Building a Zero-Trust Edge

Solutions Guide

Building a Zero-Trust Edge

Bringing networking and security technologies together to deliver an all-encompassing zero trust environment.

Solutions to consider

Building a Zero-Trust Edge

Bringing networking and security technologies together to deliver an all-encompassing zero trust environment.

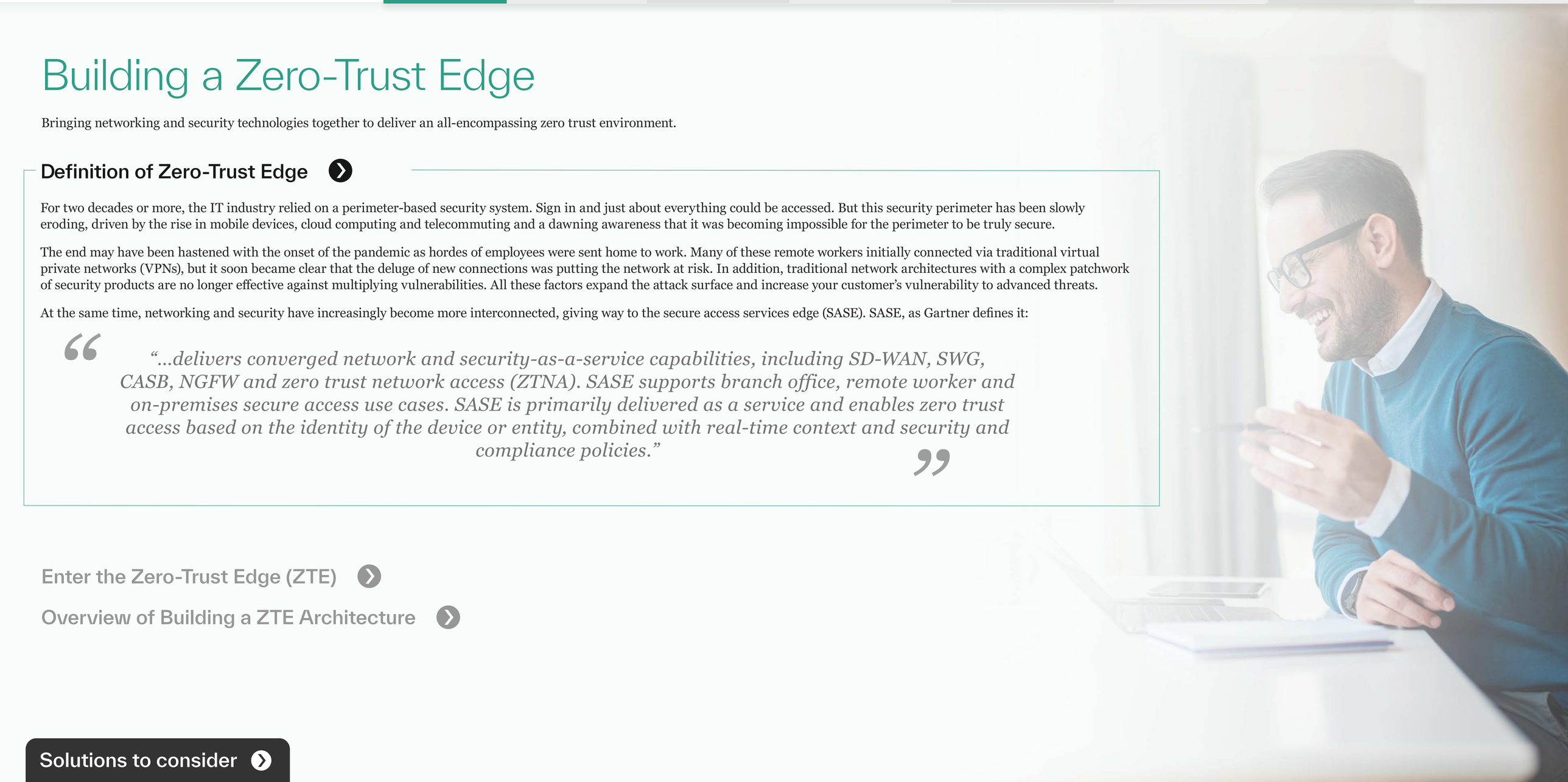
Definition of Zero-Trust Edge

For two decades or more, the IT industry relied on a perimeter-based security system. Sign in and just about everything could be accessed. But this security perimeter has been slowly eroding, driven by the rise in mobile devices, cloud computing and telecommuting and a dawning awareness that it was becoming impossible for the perimeter to be truly secure.

The end may have been hastened with the onset of the pandemic as hordes of employees were sent home to work. Many of these remote workers initially connected via traditional virtual private networks (VPNs), but it soon became clear that the deluge of new connections was putting the network at risk. In addition, traditional network architectures with a complex patchwork of security products are no longer effective against multiplying vulnerabilities. All these factors expand the attack surface and increase your customer's vulnerability to advanced threats.

At the same time, networking and security have increasingly become more interconnected, giving way to the secure access services edge (SASE). SASE, as Gartner defines it:

> *"...delivers converged network and security-as-a-service capabilities, including SD-WAN, SWG, CASB, NGFW and zero trust network access (ZTNA). SASE supports branch office, remote worker and on-premises secure access use cases. SASE is primarily delivered as a service and enables zero trust access based on the identity of the device or entity, combined with real-time context and security and compliance policies."*



Enter the Zero-Trust Edge (ZTE)

Overview of Building a ZTE Architecture

Solutions to consider

Building a Zero-Trust Edge

Bringing networking and security technologies together to deliver an all-encompassing zero trust environment.

Definition of Zero-Trust Edge

Enter the Zero-Trust Edge (ZTE)

In the simplest definition, ZTE merges networking and security functions and delivers them as a service. It "connects internet traffic to remote sites using Zero Trust access principles, primarily by utilizing cloud-based security and networking services".[2]

The tighter integration of networking and security inherent in ZTE has been hastened by these principles:[3]

1. Network traffic must adhere to strict security trust levels and comply with established policies.
2. Organizations must adopt ZTE policies and pursue networking with a security-centric approach instead of overlaying security onto corporate networks.
3. All clients and endpoints must have secure internet access, capable of neutralizing or bypassing potential malware threats at any point in the network.

In effect, ZTE uses zero trust network access (ZTNA) to authenticate and monitor users and devices as they connect, providing a more secure internet on-ramp that's accessible from anywhere. Additional ZTE components include secure web gateway (SWG), software-defined wide area networking (SD-WAN), and cloud access security broker (CASB).

But ZTE is not SASE. While their goals are largely the same, SASE converges SD-WAN and multiple network security services into a unified cloud-based offering for secure, efficient network access of increasingly remote and distributed workforces. ZTE takes a slightly different and more stringent approach. It assumes a worst-case scenario and focuses intently on zero trust to authenticate every connection and enforce zero trust principles across the network infrastructure.

