controls and processes to reinforce their cyber resilience.

- **Provide Better Endpoint Protection –** AI has a crucial role to play in securing the growing number of endpoints used by work-from-home employees. Where antivirus solutions and VPNs typically use signatures, they may not be effective against malware and ransomware attacks, particularly if the vendor is not aware of a new attack signature or your customer fails to update their software.

  AI-driven endpoint protection establishes a baseline of behavior for the endpoint through repeated learning. If something out of the ordinary occurs, AI can flag it, allowing your customer to act proactively—whether it's sending a notification to a technician or reverting to a safe state after a ransomware attack.

Finally, AI could be the answer to today's worldwide cybersecurity talent shortage and skills gaps. Finding those skills is hard enough. But many smaller organizations—such as local municipalities, small businesses, K-12 districts and nonprofits—lack the resources to even pay for that kind of talent. If AI can be leveraged to detect potential threats, it frees up their IT teams to assess them and act decisively. Or you can use AI to help them manage their cybersecurity posture.

Consider these solutions:

Cisco

- **Cisco Umbrella –** Combine multiple security functions into one cloud-delivered solution that extends data protection to devices, remote users and distributed locations anywhere, enabling you to enforce security and block malicious activity before an internet connection is ever established—no hardware to install or software to manually update.

Fortinet

- **Fortinet Universal ZTNA –** Quickly deploy a robust and reliable ZTNA solution with a low total cost of ownership (TCO) with on premises, cloud-based and hybrid options.
- **Fortinet FortiSASE –** Empower organizations to consistently apply enterprise-grade security and superior user experience across all edges with a comprehensive single-vendor SASE approach that integrates cloud-delivered SD-WAN connectivity with a cloud-delivered security service edge (SSE) to enable secure access from anywhere to the web, cloud, and applications everywhere.
- **Fortinet Secure SD-WAN –** Get fast, flexible, scalable and secure SD-WAN—whether on-premises or in the cloud—in one operating system that integrates Fortinet SD-WAN with FortiGate next-generation firewall (NGFW), advanced routing and ZTNA application gateway capabilities.

ZPE Systems

- **Advanced Threat Intelligence –** Deploy the Nodegrid platform to manage a fleet of deployed IoT and AI edge services with Out of Band Management—it can cut organizational risk by supporting large fleets with cyber physical means: power and serial access.

AI & Cybersecurity: Fight Fire With Fire

AI Power at Your Fingertips

Generative AI and Cybersecurity

Generative AI allows users to leverage intelligent models to generate new content, including text, images, video and audio. Nearly all organizations have used—or are considering using—generative AI (e.g., ChatGPT) to support business workflows and daily operations.

But while generative AI can be used for malintent—for example, creating a phishing email—it can also be used to strategically benefit your customer's cybersecurity posture. Here are some ideas for fast wins for your customer:[13]

- **Scenario-Driven Cybersecurity Training –** Use synthetic data and other features to generate simulated attacks, scenarios, and environments for cybersecurity training (e.g., The TD SYNNEX Cyber Range).
- **Synthetic Data Generation –** Securely generate anonymized data copies for AI and software app development.
- **Contextualized Security Monitoring, Reporting and Recommendations –** Help your customer search existing code and networks for vulnerabilities and provide contextualized recommendations for remediation.
- **Supply Chain and Third-Party Risk Management –** Support risk management, predictive maintenance, fraud detection, relationship management, and other components of supply chain and partner cybersecurity management.
- **Threat Intelligence and Hunting –** Assess massive amounts of data simultaneously, looking for security vulnerabilities and bigger issues. Some tools can also make recommendations about what tools your customer should use and infrastructure changes they should make for better security outcomes.

51%
of IT leaders
believe there will be a successful cyberattack credited to ChatGPT this year.[11]

71%
believe that foreign states
are likely using ChatGPT for malicious purposes against other nations.[11]

Consider these solutions:

Cisco

- **Cisco Umbrella –** Combine multiple security functions into one cloud-delivered solution that extends data protection to devices, remote users and distributed locations anywhere, enabling you to enforce security and block malicious activity before an internet connection is ever established—no hardware to install or software to manually update.

Fortinet

- **Fortinet Universal ZTNA –** Quickly deploy a robust and reliable ZTNA solution with a low total cost of ownership (TCO) with on premises, cloud-based and hybrid options.
- **Fortinet FortiSASE –** Empower organizations to consistently apply enterprise-grade security and superior user experience across all edges with a comprehensive single-vendor SASE approach that integrates cloud-delivered SD-WAN connectivity with a cloud-delivered security service edge (SSE) to enable secure access from anywhere to the web, cloud, and applications everywhere.
- **Fortinet Secure SD-WAN –** Get fast, flexible, scalable and secure SD-WAN—whether on-premises or in the cloud—in one operating system that integrates Fortinet SD-WAN with FortiGate next-generation firewall (NGFW), advanced routing and ZTNA application gateway capabilities.

ZPE Systems

- **Advanced Threat Intelligence –** Deploy the Nodegrid platform to manage a fleet of deployed IoT and AI edge services with Out of Band Management—it can cut organizational risk by supporting large fleets with cyber physical means: power and serial access.

Security Solutions: Build in Zero Trust

Zero trust is at the top of the list for today's organizations, but few know where to start their zero-trust journey. The first step is to help your customer build an effective zero-trust strategy that balances security with business needs. With a defined strategy in place, you can begin to lay a zero-trust foundation that starts with identity. From there, tweak the people and processes to build and manage those identities. Here are some ideas to create fast wins for your customer:

- **Identity Security –** Zero trust assumes that any identity with access to applications and systems may have already been compromised. As the backbone of a zero-trust approach, identity security requires that every user is verified, every device validated, and privileged access is limited. In essence, these solutions enable your customer to focus on identifying, isolating, and stopping threats from compromising identities and gaining privilege before they can do damage. With these tools, you can deliver a unified approach with seamless and secure access for all identities, intelligent privilege controls, flexible identity automation and orchestration, and continuous threat detection and protection.
- **Identity And Access Management (IAM) –** With today's boundless networks, knowing who and what is on the network and why is fundamental to a zero-trust strategy. Help your customer set and enforce policies for who has access to what and continuously verify identities to ensure that only authorized users have access to sensitive systems and resources. IAM tools typically include user provisioning, access control and identity federation and, with single sign-on, enables users to access multiple resources with a single set of credentials. IAM technologies can also detect instances of unauthorized activity, enabling your customer to not only prevent potential security breaches, but also to meet compliance requirements.
- **Privileged Access Management (PAM) –** With an increasing number of insider threats, your customer must control access to applications, endpoints, critical infrastructure (e.g., firewalls and routers), and sensitive data throughout their organization. PAM platforms provide a single pane of glass for zero-trust privilege management, enabling your customer to monitor every user, device and network for complete control over who gets access to what. Users are segmented into tiers based on the resources they need to access. With appropriate rights granted to each individual, PAM tools can then use advanced machine learning algorithms to identify anomalies across applications and devices and automatically block suspicious behavior.
- **Endpoint Detection and Response (EDR)/Extended Detection and Response (XDR) –** Where EDR solutions focus only on endpoints, XDR strategies focus on endpoints, as well as networks, cloud workloads and more. They consolidate security products across layers to automate threat detection and use threat intelligence feeds and advanced analytics to detect and prevent potential attacks. And, with "learned" intelligence and synergistic analysis from multiple sources and security layers, XDR solutions can update security policies to block any future attacks. By leveraging continuous event monitoring across all security operations, XDR acts as the "central nervous system" of your customer's zero-trust strategy to deliver threat detection in real time.

By 2026,

10%

of large enterprises

will have a mature and measurable zero-trust program in place, up from less than 1% today.[15]

- **Multi-Factor Authentication (MFA) –** Zero-trust architectures call for implementing MFA which requires users to continually authenticate themselves to access a requested resource by providing two or more authentication factors. With MFA, it's much more difficult for bad actors to gain access and integrating MFA with an IAM system adds yet another layer of security to your customer's environment.

More recent risk-based MFA solutions use machine learning to dynamically assess user risk based their location, behavior, security posture of the device, Wi-Fi network and the use of known attack patterns. In other words, low-risk users can login with a simple authentication process that still meets the needs of zero trust, but high-risk users must take additional steps to reduce the chance of breaches.

- **Cloud Security –** Highly virtualized and converged workloads, as well as dynamic public cloud workloads, often move between on-premises and external cloud service environments or between segments within a cloud service provider environment. This security model calls for network and application layer micro-segmentation to move the perimeter as close as possible to privileged apps and protected surface areas. To implement zero-trust cloud security, you'll want to focus on:

  (1) Integrate security into the workloads themselves so that policy enforcement travels with workloads wherever they go.

  (2) Adopt a zero-trust micro-segmentation strategy that allows traffic to flow between approved systems and connections, regardless of the environment they are in, which will likely require defining both network and identity policy to allow communications and behaviors.

This micro-segmentation prevents attackers from using unapproved connections to move laterally from a compromised application or system, regardless of environment.

Effective zero-trust control technology will also include some machine learning capabilities to perform analytics processing of attempted behaviors. The technology adapts dynamically over time to changes in the workloads and application environments.

Consider these solutions:

ActZero

- **ActZero Full-Stack Cybersecurity –** Get a powerful full-stack cybersecurity solution at a fair price.
- **ActZero MDR –** Cut the number of alerts/false positives and secure endpoints, network, mobile devices, cloud, identity, and email accounts with 24/7 SOC and live support, on-demand dedicated security advisor, access to ActZero's MDR platform and AI-powered auto-blocking, high-fidelity detections and managed remediation.

Cisco

- **Cisco XDR –** Collect and correlate data and provide visibility across email, endpoints, servers, cloud workloads, and networks, and apply analytics and automation to detect, analyze, hunt, and remediate today's and tomorrow's threats.
- **Cisco Duo –** Use multi-factor authentication to protect your organization's data wherever users are logging in—for every access attempt and from any device or location—by verifying user trust, establishing device trust and providing secure access to company apps and networks.

CyberArk

- **CyberArk Secure Remote Workforce Access–** Secure remote workforce access with multi-factor authentication, single sign-on and endpoint privileged management—no VPNs, agents or passwords needed.
- **CyberArk Endpoint Privilege Manager –** Remove local admin rights, enforce least privilege, and implement foundational endpoint security controls across all Windows, macOS, and Linux endpoints, from hybrid to cloud environments.
- **CyberArk Privileged Access Manager –** Reduce risk and enable secure access to critical internal resources for remote employees and external vendors using biometric multi-factor authentication—without VPNs, passwords or agents.

Fortinet

- **Fortinet Universal ZTNA –** Quickly deploy a robust and reliable ZTNA solution with a low total cost of ownership (TCO) with on premises, cloud-based and hybrid options.
- **Fortinet FortiSASE –** Empower organizations to consistently apply enterprise-grade security and superior user experience across all edges with a comprehensive single-vendor SASE approach that integrates cloud-delivered SD-WAN connectivity with a cloud-delivered security service edge (SSE) to enable secure access from anywhere to the web, cloud and applications everywhere.

ZPE Systems

- **Zero Trust Strategy with ZPE Systems –** Zero trust requires control and that starts by quickly and easily deploying in a ZT environment with the Nodegrid platform to enable Identity Security, Identity Access Management, Privileged Access Management, XDR, Multi-factor authentication (MFA), Cloud Access, Isolated Management, and Resilience and Recovery.

Networking Solutions: Make the Connection

There are, of course, challenges to modernizing your customer's networks, including network complexity, a proliferation of legacy technologies/expertise/processes, lack of training in skills needed for modern networks, performance and end-user experience issues, inability to quickly scale and gaps in security and overall visibility. A modern network will provide faster time to market, a better end-user experience, greater simplicity and operational efficiency, higher levels of availability, seamless connectivity, greater job satisfaction across the organization and ultimately, a more secure environment. Here are some ways to create fast wins for your customer:

- **Modern Networks –** In today's highly distributed environments, an efficient application-centric modern network is more important than ever. Consider these seven steps16 to help your customer modernize and future-proof their network:
  1. Take a Top-Down Approach—break down silos and unite business and IT teams with business goals to achieve the desired return on investment.
  2. Help Them Invest in Managed Services that can move them from legacy network assets to an agile and secure network—both to reduce technical debt and enable greater availability, scalability, and performance.
  3. Consider the Network-As-A-Service (NaaS) Model to move the organization forward by using and paying for only what's needed while accessing emerging technologies.
  4. Help Your Customer Embrace New Tools like AIOps in the pursuit of an agile network instead of investing and/or building their own.
  5. Evolve And Manage Their Network and improve its output by bringing their network and operational technology together for an end-to-end approach.
  6. Consider Changing Security And Regulatory Requirements (specifically regarding data privacy) and how they will affect your customer's network.
  7. Make Sure Your Customer Clearly Understands Your Costs by sharing your capabilities, track record, client relationships and governance models.
- **SD-WAN –** In a cloud-native world, traditional WAN simply can't handle the unprecedented traffic brought on by cloud adoption. SD-WAN takes a software-defined approach to solve multiple challenges associated with traditional WAN, such as lowering operational costs, improving resource usage for multi-site deployments and ensuring bandwidth efficiency without sacrificing security or data privacy. And automated operations and cloud-based management provide greater management simplicity.
- **User Experience Monitoring –** For IT teams, networks have traditionally conjured up images of hardware and software and "feeds and speeds." But for your customer's end-users, networks are what hang up their applications and keep them from being productive. Today's modern networks can give end-users the reliable, seamless application experience they want—regardless of the application they're using or the location they're accessing it from. User experience monitoring allows your customer to measure the impact of overall performance from the end user's perspective.
- **Cloud Solutions –** The cloud is changing the networking paradigm. While there's freedom in the ability to move workloads between public/private/hybrid clouds, it can quickly become a management nightmare. Your customer may not own the connections or it may be challenging to apply network protocols or security policies to an ever-changing network environment. Both applications and network functions are now moving to the cloud. This helps organizations scale up and down, but managing the network as a cloud function is different than a traditional network and not every organization can evolve from their current skillset to new requirements.
- **Platforms and Applications –** Finally, there are a variety of network management tools and applications to optimize performance, cut costs, deliver a better end-user experience and so on. Check with your TD SYNNEX representative for more information on options.