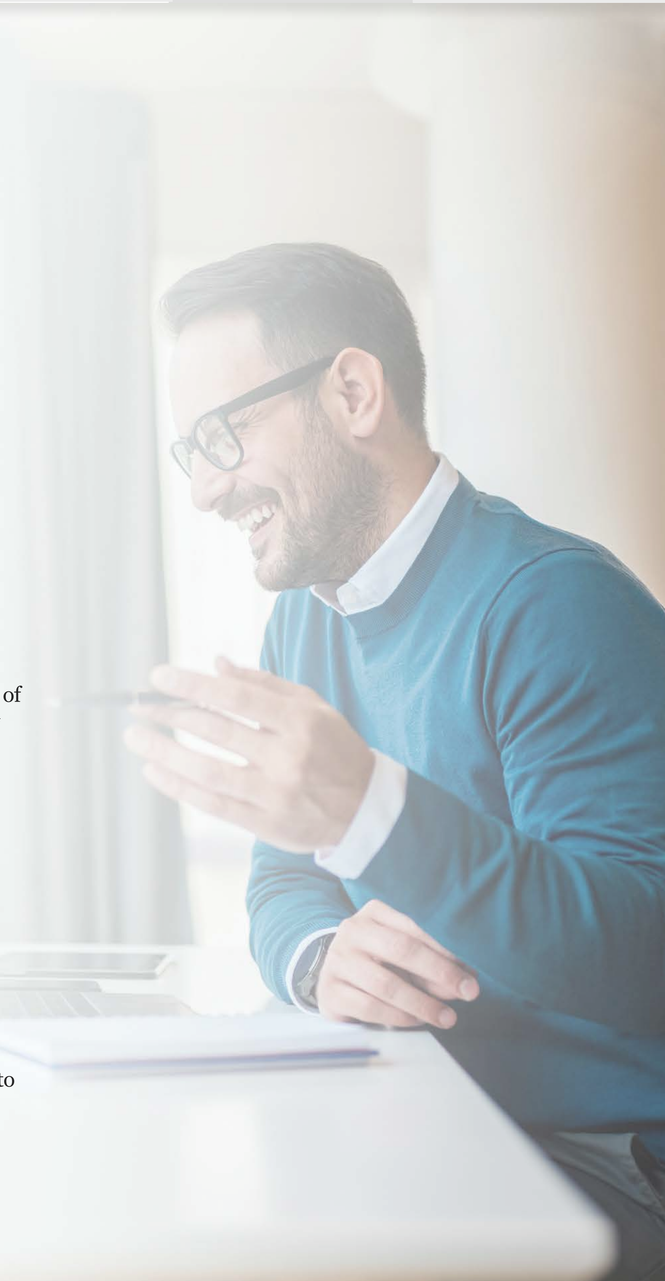
Having evolved from SASE, ZTE itself continues to evolve with Forrester describing it this way:

> *"Organizations are using ZTE to protect remote workers, retail outlets, and branch offices in the short term. In five years, they will use ZTE to securely connect data centers, factories, and hospitals. In its final form, ZTE will fully converge networking and security, combining Zero Trust security principles and software-defined networking into a cohesive set of cloud-delivered and managed services."* [4]

In other words, ZTE puts more emphasis on zero trust by viewing every network transaction as potentially risky and authenticating every transaction as a result. It provides a more secure gateway to the internet and access to an organization's applications and data for their distributed sites and remote workforce.

Overview of Building a ZTE Architecture

Solutions to consider



Building a Zero-Trust Edge

Bringing networking and security technologies together to deliver an all-encompassing zero trust environment.

Definition of Zero-Trust Edge

Enter the Zero-Trust Edge (ZTE)

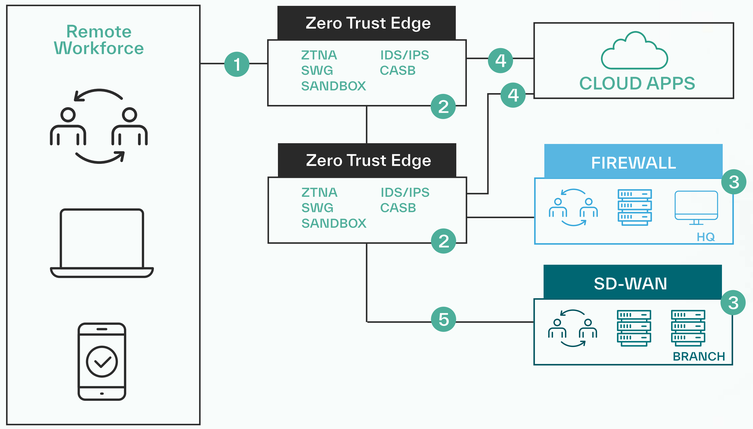
Overview of Building a ZTE Architecture

ZTE essentially forms a new perimeter by converging networking and security and through continuous validation of user identity and context, grants explicit access to applications.

Security components are put into an edge-hosted security stack, with some components requiring local infrastructure due to bandwidth constraints. A cloud-based solution is preferable due to the sheer volume of data being collected, stored and processed for analysis.

After deployment, your customer can centrally manage, monitor and analyze their security and networking services, whether they're hosted on the cloud or remotely. The ultimate objective is to provide stringent security without compromising on networking capabilities.[3]

1. Zero Trust Access Authentication
2. Security controls can be hosted in an edge network, or on-prem
3. ZTE Remote access to on-prem applications
4. Remote users directed to cloud applications via CASB
5. SD-WAN is a foundational control for physical locations



For precisely these reasons, it's crucial for you to stay on top of the fast-moving advancements in AI and how they can impact your customer's security environment.

Solutions to consider

Building a Zero-Trust Edge

Bringing networking and security technologies together to deliver an all-encompassing zero trust environment.

Definition of Zero-Trust Edge

Enter the Zero-Trust Edge (ZTE)

Overview of Building a ZTE Architecture

There are currently three approaches that can be used for a ZTE implementation:[2]

1. Cloud-based ZTE – This cloud-delivered service, which mirrors SaaS delivery models, employs multiple points of presence (POPs) with inherent ZTE capabilities.

2. ZTE as an Extension of a WAN connection service – A carrier provides ZTE functionality as well as outsourced security. There are several on-premises offerings with SD-WAN/ZTE combinations, but they typically lack the agility of cloud-based systems and require policy configurations for each individual service—all of which make a single, holistic solution impossible.

3. Homegrown ZTE – Organizations can build their own ZTE solution using cloud service providers for points of presence (POPs) and cloud-hosted firewalls, along with other cloud-based security services. Although this approach is eminently flexible, it's typically viable only for large and agile enterprises that have the resources needed to build and manage their own solution and monitor the evolving landscape for components and cloud services to stay ahead of the security curve.

As a result, an integrated, cloud-based ZTE provides:[3]

- **Unified cybersecurity infrastructure** – Consolidates multiple cybersecurity tools into a unified solution for a more efficient, manageable cybersecurity infrastructure that simplifies threat management.
- **Better risk mitigation** – Substantially enhances overall network security and provides more proactive security management with consistent and coordinated security policies ingrained at every level of the network, rigorous and continuous authentication of every transaction, and improved incident response and simplified troubleshooting.
- **Better network performance** – Eliminates traditional VPNs and associated data backhauling and employs cloud on-ramps for global connectivity and security inspection, boosting performance.
- **Optimized user experience** – Improves network performance and throughput, significantly accelerating application performance for a better, more productive user experience.
- **Improved cost-effectiveness** – Delivers significant cost savings and ensures your customer only pays for the resources they use due to automated, cloud-based ZTE.

Cloud-based ZTE delivers the most value because it relies on:[2]

- *Cloud-based network and security management* that provides a single set of policies for users across the enterprise, as well as management tools for networking, firewall, and other SD-WAN functionality to reduce errors, increase efficiency, and facilitate setting up similar policies for multiple systems.
- *Monitoring, management and analysis tools* that link networking and security. This hallmark of ZTE enables better use of links, helps identify network anomalies that can lead to security issues, and enables the entire network to be monitored. Cloud-based solutions are also needed to collect, store, and process the sheer volume of data needed to produce the needed analytics.