Top Five Reasons to Run Applications in a Hybrid Cloud Environment[17]

51% Increased Performance

48% Improved Security

45% Reduced IT Infrastructure

44% Improved Data Protection/Disaster Recovery

44% Improved User Productivity

***"Increasingly, networks have moved away from being just a hygiene factor to actually being true differentiators, and the businesses that recognize this outperform their peers."*[16]**

Nearly 9 in 10 organizations say they need a third party to fulfill their network needs and stay ahead of change, network innovation, and internal skills gaps.[16]

Consider these solutions:

ActZero

- **ActZero MDR –** Cut the number of alerts/false positives and secure endpoints, network, mobile devices, cloud, identity, and email accounts with 24/7 SOC and live support, on-demand dedicated security advisor, access to ActZero's MDR platform and AI-powered auto-blocking, high-fidelity detections and managed remediation.

Cisco

- **Cisco XDR –** Collect and correlate data and provide visibility across email, endpoints, servers, cloud workloads, and networks, and apply analytics and automation to detect, analyze, hunt, and remediate today's and tomorrow's threats.
- **Cisco Umbrella –** Combine multiple security functions into one cloud-delivered solution that extends data protection to devices, remote users and distributed locations anywhere, enabling you to enforce security and block malicious activity before an internet connection is ever established—no hardware to install or software to manually update.

Fortinet

- **Fortinet Universal ZTNA –** Quickly deploy a robust and reliable ZTNA solution with a low total cost of ownership (TCO) with on premises, cloud-based and hybrid options.
- **Fortinet FortiSASE –** Empower organizations to consistently apply enterprise-grade security and superior user experience across all edges with a comprehensive single-vendor SASE approach that integrates cloud-delivered SD-WAN connectivity with a cloud-delivered security service edge (SSE) to enable secure access from anywhere to the web, cloud and applications everywhere.
- **Fortinet Secure SD-WAN –** Get fast, flexible, scalable and secure SD-WAN—whether on-premises or in the cloud—in one operating system that integrates Fortinet SD-WAN with FortiGate next-generation firewall (NGFW), advanced routing and ZTNA application gateway capabilities.

HPE Aruba Networking

- **Aruba EdgeConnect SD-WAN + SSE –** Improve application performance and dramatically reduce the cost and complexity of building a WAN with a unified SASE security platform that enables enterprises to leverage broadband to connect users to applications.
- **Aruba Central –** Leverage a cloud-based networking solution that empowers IT to manage campus, branch, remote, data center, and IoT networks from one dashboard with AI-powered insights, intuitive visualizations, workflow automation and edge-to-cloud security.

- **Fortinet Secure SD-WAN –** Get fast, flexible, scalable and secure SD-WAN—whether on-premises or in the cloud—in one operating system that integrates Fortinet SD-WAN with FortiGate next-generation firewall (NGFW), advanced routing and ZTNA application gateway capabilities.

Opengear

- **Opengear Operations Manager (OM) 1200/2200 Console Servers –** Create a secure management plane for administrators with the OM series, featuring Smart Out-of-BandTM management and network automation—perfect for datacenters and edge sites.
- **Opengear Console Manager (CM) 8100 Console Server –** Manage high-density datacenters with the Smart Out-of-Band™ management and energy-efficient capabilities found in the CM8100.
- **Opengear Console Manager (CM) 8100 Console Server –** Manage high-density datacenters with the Smart Out-of-Band™ management and energy-efficient capabilities found in the CM8100.

ZPE Systems

- **Modernized networking –** Deploy Edge virtualization on a platform that utilizes its own and can deploy third-party solutions—such as SD-WAN, User Experience Monitoring, Cloud Access and Hybrid Infrastructure, and Platforms and Applications—or make the one you have more resilient with Wireless Backup Networking, ZT Interfaces, and recovery systems.

Human Error in Cybersecurity: Embrace Awareness

Human Error in Cybersecurity: Embrace Awareness

The Human Element

The consequences of human error in cybersecurity are high. According to a recent report, 74% of all breaches include the human element, with people being involved either via error, privilege misuse, use of stolen credentials, or social engineering.[19] These are not malicious actors. Rather, human error comprises unforced errors by individuals.

Employees at every level of an organization can make mistakes, such as using weak passwords or sharing passwords, losing devices with sensitive data, accessing unsafe websites, opening unsafe emails, misconfiguring tools and sending a confidential email to the wrong person. Inadequate training can open the door for bad actors to circumvent technical safeguards and launch an attack. Here are some things to consider:

- **Phishing and Social Engineering –** In social engineering attacks, the attackers use their social skills to get or compromise information about their target organization or its computer systems. Typically, these attackers rely on the good graces and helpfulness of humans to get the information they seek. In fact, social engineering attacks are quite effective and extremely lucrative for cybercriminals.

  Phishing is a form of social engineering that, according to a recent report, was the most common initial attack vector for 16% of attacks.[20] These attacks typically use email or malicious websites to portray themselves as trustworthy and to steal personal information. They can be easily identified by their strange greetings, misspellings, poor grammar, urgent requests or nonsensical URLs. The goal is to reach that one person who fails, for whatever reason, to recognize potential fraud.

- **ChatGPT –** You can ask ChatGPT to write a "phishing" email and they will politely decline. But that hasn't stopped bad actors from politely asking it to write a convincing email that gets users to click on a malicious link.

  And with advances in AI, it's becoming increasingly difficult for users to differentiate between a legitimate email and one produced by ChatGPT. The good news for your customer is that ChatGPT can also turn dull employee missives on security awareness into customized communications that improve engagement, readability and comprehension—and can be easily shared on a collaboration platform.

26%
of employees
said they had fallen for a phishing scam at work in the last 12 months,
up from 25% in 2020.[21]

Consider these solutions:

ActZero

- **ActZero Full-Stack Cybersecurity –** Get a powerful full-stack cybersecurity solution at a fair price.
- **ActZero MDR –** Cut the number of alerts/false positives and secure endpoints, network, mobile devices, cloud, identity, and email accounts with 24/7 SOC and live support, on-demand dedicated security advisor, access to ActZero's MDR platform and AI-powered auto-blocking, high-fidelity detections and managed remediation.

Cisco

- **Cisco XDR –** Collect and correlate data and provide visibility across email, endpoints, servers, cloud workloads, and networks, and apply analytics and automation to detect, analyze, hunt, and remediate today's and tomorrow's threats.
- **Cisco Umbrella –** Combine multiple security functions into one cloud-delivered solution that extends data protection to devices, remote users and distributed locations anywhere, enabling you to enforce security and block malicious activity before an internet connection is ever established—no hardware to install or software to manually update.

CyberArk

- **CyberArk Endpoint Privilege Manager –** Remove local admin rights, enforce least privilege, and implement foundational endpoint security controls across all Windows, macOS, and Linux endpoints, from hybrid to cloud environments.
- **CyberArk Privileged Access Manager –** Reduce risk and enable secure access to critical internal resources for remote employees and external vendors using biometric multi-factor authentication—without VPNs, passwords or agents.

Build a Security-First Culture

Human Error in Cybersecurity: Embrace Awareness

The Human Element

Build a Security-First Culture

We get it, forcing end-users to periodically attend security awareness training when they've got other things to do usually doesn't work out very well. So, how can you help your customer build a security-first culture? Start by engaging employees in a common cause.

- **Security Is Everyone's Job –** Many believe that the job of security falls on the IT team. In fact, security is everyone's job. One way to share the responsibility is to instill security into the organization's overall mission, ensure all C-suite executives "own" and talk about security, and make it a non-negotiable. Employees need to feel "all in" on security.
- **Focus On Awareness, PLUS –** Because employees want to do the right thing, test their knowledge following an awareness program and hold them accountable for decisions they make after learning the material. Not only should you teach your team security basics, but they should also have basic knowledge of threats so they can fairly judge the depth of threats. Finally, create teachable moments. Talk openly about the impact of decisions made by employees and about the impact of security incidents and breaches on the organization.
- **Reward and Recognize –** Every milestone should be recognized and rewarded. Complete mandatory security awareness training, get recognized or rewarded. Record a teachable moment for your peers, get rewarded. And instead of balking at the idea of "meaningful" rewards, consider the value of preventing a data breach for a relatively small investment.
- **Build a Community –** Connect and unite people from across the organization with different interests in security against a common problem. Some may be passionate about security, some may understand the value of security and some may be leaders who direct security efforts. This group can meet periodically to discuss the latest security issues and develop ways to engage, recognize and reward employees.
- **Make Security Fun –** Security isn't boring and awareness training shouldn't be boring either. Skip the sleep-inducing PowerPoint and build fun and engagement into security awareness. Share the learning materials with employees and ask them to create a talent show, a dramatic or comedic presentation, or a trivia or other game. Give out prizes (best phishing costume?) for those who hit the mark.

26%
of employees
said they had fallen for a phishing scam at work in the last 12 months, **up from 25% in 2020.**[21]

Consider these solutions:

ActZero

- **ActZero Full-Stack Cybersecurity –** Get a powerful full-stack cybersecurity solution at a fair price.
- **ActZero MDR –** Cut the number of alerts/false positives and secure endpoints, network, mobile devices, cloud, identity, and email accounts with 24/7 SOC and live support, on-demand dedicated security advisor, access to ActZero's MDR platform and AI-powered auto-blocking, high-fidelity detections and managed remediation.

Cisco

- **Cisco XDR –** Collect and correlate data and provide visibility across email, endpoints, servers, cloud workloads, and networks, and apply analytics and automation to detect, analyze, hunt, and remediate today's and tomorrow's threats.
- **Cisco Umbrella –** Combine multiple security functions into one cloud-delivered solution that extends data protection to devices, remote users and distributed locations anywhere, enabling you to enforce security and block malicious activity before an internet connection is ever established—no hardware to install or software to manually update.

CyberArk

- **CyberArk Endpoint Privilege Manager –** Remove local admin rights, enforce least privilege, and implement foundational endpoint security controls across all Windows, macOS, and Linux endpoints, from hybrid to cloud environments.
- **CyberArk Privileged Access Manager –** Reduce risk and enable secure access to critical internal resources for remote employees and external vendors using biometric multi-factor authentication—without VPNs, passwords or agents.

Opportunities for MSPs & MSSPs

Your customers require a new security approach as they seek to move from perimeter-based security to zero trust to help protect against targeted threats and improve business performance. It can also mitigate supply chain risk and secure cloud environments. Is your customer ready to take their first steps? Start by offering these services:

1 Build a Zero-Trust Roadmap

Success starts with a comprehensive zero-trust roadmap that outlines the activities needed to implement your customer's zero-trust strategy. This strategy document will provide a clear view of the deliverables, budget, and business outcomes expected.

- Determine a framework, whether it's the NIST or CISA framework or a framework from Gartner, Forrester, or others. TD SYNNEX can help you select the right vendors to help you craft a zero-trust vision.
- Identify interdependencies between the zero-trust implementation and other IT and b usiness projects.
- Recruit business and IT stakeholders—from IT operators to enterprise architects to business unit leaders to C-suite executives—who can help build your customer's zero trust roadmap and evangelize the need for new or shifting investments or significant cultural and organizational change.

2 3 4 5

Consider these solutions:

Cisco

- **Cisco XDR –** Collect and correlate data and provide visibility across email, endpoints, servers, cloud workloads, and networks, and apply analytics and automation to detect, analyze, hunt, and remediate today's and tomorrow's threats.
- **Cisco Umbrella –** Combine multiple security functions into one cloud-delivered solution that extends data protection to devices, remote users and distributed locations anywhere, enabling you to enforce security and block malicious activity before an internet connection is ever established—no hardware to install or software to manually update.
- **Cisco Duo –** Use multi-factor authentication to protect your organization's data wherever users are logging in—for every access attempt and from any device or location—by verifying user trust, establishing device trust and providing secure access to company apps and networks

CyberArk

- **CyberArk Secure Remote Workforce Access –** Secure remote workforce access with multi-factor authentication, single sign-on and endpoint privileged management—no VPNs, agents or passwords needed.
- **CyberArk Endpoint Privilege Manager –** Remove local admin rights, enforce least privilege, and implement foundational endpoint security controls across all Windows, macOS, and Linux endpoints, from hybrid to cloud environments.
- **CyberArk Privileged Access Manager –** Reduce risk and enable secure access to critical internal resources for remote employees and external vendors using biometric multi-factor authentication—without VPNs, passwords or agents.

Fortinet

- **Fortinet Universal ZTNA –** Quickly deploy a robust and reliable ZTNA solution with a low total cost of ownership (TCO) with on premises, cloud-based and hybrid options.
- **Fortinet FortiSASE –** Empower organizations to consistently apply enterprise-grade security and superior user experience across all edges with a comprehensive single-vendor SASE approach that integrates cloud-delivered SD-WAN connectivity with a cloud-delivered security service edge (SSE) to enable secure access from anywhere to the web, cloud and applications everywhere.
- **Fortinet Secure SD-WAN –** Get fast, flexible, scalable and secure SD-WAN—whether on-premises or in the cloud—in one operating system that integrates Fortinet SD-WAN with FortiGate next-generation firewall (NGFW), advanced routing and ZTNA application gateway capabilities.

HPE Aruba Networking

- **Aruba EdgeConnect SD-WAN + SSE –** Improve application performance and dramatically reduce the cost and complexity of building a WAN with a unified SASE security platform that enables enterprises to leverage broadband to connect users to applications.
- **Aruba Central –** Leverage a cloud-based networking solution that empowers IT to manage campus, branch, remote, data center, and IoT networks from one dashboard with AI-powered insights, intuitive visualizations, workflow automation and edge-to-cloud security.
- **Aruba ClearPass –** Enable IT managers to profile devices, deploy network policies, manage guest access, secure BYOD onboarding and check device health for zero trust security.

Opengear

- **Opengear Operations Manager (OM) 1200/2200 Console Servers –** Create a secure management plane for administrators with the OM series, featuring Smart Out-of-Band™ management and network automation—perfect for datacenters and edge sites.
- **Opengear Console Manager (CM) 8100 Console Server –** Manage high-density datacenters with the Smart Out-of-Band™ management and energy-efficient capabilities found in the CM8100.
- **Opengear Lighthouse –** Get unmatched visibility of distributed networks and proximity to critical devices through a centralized, single pane of control—built with multi-instance capabilities and designed for everyday use with security, scalability and automation.