Solutions to consider

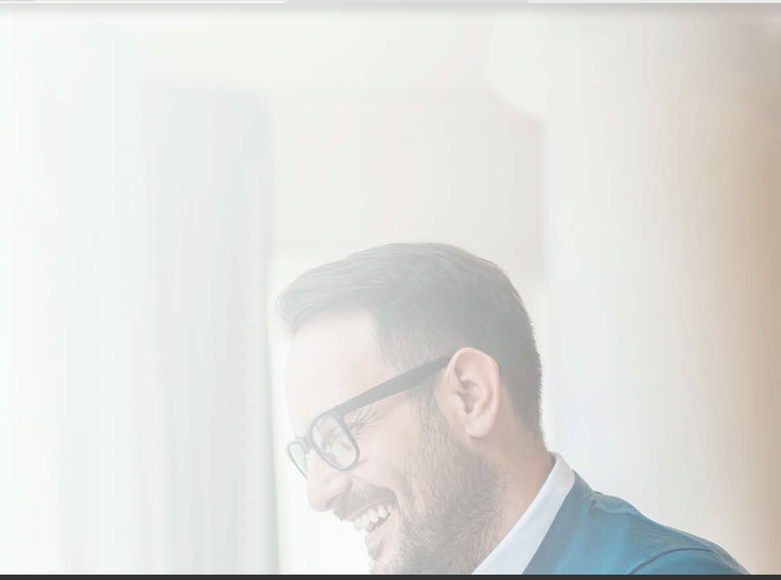
Building a Zero-Trust Edge

Bringing networking and security technologies together to deliver an all-encompassing zero trust environment.

Definition of Zero-Trust Edge

Enter the Zero-Trust Edge (ZTE)

Overview of Building a ZTE Architecture



Solutions to consider

Dell Technologies

- **Dell EMC PowerEdge Servers –** These servers provide a cyber-resilient infrastructure with built-in security features that support zero trust principles. They offer secure boot, system lockdown and firmware protection.
- **Dell EMC OpenManage –** This suite includes tools for managing and automating server infrastructure, ensuring consistent security configurations and compliance with zero trust policies.
- **Dell EMC PowerScale –** This scale-out NAS solution follows the zero trust model and can be deployed across the enterprise, from edge to core to cloud, handling demanding file-based workloads securely.

HPE Aruba

- **HPE Aruba Networking Zero Trust Network Access (ZTNA) –** This advanced ZTNA service uses identity, policy and context to broker secure, one-to-one connections to private apps (even VoIP, AS400 and ICMP)—replacing VPN without network access or exposure.
- **Secure web gateway (SWG) –** Using advanced SSL inspection, URL filtering and DNS filtering, this SWG ensures that authorized users get fast, secure internet access—while protecting the business from Internet- based threats.
- **Cloud access security broker (CASB) –** This solution mediates the connections between users and cloud applications, helps discover shadow IT to apps and ensures sensitive data in motion remains protected, while helping prevent cyberthreats.

Palo Alto Networks

Palo Alto's portfolio of platforms consolidates best-in-class capabilities under a single, unified cybersecurity solution to outpace cyberthreats with:

- **Network Security –** Leverage an industry-leading firewall platform and comprehensive Prisma SASE solution available across hardware, software and cloud-based form factors.
- **Cloud Security –** Comprehensive security through Prisma Cloud from development to runtime across multicloud and hybrid environments
- **Security Operations –** A new approach to SOC with Cortex XDR, XSOAR and XSIAM providing advanced visibility, data, analytics and automation capabilities.

Splunk

- **Splunk Enterprise Security (ES) –** Get real-time monitoring, advanced threat detection, and data-driven security insights for fast response to potential threats. Robust analytics capabilities enhance visibility for easier management of tasks to complex cyber threats.
- **Splunk SOAR (Security Orchestration, Automation, and Response) –** Streamline security operations across security tools and accelerate incident response, helping teams efficiently resolve threats while freeing time for strategic activities. Customizable playbooks ensure a proactive and adaptive security posture.
- **Splunk User Behavior Analytics (UBA) –** Detect unusual behavior and potential threats with contextual insights that help security teams quickly identify and mitigate risks. Supports multiple use cases to enhance overall security visibility and operational effectiveness.

Understanding Zero-Trust Principles

As the number and sophistication of cyberattacks increases, your customer knows how critical it is to build and refine their cybersecurity strategies. With zero trust as the foundation for ZTE, it's also important to understand that the "never trust, always verify" approach requires every access request to be verified. Here are some additional zero-trust principles to understand in the context of ZTE:

Principle of Least Privilege[5]

Microsegmentation

Continuous Authentication and Authorization[6]

Zero-Trust Network Access (ZTNA)[6]

Device and User Identity Verification[6]

Solutions to consider

Understanding Zero-Trust Principles

As the number and sophistication of cyberattacks increases, your customer knows how critical it is to build and refine their cybersecurity strategies. With zero trust as the foundation for ZTE, it's also important to understand that the "never trust, always verify" approach requires every access request to be verified. Here are some additional zero-trust principles to understand in the context of ZTE:

Principle of Least Privilege[5]

Both zero trust and least privilege address shortcomings of traditional models by establishing secure, identity-based access controls and both play a critical role in helping your customer define and refine a strong cybersecurity framework to minimize the attack surface. It starts with a thorough understanding of your customer's data and systems and identifying the resources that need to be protected. Then you can restrict user access to only what's necessary for each user or group of users and their associated job functions to minimize potential damage and protect sensitive data from unauthorized access.