ZPE Systems

- **Advanced threat intelligence –** Deploy the Nodegrid platform to manage a fleet of deployed IoT and AI edge services with Out of Band Management—it can cut organizational risk by supporting large fleets with cyber physical means: power and serial access.
- **Zero Trust Strategy With ZPE Systems –** Zero trust requires control and that starts by quickly and easily deploying in a ZT environment with the Nodegrid platform to enable Identity Security, Identity Access Management, Privileged Access Management, XDR, Multi-factor authentication (MFA), Cloud Access, Isolated Management and Resilience and Recovery.
- **Modernized networking –**Deploy Edge virtualization on a platform that utilizes its own and can deploy third-party solutions—such as SD-WAN, User Experience Monitoring, Cloud Access and Hybrid Infrastructure, and Platforms and Applications—or make the one you have more resilient with Wireless Backup Networking, ZT Interfaces, and recovery systems.

Opportunities for MSPs & MSSPs

Your customers require a new security approach as they seek to move from perimeter-based security to zero trust to help protect against targeted threats and improve business performance. It can also mitigate supply chain risk and secure cloud environments. Is your customer ready to take their first steps? Start by offering these services:

1 3 4 5

2 Refine the Business Continuity Plan

Every organization today should have a business continuity plan that outlines what happens when (not if) they're attacked. The next step is to help them adopt or periodically stress-test and refine their business continuity plan.

Then, put together an up-to-date inventory of systems and their criticality to make it easy to prioritize actions in case there's a threat or attack. Create playbooks, conduct tabletop exercises, and test backups for critical assets.

The more you can help them prepare, the better off they'll be in the event of a cyberattack or other disaster.

Consider these solutions:

Cisco

- **Cisco XDR –** Collect and correlate data and provide visibility across email, endpoints, servers, cloud workloads, and networks, and apply analytics and automation to detect, analyze, hunt, and remediate today's and tomorrow's threats.
- **Cisco Umbrella –** Combine multiple security functions into one cloud-delivered solution that extends data protection to devices, remote users and distributed locations anywhere, enabling you to enforce security and block malicious activity before an internet connection is ever established—no hardware to install or software to manually update.
- **Cisco Duo –** Use multi-factor authentication to protect your organization's data wherever users are logging in—for every access attempt and from any device or location—by verifying user trust, establishing device trust and providing secure access to company apps and networks

CyberArk

- **CyberArk Secure Remote Workforce Access –** Secure remote workforce access with multi-factor authentication, single sign-on and endpoint privileged management—no VPNs, agents or passwords needed.
- **CyberArk Endpoint Privilege Manager –** Remove local admin rights, enforce least privilege, and implement foundational endpoint security controls across all Windows, macOS, and Linux endpoints, from hybrid to cloud environments.
- **CyberArk Privileged Access Manager –** Reduce risk and enable secure access to critical internal resources for remote employees and external vendors using biometric multi-factor authentication—without VPNs, passwords or agents.

Fortinet

- **Fortinet Universal ZTNA –** Quickly deploy a robust and reliable ZTNA solution with a low total cost of ownership (TCO) with on premises, cloud-based and hybrid options.
- **Fortinet FortiSASE –** Empower organizations to consistently apply enterprise-grade security and superior user experience across all edges with a comprehensive single-vendor SASE approach that integrates cloud-delivered SD-WAN connectivity with a cloud-delivered security service edge (SSE) to enable secure access from anywhere to the web, cloud and applications everywhere.
- **Fortinet Secure SD-WAN –** Get fast, flexible, scalable and secure SD-WAN—whether on-premises or in the cloud—in one operating system that integrates Fortinet SD-WAN with FortiGate next-generation firewall (NGFW), advanced routing and ZTNA application gateway capabilities.

HPE Aruba Networking

- **Aruba EdgeConnect SD-WAN + SSE –** Improve application performance and dramatically reduce the cost and complexity of building a WAN with a unified SASE security platform that enables enterprises to leverage broadband to connect users to applications.
- **Aruba Central –** Leverage a cloud-based networking solution that empowers IT to manage campus, branch, remote, data center, and IoT networks from one dashboard with AI-powered insights, intuitive visualizations, workflow automation and edge-to-cloud security.
- **Aruba ClearPass –** Enable IT managers to profile devices, deploy network policies, manage guest access, secure BYOD onboarding and check device health for zero trust security.

Opengear

- **Opengear Operations Manager (OM) 1200/2200 Console Servers –** Create a secure management plane for administrators with the OM series, featuring Smart Out-of-Band™ management and network automation—perfect for datacenters and edge sites.
- **Opengear Console Manager (CM) 8100 Console Server –** Manage high-density datacenters with the Smart Out-of-Band™ management and energy-efficient capabilities found in the CM8100.
- **Opengear Lighthouse –** Get unmatched visibility of distributed networks and proximity to critical devices through a centralized, single pane of control—built with multi-instance capabilities and designed for everyday use with security, scalability and automation.

ZPE Systems

- **Advanced threat intelligence –** Deploy the Nodegrid platform to manage a fleet of deployed IoT and AI edge services with Out of Band Management—it can cut organizational risk by supporting large fleets with cyber physical means: power and serial access.
- **Zero Trust Strategy With ZPE Systems –** Zero trust requires control and that starts by quickly and easily deploying in a ZT environment with the Nodegrid platform to enable Identity Security, Identity Access Management, Privileged Access Management, XDR, Multi-factor authentication (MFA), Cloud Access, Isolated Management and Resilience and Recovery.
- **Modernized networking –**Deploy Edge virtualization on a platform that utilizes its own and can deploy third-party solutions—such as SD-WAN, User Experience Monitoring, Cloud Access and Hybrid Infrastructure, and Platforms and Applications—or make the one you have more resilient with Wireless Backup Networking, ZT Interfaces, and recovery systems.

Opportunities for MSPs & MSSPs

Your customers require a new security approach as they seek to move from perimeter-based security to zero trust to help protect against targeted threats and improve business performance. It can also mitigate supply chain risk and secure cloud environments. Is your customer ready to take their first steps? Start by offering these services:

1 2

3 Assess Their Environment

4 5

Next, help your customer understand their unique risks by identifying vulnerabilities in their environment and providing recommendations. Take advantage of these assessments:

- **Security Maturity Assessment –** Get a complimentary 45-minute assessment of your customer's security practices and controls and provide a graded report with a customized action plan to improve their security posture.
- **Penetration Testing –** Show them how bad actors exploit their systems to access and disclose sensitive data and how to best prioritize vulnerabilities for remediation.
- **Vulnerability Assessments –** Point out the pathways that attackers use to exploit their systems and provide a complete financial risk analysis with ways to re-allocate limited resources to ensure they're protected.
- **Additional Assessments –** Access additional assessment capabilities, including Security Risk Assessments, Physical Security Assessments, Physical Penetration Testing, GDPR Assessments, and many others.

Consider these solutions:

Cisco

- **Cisco XDR –** Collect and correlate data and provide visibility across email, endpoints, servers, cloud workloads, and networks, and apply analytics and automation to detect, analyze, hunt, and remediate today's and tomorrow's threats.
- **Cisco Umbrella –** Combine multiple security functions into one cloud-delivered solution that extends data protection to devices, remote users and distributed locations anywhere, enabling you to enforce security and block malicious activity before an internet connection is ever established—no hardware to install or software to manually update.
- **Cisco Duo –** Use multi-factor authentication to protect your organization's data wherever users are logging in—for every access attempt and from any device or location—by verifying user trust, establishing device trust and providing secure access to company apps and networks

CyberArk

- **CyberArk Secure Remote Workforce Access –** Secure remote workforce access with multi-factor authentication, single sign-on and endpoint privileged management—no VPNs, agents or passwords needed.
- **CyberArk Endpoint Privilege Manager –** Remove local admin rights, enforce least privilege, and implement foundational endpoint security controls across all Windows, macOS, and Linux endpoints, from hybrid to cloud environments.
- **CyberArk Privileged Access Manager –** Reduce risk and enable secure access to critical internal resources for remote employees and external vendors using biometric multi-factor authentication—without VPNs, passwords or agents.