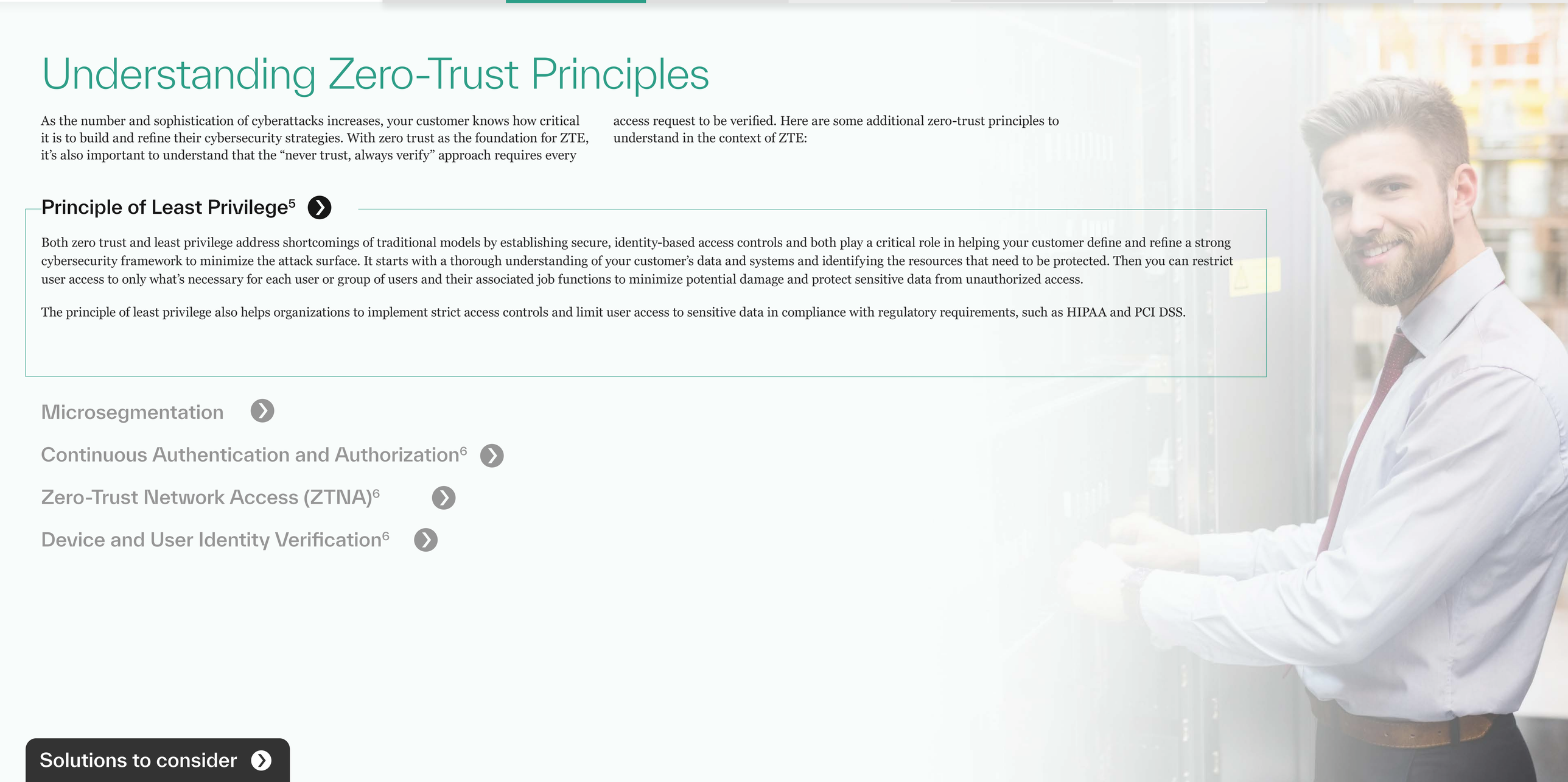
The principle of least privilege also helps organizations to implement strict access controls and limit user access to sensitive data in compliance with regulatory requirements, such as HIPAA and PCI DSS.

Microsegmentation

Continuous Authentication and Authorization[6]

Zero-Trust Network Access (ZTNA)[6]

Device and User Identity Verification[6]



Understanding Zero-Trust Principles

As the number and sophistication of cyberattacks increases, your customer knows how critical it is to build and refine their cybersecurity strategies. With zero trust as the foundation for ZTE, it's also important to understand that the "never trust, always verify" approach requires every access request to be verified. Here are some additional zero-trust principles to understand in the context of ZTE:

Principle of Least Privilege[5]

Microsegmentation

Network segmentation isn't new, but a zero-trust strategy suggests segmenting the network into even smaller, isolated units—such as networks, workloads, and applications—for even more granular control. If your customer's environment is breached, having microsegmentation will limit the lateral movement of potential threats, contain the threat and keep the malware from spreading throughout the environment.

Continuous Authentication and Authorization[6]

Zero-Trust Network Access (ZTNA)[6]

Device and User Identity Verification[6]

Solutions to consider

Understanding Zero-Trust Principles

As the number and sophistication of cyberattacks increases, your customer knows how critical it is to build and refine their cybersecurity strategies. With zero trust as the foundation for ZTE, it's also important to understand that the "never trust, always verify" approach requires every access request to be verified. Here are some additional zero-trust principles to understand in the context of ZTE:

Principle of Least Privilege[5]

Microsegmentation

Continuous Authentication and Authorization[6]

An ongoing process that requires significant resources, continuous monitoring and authorization is essential to maintaining the security of an organization's systems and data. It includes:

- Monitoring user activity, network traffic, and device posture to detect any suspicious activities and respond accordingly.
- Ensuring that users maintain the required level of privileges to mitigate the risk of unauthorized access and potential data breaches.
- Getting a more complete picture of user activity and network traffic and assessing suspicious activity through log collection, analysis, and correlation.
- Verifying user identities and device posture, including checking user credentials and ensuring that devices have the latest security patches and configurations.
- Monitoring for anomalies in user behavior, such as unusual login times or access to sensitive resources.

Zero-Trust Network Access (ZTNA)[6]

Device and User Identity Verification[6]

Solutions to consider

Understanding Zero-Trust Principles

As the number and sophistication of cyberattacks increases, your customer knows how critical it is to build and refine their cybersecurity strategies. With zero trust as the foundation for ZTE, it's also important to understand that the "never trust, always verify" approach requires every access request to be verified. Here are some additional zero-trust principles to understand in the context of ZTE:

Principle of Least Privilege[5]

Microsegmentation

Continuous Authentication and Authorization[6]

Zero-Trust Network Access (ZTNA)[6]

Where a traditional VPN assumes that anyone or anything that passes network perimeter controls can be trusted, ZTNA assumes that no user or device can be trusted to access anything until it proves otherwise. It creates a context-based logical boundary for application access by hiding all applications on the network and allowing access based on attributes such as user identity, device, geolocation, and other factors to reduce the attack surface. ZTNA then provides secure remote access—based on clearly defined access control policies—to applications, data and services when users, workloads or data may reside outside the traditional perimeter.[7]

Device and User Identity Verification[6]

Understanding Zero-Trust Principles

As the number and sophistication of cyberattacks increases, your customer knows how critical it is to build and refine their cybersecurity strategies. With zero trust as the foundation for ZTE, it's also important to understand that the "never trust, always verify" approach requires every access request to be verified. Here are some additional zero-trust principles to understand in the context of ZTE:

Principle of Least Privilege[5]

Microsegmentation

Continuous Authentication and Authorization[6]

Zero-Trust Network Access (ZTNA)[6]

Device and User Identity Verification[6]

When identity is verified only once at login, bad actors only have to bypass this one layer to gain access to a user's account. Breaches, account takeover attacks and other potential threats typically follow. To protect against these and other threats, organizations need to consider both user and device verification.

Most user identity verification methods verify a user's identity in real-time, from the beginning of their session to the end, while device authentication verifies the device's legitimacy for access using methods such as certificates installed on the device, client apps or hardware tokens. Biometrics can also be used for both user and device authentication.

Continuous authentication systems use multiple streams of data to develop a profile of each user's expected behaviors. If a given user behaves in the expected way, they continue their session normally. But if a user does something unexpected—such as logging in from a new location, using a different device or moving their mouse in an unusual way—it can be further investigated or an additional step can be introduced. This process allows your customer to be "less trusting" without sacrificing the user experience.

Solutions to consider

Understanding Zero-Trust Principles

As the number and sophistication of cyberattacks increases, your customer knows how critical it is to build and refine their cybersecurity strategies. With zero trust as the foundation for ZTE, it's also important to understand that the "never trust, always verify" approach requires every access request to be verified. Here are some additional zero-trust principles to understand in the context of ZTE:

Principle of Least Privilege[5]

Microsegmentation

Continuous Authentication and Authorization[6]

Solutions to consider

s (ZTNA)[6]

Dell Technologies

- **Dell EMC PowerEdge Servers –** These servers provide a cyber-resilient infrastructure with built-in security features that support zero trust principles. They offer secure boot, system lockdown and firmware protection.
- **Dell EMC OpenManage –** This suite includes tools for managing and automating server infrastructure, ensuring consistent security configurations and compliance with zero trust policies.
- **Dell EMC PowerScale –** This scale-out NAS solution follows the zero trust model and can be deployed across the enterprise, from edge to core to cloud, handling demanding file-based workloads securely.