Fortinet

- **Fortinet Universal ZTNA –** Quickly deploy a robust and reliable ZTNA solution with a low total cost of ownership (TCO) with on premises, cloud-based and hybrid options.
- **Fortinet FortiSASE –** Empower organizations to consistently apply enterprise-grade security and superior user experience across all edges with a comprehensive single-vendor SASE approach that integrates cloud-delivered SD-WAN connectivity with a cloud-delivered security service edge (SSE) to enable secure access from anywhere to the web, cloud and applications everywhere.
- **Fortinet Secure SD-WAN –** Get fast, flexible, scalable and secure SD-WAN—whether on-premises or in the cloud—in one operating system that integrates Fortinet SD-WAN with FortiGate next-generation firewall (NGFW), advanced routing and ZTNA application gateway capabilities.

HPE Aruba Networking

- **Aruba EdgeConnect SD-WAN + SSE –** Improve application performance and dramatically reduce the cost and complexity of building a WAN with a unified SASE security platform that enables enterprises to leverage broadband to connect users to applications.
- **Aruba Central –** Leverage a cloud-based networking solution that empowers IT to manage campus, branch, remote, data center, and IoT networks from one dashboard with AI-powered insights, intuitive visualizations, workflow automation and edge-to-cloud security.
- **Aruba ClearPass –** Enable IT managers to profile devices, deploy network policies, manage guest access, secure BYOD onboarding and check device health for zero trust security.

Opengear

- **Opengear Operations Manager (OM) 1200/2200 Console Servers –** Create a secure management plane for administrators with the OM series, featuring Smart Out-of-Band™ management and network automation—perfect for datacenters and edge sites.
- **Opengear Console Manager (CM) 8100 Console Server –** Manage high-density datacenters with the Smart Out-of-Band™ management and energy-efficient capabilities found in the CM8100.
- **Opengear Lighthouse –** Get unmatched visibility of distributed networks and proximity to critical devices through a centralized, single pane of control—built with multi-instance capabilities and designed for everyday use with security, scalability and automation.

ZPE Systems

- **Advanced threat intelligence –** Deploy the Nodegrid platform to manage a fleet of deployed IoT and AI edge services with Out of Band Management—it can cut organizational risk by supporting large fleets with cyber physical means: power and serial access.
- **Zero Trust Strategy With ZPE Systems –** Zero trust requires control and that starts by quickly and easily deploying in a ZT environment with the Nodegrid platform to enable Identity Security, Identity Access Management, Privileged Access Management, XDR, Multi-factor authentication (MFA), Cloud Access, Isolated Management and Resilience and Recovery.
- **Modernized networking –**Deploy Edge virtualization on a platform that utilizes its own and can deploy third-party solutions—such as SD-WAN, User Experience Monitoring, Cloud Access and Hybrid Infrastructure, and Platforms and Applications—or make the one you have more resilient with Wireless Backup Networking, ZT Interfaces, and recovery systems.

Opportunities for MSPs & MSSPs

Your customers require a new security approach as they seek to move from perimeter-based security to zero trust to help protect against targeted threats and improve business performance. It can also mitigate supply chain risk and secure cloud environments. Is your customer ready to take their first steps? Start by offering these services:

1 2 3

4 Offer Comprehensive Services

5

Help customers focus on their core business by leveraging our advanced managed and other security services.

- **Incident Response Services –** Comprehensive Incident Response (IR) services—including Plan Development, Readiness Review, and Emergency Response—ensure they have the right capabilities to respond to and recover from threats.
- **Compliance Services –** Governance and compliance readiness services for HIPAA, HITRUST, PCI-DSS, NIST 800-171, ISO 27001, NERC-CIP, SOC 1&2, GDPR and others—ideal for businesses that face a high regulatory burden.
- **Implementation Services –** Services for new installations, integrations, patch services, configurations, and staff augmentations to help you design the best solution for them.
- **Managed Security Services –** These managed services help you maximize limited resources:
  - **SOC as a Service –** Have a bench of cyber experts who can monitor, analyze, manage and act on threats across your customer's business.
  - **Firewall Services –** Help your customer focus on their core business while you administer, monitor, and maintain their firewall infrastructure.
  - **ISAO Threat Feed –** Join a very large community of companies, local governments and security professionals to collaborate, share intelligence, and participate in training and conferences and leverage competent collaborative analysis.

Consider these solutions:

Cisco

- **Cisco XDR –** Collect and correlate data and provide visibility across email, endpoints, servers, cloud workloads, and networks, and apply analytics and automation to detect, analyze, hunt, and remediate today's and tomorrow's threats.
- **Cisco Umbrella –** Combine multiple security functions into one cloud-delivered solution that extends data protection to devices, remote users and distributed locations anywhere, enabling you to enforce security and block malicious activity before an internet connection is ever established—no hardware to install or software to manually update.
- **Cisco Duo –** Use multi-factor authentication to protect your organization's data wherever users are logging in—for every access attempt and from any device or location—by verifying user trust, establishing device trust and providing secure access to company apps and networks

CyberArk

- **CyberArk Secure Remote Workforce Access –** Secure remote workforce access with multi-factor authentication, single sign-on and endpoint privileged management—no VPNs, agents or passwords needed.
- **CyberArk Endpoint Privilege Manager –** Remove local admin rights, enforce least privilege, and implement foundational endpoint security controls across all Windows, macOS, and Linux endpoints, from hybrid to cloud environments.
- **CyberArk Privileged Access Manager –** Reduce risk and enable secure access to critical internal resources for remote employees and external vendors using biometric multi-factor authentication—without VPNs, passwords or agents.

Fortinet

- **Fortinet Universal ZTNA –** Quickly deploy a robust and reliable ZTNA solution with a low total cost of ownership (TCO) with on premises, cloud-based and hybrid options.
- **Fortinet FortiSASE –** Empower organizations to consistently apply enterprise-grade security and superior user experience across all edges with a comprehensive single-vendor SASE approach that integrates cloud-delivered SD-WAN connectivity with a cloud-delivered security service edge (SSE) to enable secure access from anywhere to the web, cloud and applications everywhere.
- **Fortinet Secure SD-WAN –** Get fast, flexible, scalable and secure SD-WAN—whether on-premises or in the cloud—in one operating system that integrates Fortinet SD-WAN with FortiGate next-generation firewall (NGFW), advanced routing and ZTNA application gateway capabilities.

HPE Aruba Networking

- **Aruba EdgeConnect SD-WAN + SSE –** Improve application performance and dramatically reduce the cost and complexity of building a WAN with a unified SASE security platform that enables enterprises to leverage broadband to connect users to applications.
- **Aruba Central –** Leverage a cloud-based networking solution that empowers IT to manage campus, branch, remote, data center, and IoT networks from one dashboard with AI-powered insights, intuitive visualizations, workflow automation and edge-to-cloud security.
- **Aruba ClearPass –** Enable IT managers to profile devices, deploy network policies, manage guest access, secure BYOD onboarding and check device health for zero trust security.