HPE Aruba

- **HPE Aruba Networking Zero Trust Network Access (ZTNA) –** This advanced ZTNA service uses identity, policy and context to broker secure, one-to-one connections to private apps (even VoIP, AS400 and ICMP)—replacing VPN without network access or exposure.
- **Secure web gateway (SWG) –** Using advanced SSL inspection, URL filtering and DNS filtering, this SWG ensures that authorized users get fast, secure internet access—while protecting the business from Internet- based threats.
- **Cloud access security broker (CASB) –** This solution mediates the connections between users and cloud applications, helps discover shadow IT to apps and ensures sensitive data in motion remains protected, while helping prevent cyberthreats.

Palo Alto Networks

Palo Alto's portfolio of platforms consolidates best-in-class capabilities under a single, unified cybersecurity solution to outpace cyberthreats with:

- **Network Security –** Leverage an industry-leading firewall platform and comprehensive Prisma SASE solution available across hardware, software and cloud-based form factors.
- **Cloud Security –** Comprehensive security through Prisma Cloud from development to runtime across multicloud and hybrid environments
- **Security Operations –** A new approach to SOC with Cortex XDR, XSOAR and XSIAM providing advanced visibility, data, analytics and automation capabilities.

Splunk

- **Splunk Enterprise Security (ES) –** Get real-time monitoring, advanced threat detection, and data-driven security insights for fast response to potential threats. Robust analytics capabilities enhance visibility for easier management of tasks to complex cyber threats.
- **Splunk SOAR (Security Orchestration, Automation, and Response) –** Streamline security operations across security tools and accelerate incident response, helping teams efficiently resolve threats while freeing time for strategic activities. Customizable playbooks ensure a proactive and adaptive security posture.
- **Splunk User Behavior Analytics (UBA) –** Detect unusual behavior and potential threats with contextual insights that help security teams quickly identify and mitigate risks. Supports multiple use cases to enhance overall security visibility and operational effectiveness.

Designing the Zero-Trust Edge Architecture

A zero-trust architecture (ZTA) helps your customer manage today's most pressing cybersecurity and audit concerns. By instilling the core zero-trust principles of "never trust, always verify" and "assume breach," you can help bring about a new cybersecurity standard that can reduce the chance of a successful cyber incident. As an architectural framework, zero trust complements what already exists in the security stack, enabling your customer to gradually make improvements by adding solutions, service provider expansions, integrations or strategic capability consolidations.[8]

Identifying Edge Devices and Endpoints

Establishing Trust Boundaries

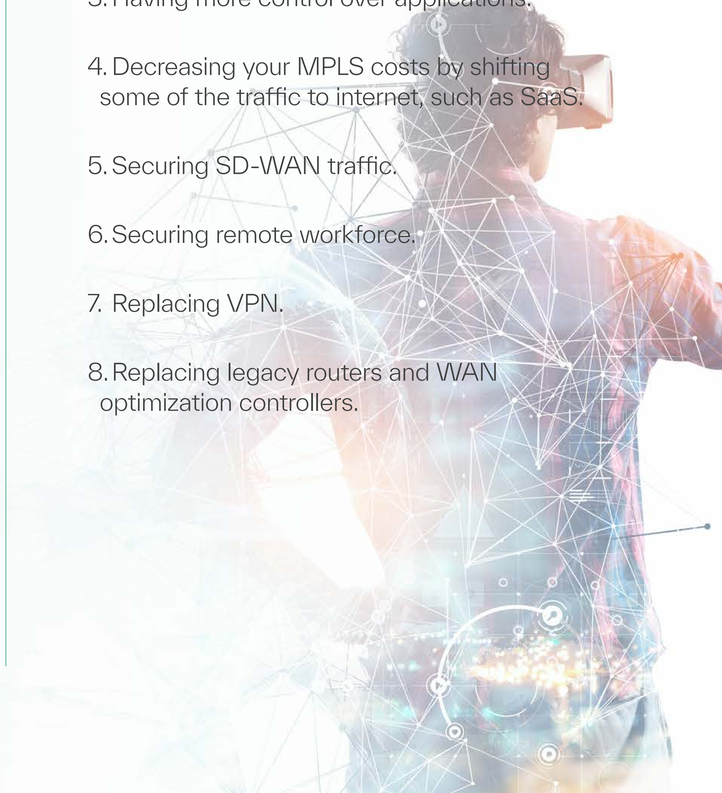
Implementing Secure Access Technologies

Leveraging Identity and Authentication Mechanisims

Monitoring and Visibility

Vendor Solutions for AI-Powered Cybersecurity

1. Increasing the reliability of the sites by using all the links available at the site (move to active-active configuration).
2. Getting away from MPLS and shifting to all internet.
3. Having more control over applications.
4. Decreasing your MPLS costs by shifting some of the traffic to internet, such as SaaS.
5. Securing SD-WAN traffic.
6. Securing remote workforce.
7. Replacing VPN.
8. Replacing legacy routers and WAN optimization controllers.



Solutions to consider

Designing the Zero-Trust Edge Architecture

A zero-trust architecture (ZTA) helps your customer manage today's most pressing cybersecurity and audit concerns. By instilling the core zero-trust principles of "never trust, always verify" and "assume breach," you can help bring about a new cybersecurity standard that can reduce the chance of a successful cyber incident. As an architectural framework, zero trust complements what already exists in the security stack, enabling your customer to gradually make improvements by adding solutions, service provider expansions, integrations or strategic capability consolidations.[8]

Identifying Edge Devices and Endpoints

Even as your customer continues to add devices—including IoT and mobile devices, as well as remote workstations—they need to ensure reliability out to the edge. Start by mapping their environment, including on-premises data centers and cloud services. Then, list all endpoints, specifically the devices that end-users are using. Include any mobile devices—smartphones, tablets, laptops, etc.—and both company-owned and personal workstations. Any devices that will be accessing the network and resources need to be on the list. In thinking only about remote offices when deploying ZTE, your customer may be missing vulnerable connection points.

Establishing Trust Boundaries

Implementing Secure Access Technologies

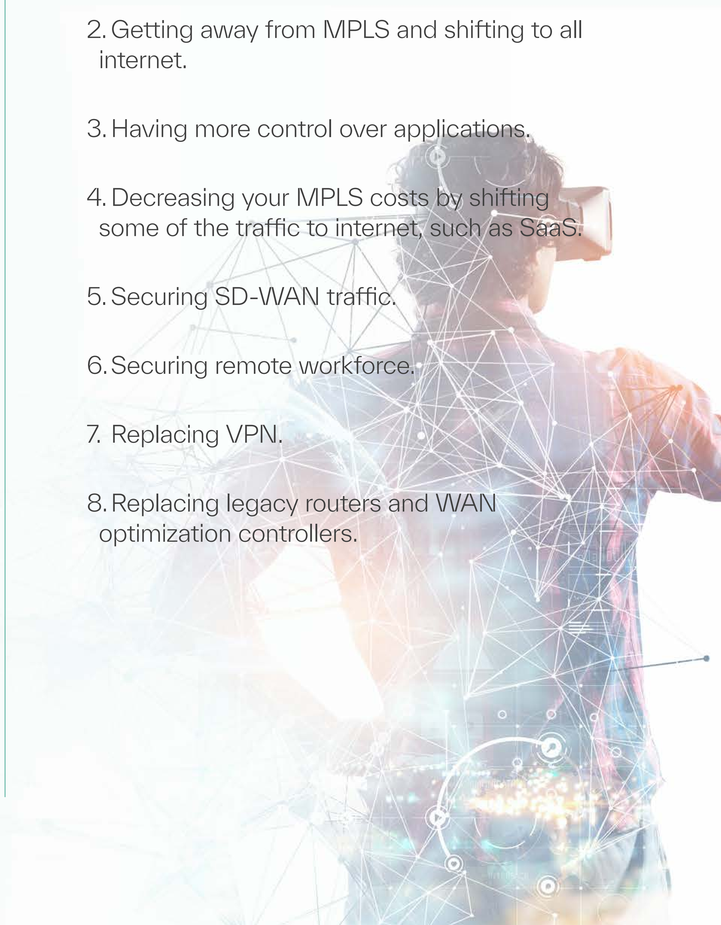
Leveraging Identity and Authentication Mechanisims

Monitoring and Visibility

Solutions to consider

Vendor Solutions for AI-Powered Cybersecurity

1. Increasing the reliability of the sites by using all the links available at the site (move to active-active configuration).
2. Getting away from MPLS and shifting to all internet.
3. Having more control over applications.
4. Decreasing your MPLS costs by shifting some of the traffic to internet, such as SaaS.
5. Securing SD-WAN traffic.
6. Securing remote workforce.
7. Replacing VPN.
8. Replacing legacy routers and WAN optimization controllers.



Designing the Zero-Trust Edge Architecture

A zero-trust architecture (ZTA) helps your customer manage today's most pressing cybersecurity and audit concerns. By instilling the core zero-trust principles of "never trust, always verify" and "assume breach," you can help bring about a new cybersecurity standard that can reduce the chance of a successful cyber incident. As an architectural framework, zero trust complements what already exists in the security stack, enabling your customer to gradually make improvements by adding solutions, service provider expansions, integrations or strategic capability consolidations.[8]

Identifying Edge Devices and Endpoints

Establishing Trust Boundaries

- ***Segmenting network zones***[9] **–** Network segmentation is a core concept in a zero-trust security strategy that involves dividing a network into distinct, secure zones or segments. Each segment contains network objects that share similar security requirements, such as workstations, servers and devices. This granular approach helps to confine the impact of a breach to the compromised segment, making it more difficult for attackers to move laterally across the network.

- ***Defining access control policies***[10] **–** Access control policies regulate access to resources within your customer's environment, minimizing risk to the organization. It can be physical in controlling access to tangible assets or logical by managing connections to networks, system files and data. Zero trust guides the development and implementation of access control policies, while access control policies enforce zero trust to ensure that only authenticated and authorized users and devices gain access to specific resources.

- ***Implementing software-defined perimeters (SDPs)***[11] **–** A zero-trust implementation using SDPs enables your customer to defend new variations of old attack methods that are constantly surfacing in existing perimeter-centric networks. Implementing SDP improves the security posture of organizations challenged to continuously adapt to expanding attack surfaces that are increasingly more complex.

Implementing Secure Access Technologies

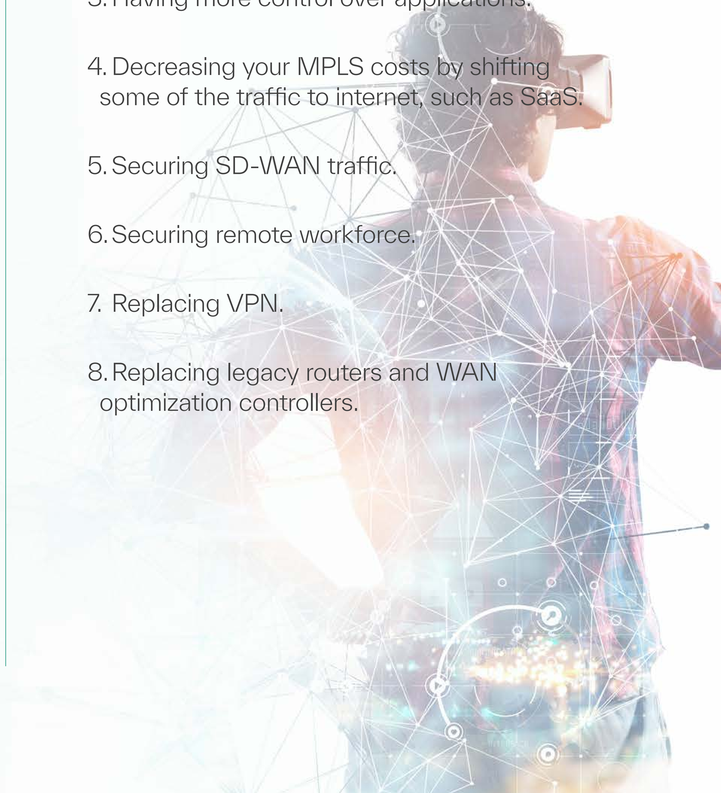
Leveraging Identity and Authentication Mechanisims

Monitoring and Visibility

Solutions to consider

Vendor Solutions for AI-Powered Cybersecurity

1. Increasing the reliability of the sites by using all the links available at the site (move to active-active configuration).
2. Getting away from MPLS and shifting to all internet.
3. Having more control over applications.
4. Decreasing your MPLS costs by shifting some of the traffic to internet, such as SaaS.
5. Securing SD-WAN traffic.
6. Securing remote workforce.
7. Replacing VPN.
8. Replacing legacy routers and WAN optimization controllers.



Designing the Zero-Trust Edge Architecture

A zero-trust architecture (ZTA) helps your customer manage today's most pressing cybersecurity and audit concerns. By instilling the core zero-trust principles of "never trust, always verify" and "assume breach," you can help bring about a new cybersecurity standard that can reduce the chance of a successful cyber incident. As an architectural framework, zero trust complements what already exists in the security stack, enabling your customer to gradually make improvements by adding solutions, service provider expansions, integrations or strategic capability consolidations.[8]

Identifying Edge Devices and Endpoints

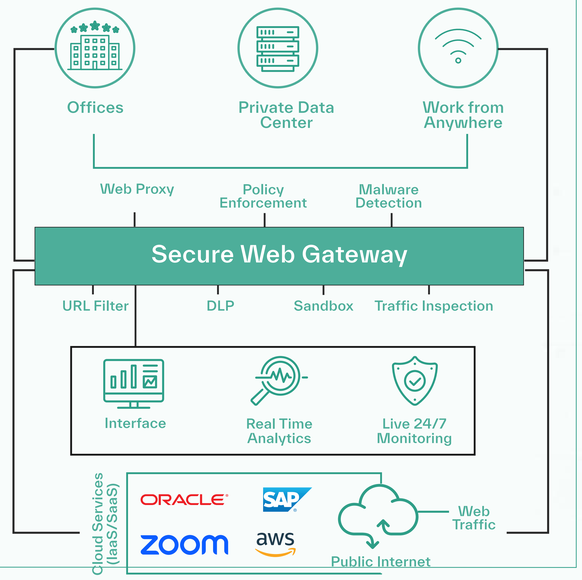
Establishing Trust Boundaries

Implementing Secure Access Technologies

• **ZTNA solutions**[12] **–** ZTNA implementation can be either endpoint-initiated or service-initiated. In an endpoint-initiated architecture, the user initiates access to an application from an endpoint-connected device. A device-based agent communicates with the ZTNA controller to authenticate and connect the user to the needed service. In a service-initiated ZTNA, the connection is initiated by a broker between application and user. This requires a lightweight ZTNA connector to sit in front of the business applications located either on-premises or at cloud providers. Once the outbound connection from the requested application authenticates the user or application, traffic will flow through the ZTNA service provider, isolating applications from direct access via a proxy. The advantage here is that no agent is required on end-user devices, making it a better option for unmanaged or BYOD devices for partner access.