Opengear

- **Opengear Operations Manager (OM) 1200/2200 Console Servers –** Create a secure management plane for administrators with the OM series, featuring Smart Out-of-Band™ management and network automation—perfect for datacenters and edge sites.
- **Opengear Console Manager (CM) 8100 Console Server –** Manage high-density datacenters with the Smart Out-of-Band™ management and energy-efficient capabilities found in the CM8100.
- **Opengear Lighthouse –** Get unmatched visibility of distributed networks and proximity to critical devices through a centralized, single pane of control—built with multi-instance capabilities and designed for everyday use with security, scalability and automation.

ZPE Systems

- **Advanced threat intelligence –** Deploy the Nodegrid platform to manage a fleet of deployed IoT and AI edge services with Out of Band Management—it can cut organizational risk by supporting large fleets with cyber physical means: power and serial access.
- **Zero Trust Strategy With ZPE Systems –** Zero trust requires control and that starts by quickly and easily deploying in a ZT environment with the Nodegrid platform to enable Identity Security, Identity Access Management, Privileged Access Management, XDR, Multi-factor authentication (MFA), Cloud Access, Isolated Management and Resilience and Recovery.
- **Modernized networking –** Deploy Edge virtualization on a platform that utilizes its own and can deploy third-party solutions—such as SD-WAN, User Experience Monitoring, Cloud Access and Hybrid Infrastructure, and Platforms and Applications—or make the one you have more resilient with Wireless Backup Networking, ZT Interfaces, and recovery systems.

Opportunities for MSPs & MSSPs

Your customers require a new security approach as they seek to move from perimeter-based security to zero trust to help protect against targeted threats and improve business performance. It can also mitigate supply chain risk and secure cloud environments. Is your customer ready to take their first steps? Start by offering these services:

1 2 3 4

5 Engage Through Training and Engagement Experiences

Finally, engage your customer's team with numerous training and engagement experiences for both new and advanced users.

Training

- **Foundational –** Develop the foundational cybersecurity skills needed to advance to the next level through the Cyber Essentials Series.
- **Accelerated –** Access over 50 cloud-based, instructor-led classroom learning courses to prepare for cybersecurity careers and train on a hyper-realistic network within a cloud-hosted cyber range using the tools your team uses every day.
- **Virtual –** Choose from an extensive set of courses for new cybersecurity team members or, for more advanced users, an upgraded training program that includes the entire course library, 200+ Virtual Lab Environments, a guided mentor, and industry certification practice tests.
- **Advanced threat training –** Learn how to contain threats, fix weaknesses, and use the latest threat hunting tools via online, gamified training using real-world simulations within a protected environment.

Engagement

- **Demos –** Test and engage with leading cybersecurity offerings to see how they work in real time.
- **Engagement –** Engage in an "up close and personal" live cyber experience to test the responses of your team and/or environment in a cyber range.

Consider these solutions:

Cisco

- **Cisco XDR –** Collect and correlate data and provide visibility across email, endpoints, servers, cloud workloads, and networks, and apply analytics and automation to detect, analyze, hunt, and remediate today's and tomorrow's threats.
- **Cisco Umbrella –** Combine multiple security functions into one cloud-delivered solution that extends data protection to devices, remote users and distributed locations anywhere, enabling you to enforce security and block malicious activity before an internet connection is ever established—no hardware to install or software to manually update.
- **Cisco Duo –** Use multi-factor authentication to protect your organization's data wherever users are logging in—for every access attempt and from any device or location—by verifying user trust, establishing device trust and providing secure access to company apps and networks

CyberArk

- **CyberArk Secure Remote Workforce Access –** Secure remote workforce access with multi-factor authentication, single sign-on and endpoint privileged management—no VPNs, agents or passwords needed.
- **CyberArk Endpoint Privilege Manager –** Remove local admin rights, enforce least privilege, and implement foundational endpoint security controls across all Windows, macOS, and Linux endpoints, from hybrid to cloud environments.
- **CyberArk Privileged Access Manager –** Reduce risk and enable secure access to critical internal resources for remote employees and external vendors using biometric multi-factor authentication—without VPNs, passwords or agents.

Fortinet

- **Fortinet Universal ZTNA –** Quickly deploy a robust and reliable ZTNA solution with a low total cost of ownership (TCO) with on premises, cloud-based and hybrid options.
- **Fortinet FortiSASE –** Empower organizations to consistently apply enterprise-grade security and superior user experience across all edges with a comprehensive single-vendor SASE approach that integrates cloud-delivered SD-WAN connectivity with a cloud-delivered security service edge (SSE) to enable secure access from anywhere to the web, cloud and applications everywhere.
- **Fortinet Secure SD-WAN –** Get fast, flexible, scalable and secure SD-WAN—whether on-premises or in the cloud—in one operating system that integrates Fortinet SD-WAN with FortiGate next-generation firewall (NGFW), advanced routing and ZTNA application gateway capabilities.

HPE Aruba Networking

- **Aruba EdgeConnect SD-WAN + SSE –** Improve application performance and dramatically reduce the cost and complexity of building a WAN with a unified SASE security platform that enables enterprises to leverage broadband to connect users to applications.
- **Aruba Central –** Leverage a cloud-based networking solution that empowers IT to manage campus, branch, remote, data center, and IoT networks from one dashboard with AI-powered insights, intuitive visualizations, workflow automation and edge-to-cloud security.
- **Aruba ClearPass –** Enable IT managers to profile devices, deploy network policies, manage guest access, secure BYOD onboarding and check device health for zero trust security.

Opengear

- **Opengear Operations Manager (OM) 1200/2200 Console Servers –** Create a secure management plane for administrators with the OM series, featuring Smart Out-of-Band™ management and network automation—perfect for datacenters and edge sites.
- **Opengear Console Manager (CM) 8100 Console Server –** Manage high-density datacenters with the Smart Out-of-Band™ management and energy-efficient capabilities found in the CM8100.
- **Opengear Lighthouse –** Get unmatched visibility of distributed networks and proximity to critical devices through a centralized, single pane of control—built with multi-instance capabilities and designed for everyday use with security, scalability and automation.