• **Software-defined wide area network (SD-WAN)**[9] **–** Zero-trust SD-WAN securely connects users, IoT/OT devices and servers without the complexity of VPNs. Instead of implicit trust within the network perimeter, it instead assumes that verification and scrutiny are prerequisites for granting access. Zero-trust SD-WAN can help enhancethe security of remote locations, while mitigating cyber risk, lowering cost and complexity and enhancing business agility.

• **Secure web gateways (SWGs)**[13] **–** The SWG sits between users and the internet to filter traffic and enforce acceptable use and security policies. Its capabilities include URL filtering, anti-malware and threat prevention and application control capabilities. Deployment can take several forms, including on physical servers, cloud-based virtual machines and services and software applications.



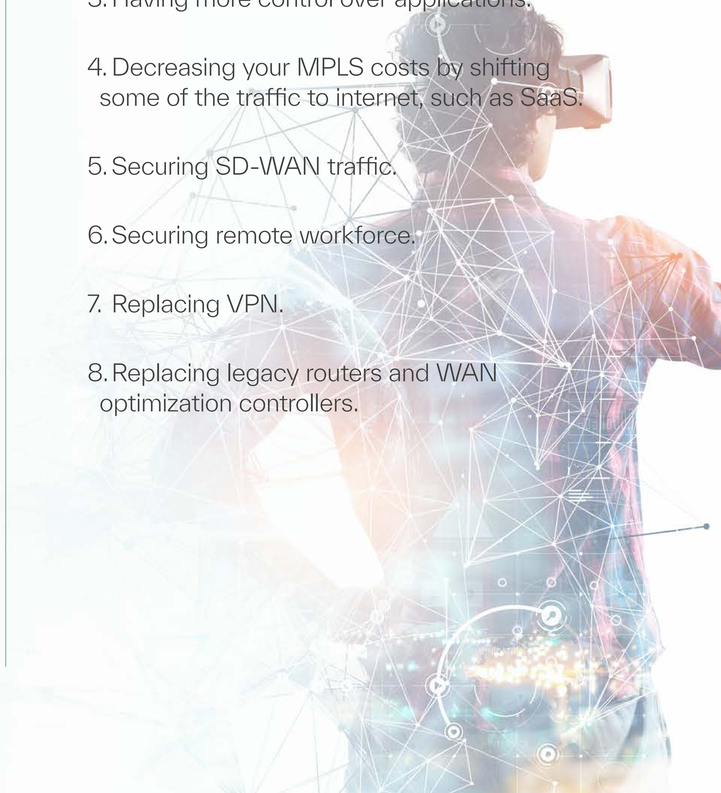
Leveraging Identity and Authentication Mechanisims

Monitoring and Visibility

Solutions to consider

Vendor Solutions for AI-Powered Cybersecurity

1. Increasing the reliability of the sites by using all the links available at the site (move to active-active configuration).
2. Getting away from MPLS and shifting to all internet.
3. Having more control over applications.
4. Decreasing your MPLS costs by shifting some of the traffic to internet, such as SaaS.
5. Securing SD-WAN traffic.
6. Securing remote workforce.
7. Replacing VPN.
8. Replacing legacy routers and WAN optimization controllers.



Designing the Zero-Trust Edge Architecture

A zero-trust architecture (ZTA) helps your customer manage today's most pressing cybersecurity and audit concerns. By instilling the core zero-trust principles of "never trust, always verify" and "assume breach," you can help bring about a new cybersecurity standard that can reduce the chance of a successful cyber incident. As an architectural framework, zero trust complements what already exists in the security stack, enabling your customer to gradually make improvements by adding solutions, service provider expansions, integrations or strategic capability consolidations.[8]

Identifying Edge Devices and Endpoints

Establishing Trust Boundaries

Implementing Secure Access Technologies

Leveraging Identity and Authentication Mechanisms

- **Multi-factor authentication (MFA)[14] –** MFA is a key component of zero trust, providing an extra layer of security by requiring multiple forms of verification before granting access to resources. MFA reduces the risk of identity theft and phishing, requiring more than just a username and password and enhances MFA security by continuously validating the user's identity, even after initial access has been granted. This continuous authentication and authorization process ensures that any change in the user's behavior or status triggers a re-authentication, further bolstering security.

- **Identity federation[15] –** Identity federation includes the technology, policies, standards and processes that allow organizations to accept digital identities, attributes and credentials to securely share information in compliance with access policies. They may have identity, credential and access management implementations of varying maturity and likely implementations that complicate sharing. Zero-trust mechanisms do not remove these requirements, even when sensitive data creates excessive risk or when maturity levels vary widely.

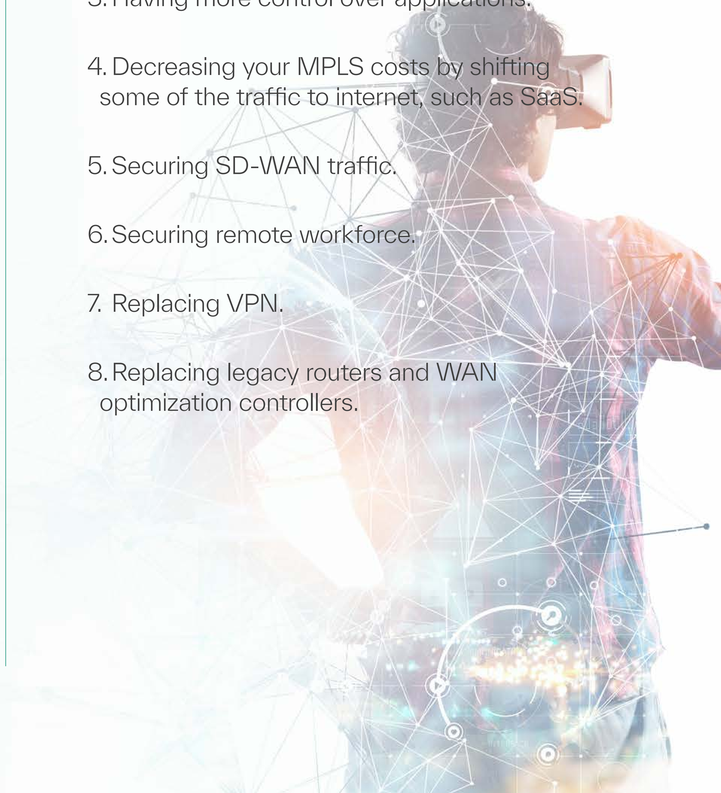
- **Continuous authentication[9] –** A key part of zero trust, continuous authentication assumes that all users, devices, applications and resources are vulnerable at any given time. This identity verification method verifies a user's identity in real-time, from the beginning of their session to the end. It makes zero trust possible by verifying the identity of users behind company devices at all times, with the goal of keeping intruders from accessing enterprise resources.

Monitoring and Visibility

Solutions to consider

Vendor Solutions for AI-Powered Cybersecurity

1. Increasing the reliability of the sites by using all the links available at the site (move to active-active configuration).
2. Getting away from MPLS and shifting to all internet.
3. Having more control over applications.
4. Decreasing your MPLS costs by shifting some of the traffic to internet, such as SaaS.
5. Securing SD-WAN traffic.
6. Securing remote workforce.
7. Replacing VPN.
8. Replacing legacy routers and WAN optimization controllers.