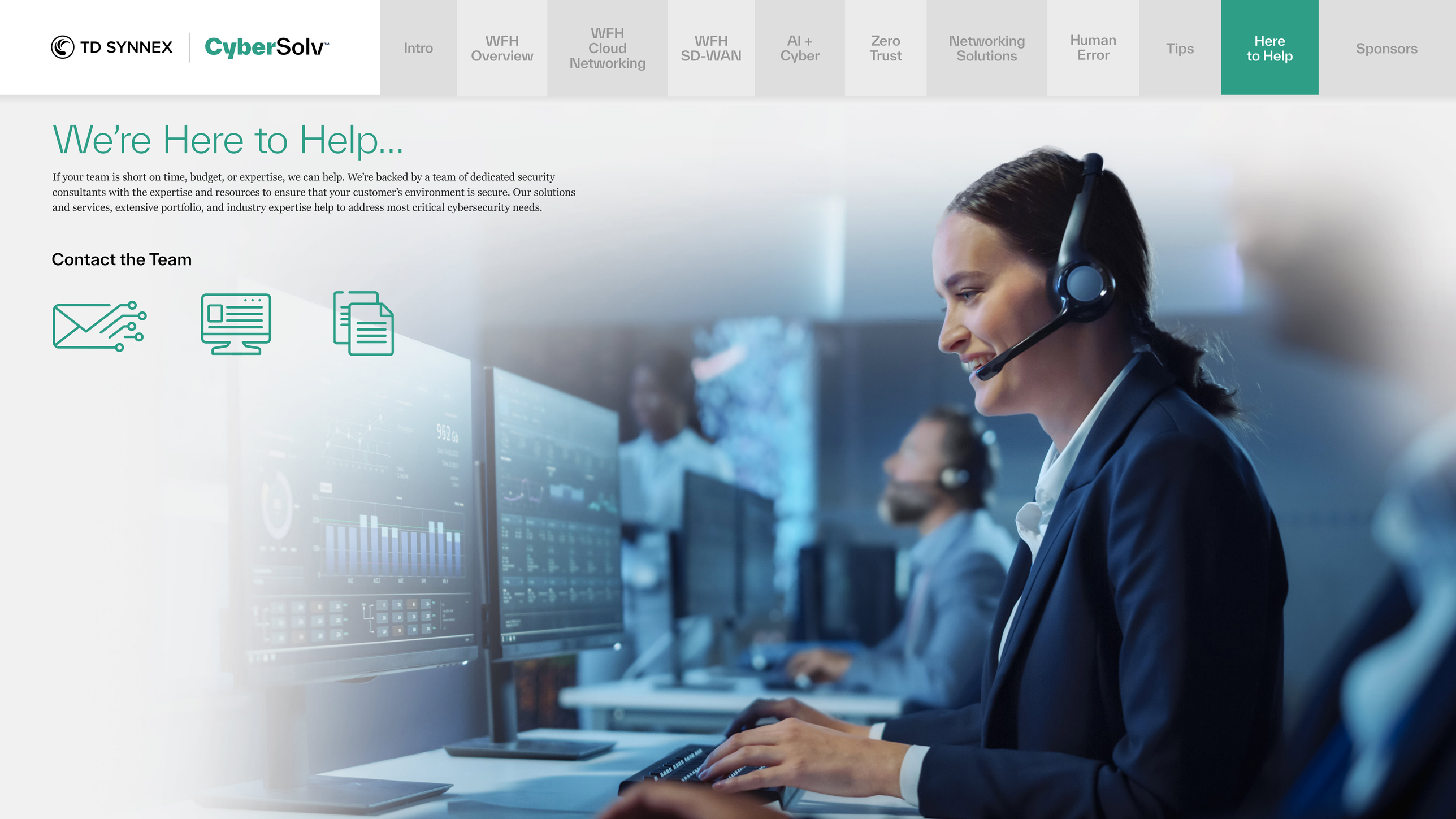
ZPE Systems

- **Advanced threat intelligence –** Deploy the Nodegrid platform to manage a fleet of deployed IoT and AI edge services with Out of Band Management—it can cut organizational risk by supporting large fleets with cyber physical means: power and serial access.
- **Zero Trust Strategy With ZPE Systems –** Zero trust requires control and that starts by quickly and easily deploying in a ZT environment with the Nodegrid platform to enable Identity Security, Identity Access Management, Privileged Access Management, XDR, Multi-factor authentication (MFA), Cloud Access, Isolated Management and Resilience and Recovery.
- **Modernized networking –** Deploy Edge virtualization on a platform that utilizes its own and can deploy third-party solutions—such as SD-WAN, User Experience Monitoring, Cloud Access and Hybrid Infrastructure, and Platforms and Applications—or make the one you have more resilient with Wireless Backup Networking, ZT Interfaces, and recovery systems.

We're Here to Help...

If your team is short on time, budget, or expertise, we can help. We're backed by a team of dedicated security consultants with the expertise and resources to ensure that your customer's environment is secure. Our solutions and services, extensive portfolio, and industry expertise help to address most critical cybersecurity needs.

Contact the Team



Thank You to Our Sponsors!

For more information on any one of these or other TD SYNNEX security solutions or services, please contact the security professionals below:

ActZero

Special offer! Learn more about our service and how you can leave the defense to us—and get a free dark web scan to see if your credentials have been compromised.

Contact: ActZero@tdsynnex.com

Cisco Distributor

For more information, contact us.

Contact: James.McGregor@tdsynnex.com

CYBERARK

Visit cyberark.com or contact us.

Contact: CyberArk@tdsynnex.com

FORTINET

For more information, contact us.

Contact: FortinetBD@tdsynnex.com

HPE aruba networking

Special offer! Contact us for help with configuring and quoting and ask how you can get 60% off plus cash SPIFFS when you sell EdgeConnect Foundation SD-WAN products.

Contact: Aruba.US@tdsynnex.com

opengear A DIGI COMPANY

Visit Opengear's CyberSolv page or contact us to learn more.

Contact: Josh.Payne@tdsynnex.com

zpe

Visit the ZPE Systems CyberSolv page to learn more.

Contact: Gerry.Poynter@tdsynnex.com

Footnotes

1. Channel Futures. How Network Technology Shifts Are Changing the Way Things Are Done. March 17, 2021.
2. Flexera.com. 2023 State of the Cloud Report. 2023.
3. Netwirx. 2020 Cyber Threats Report. 2020.
4. Enterprise Strategy Group End-to-end Networking Visibility and Management. April 2023.
5. Enterprise Strategy Group. The Buyer's Journey to Integrated Solutions from Strategic Partners. April 2023.
6. Cisco.com. 2023 Global Networking Trends Report. 2023.
7. Enterprise Strategy Group. Cyber-threat Intelligence Programs: Ubiquitous and Immature. March 2023.
8. Tessian.com. Back to Work Security Behaviors Report.
9. Nwankpa, Joseph K & Datta, Pratim Milton. Remote vigilance: The roles of cyber awareness and cybersecurity policies among remote workers. Computers & Security, Computers & Security, Vol. 130, 103266. July 2023.
10. Frost & Sullivan. The Top Growth Opportunities for IoT in 2023. March 14, 2023.
11. Blackberry.com. ChatGPT May Already Be Used in Nation State Cyberattacks, Say IT Decision Makers in BlackBerry Global Research. Feb. 2, 2023.
12. IEEE.org. The Use of Artificial Intelligence in Cybersecurity: A Review. Retrieved Sept. 25, 2023.
13. eWeek.com. Generative AI and Cybersecurity. June 16, 2023.
14. TechTarget.com. How to implement zero-trust cloud security. Retrieved Sept. 25, 2023.
15. Gartner. Gartner Predicts 10% of Large Enterprises Will Have a Mature and Measurable Zero-Trust Program in Place by 2026. Jan. 23, 2023.
16. NTT.com. 2022-2023 Global Network Report. 2023.
17. ESG.com. Key Attributes of Network Modernization. Nov. 2020.
18. CIO.com. Modern cloud-based networks: The key to high-level commercial performance? Dec. 8, 2022.
19. Verizon. 2023 Data Breach Investigations Report. 2023.
20. IBM and Ponemon Institute. Cost of a Data Breach Report 2023. 2023.
21. Stanford University/Tessian. The Psychology of Human Error 2022: Understand the Mistakes that Compromise Your Company's Cybersecurity. 2022.