Designing the Zero-Trust Edge Architecture

A zero-trust architecture (ZTA) helps your customer manage today's most pressing cybersecurity and audit concerns. By instilling the core zero-trust principles of "never trust, always verify" and "assume breach," you can help bring about a new cybersecurity standard that can reduce the chance of a successful cyber incident. As an architectural framework, zero trust complements what already exists in the security stack, enabling your customer to gradually make improvements by adding solutions, service provider expansions, integrations or strategic capability consolidations.[8]

Identifying Edge Devices and Endpoints

Establishing Trust Boundaries

Implementing Secure Access Technologies

Leveraging Identity and Authentication Mechanisims

Monitoring and Visibility

- **Network traffic analysis (NTA)[16] –** NTA solutions use a combination of machine learning, behavioral modeling, and rule-based detection to generate a baseline that reflects what normal network behavior looks like for your customer. When abnormal traffic patterns or irregular network activities are detected, these tools alert you to the potential threat.

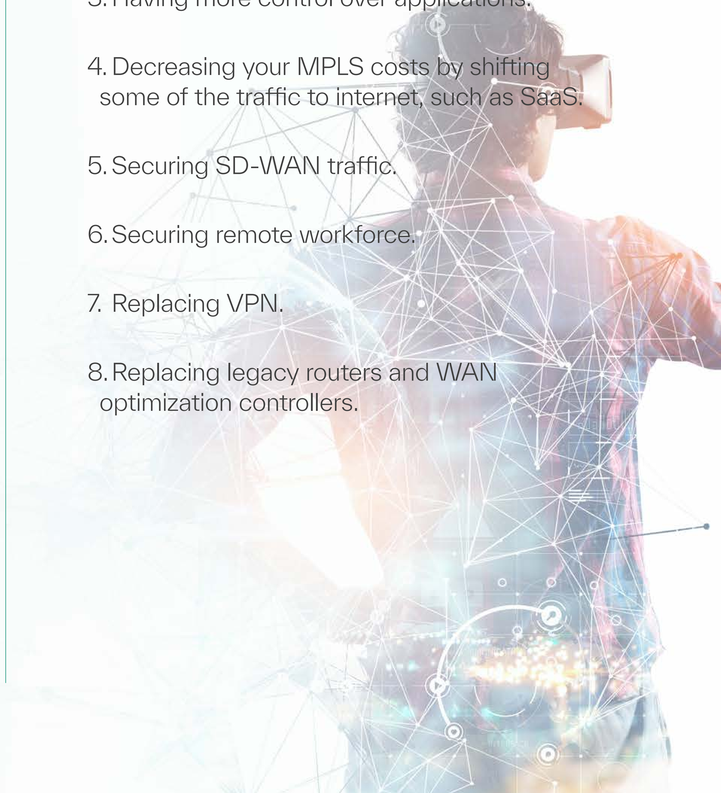
- **Endpoint detection and response (EDR)[9] –** EDR and zero trust work together to identify and respond to threats on endpoints, such as desktops, laptops and servers. Zero trust reduces a network's attack surface by eliminating implicit trust of users and devices. EDR provides visibility and remediation insight beyond basic security and enables an organization to better understand the nature of incidents, their root causes and how to effectively address them.

- **Security information and event management (SIEM)[17] –** SIEM enables your customer to continuously monitor their infrastructure for signs of potential threats or risks. It uses AI to spot changes and patterns matching current threats and proactively provides—and prioritizes—alerts on potential issues, ensuring their team can better focus their time and resources. While creating this zero-trust environment can quickly overwhelm users, using SIEM as part of zero trust gives your customer visibility and security—without disrupting the user experience.

Solutions to consider

Vendor Solutions for AI-Powered Cybersecurity

1. Increasing the reliability of the sites by using all the links available at the site (move to active-active configuration).
2. Getting away from MPLS and shifting to all internet.
3. Having more control over applications.
4. Decreasing your MPLS costs by shifting some of the traffic to internet, such as SaaS.
5. Securing SD-WAN traffic.
6. Securing remote workforce.
7. Replacing VPN.
8. Replacing legacy routers and WAN optimization controllers.



Designing the Zero-Trust Edge Architecture

A zero-trust architecture (ZTA) helps your customer manage today's most pressing cybersecurity and audit concerns. By instilling the core zero-trust principles of "never trust, always verify" and "assume breach," you can help bring about a new cybersecurity standard that can reduce the chance of a successful cyber incident. As an architectural framework, zero trust complements what already exists in the security stack, enabling your customer to gradually make improvements by adding solutions, service provider expansions, integrations or strategic capability consolidations.[8]

Identifying Edge Devices and Endpoints

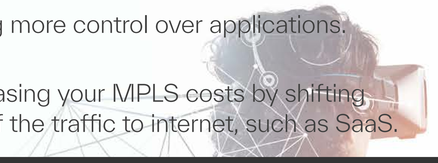
Establishing Trust Boundaries

Implementing Secure Access Technologies

Leveraging Identity and Authentication Mechanisims

Vendor Solutions for AI-Powered Cybersecurity

1. Increasing the reliability of the sites by using all the links available at the site (move to active-active configuration).
2. Getting away from MPLS and shifting to all internet.
3. Having more control over applications.
4. Decreasing your MPLS costs by shifting some of the traffic to internet, such as SaaS.



Solutions to consider

Dell Technologies

- **Dell EMC PowerEdge Servers –** These servers provide a cyber-resilient infrastructure with built-in security features that support zero trust principles. They offer secure boot, system lockdown and firmware protection.
- **Dell EMC OpenManage –** This suite includes tools for managing and automating server infrastructure, ensuring consistent security configurations and compliance with zero trust policies.
- **Dell EMC PowerScale –**This scale-out NAS solution follows the zero trust model and can be deployed across the enterprise, from edge to core to cloud, handling demanding file-based workloads securely.

HPE Aruba

- **HPE Aruba Networking Zero Trust Network Access (ZTNA) –** This advanced ZTNA service uses identity, policy and context to broker secure, one-to-one connections to private apps (even VoIP, AS400 and ICMP)—replacing VPN without network access or exposure.
- **Secure web gateway (SWG) –** Using advanced SSL inspection, URL filtering and DNS filtering, this SWG ensures that authorized users get fast, secure internet access—while protecting the business from Internet- based threats.
- **Cloud access security broker (CASB) –** This solution mediates the connections between users and cloud applications, helps discover shadow IT to apps and ensures sensitive data in motion remains protected, while helping prevent cyberthreats.

Palo Alto Networks

Palo Alto's portfolio of platforms consolidates best-in-class capabilities under a single, unified cybersecurity solution to outpace cyberthreats with:

- **Network Security –** Leverage an industry-leading firewall platform and comprehensive Prisma SASE solution available across hardware, software and cloud-based form factors.
- **Cloud Security –** Comprehensive security through Prisma Cloud from development to runtime across multicloud and hybrid environments
- **Security Operations –** A new approach to SOC with Cortex XDR, XSOAR and XSIAM providing advanced visibility, data, analytics and automation capabilities.

Splunk

- **Splunk Enterprise Security (ES) –** Get real-time monitoring, advanced threat detection, and data-driven security insights for fast response to potential threats. Robust analytics capabilities enhance visibility for easier management of tasks to complex cyber threats.
- **Splunk SOAR (Security Orchestration, Automation, and Response) –** Streamline security operations across security tools and accelerate incident response, helping teams efficiently resolve threats while freeing time for strategic activities. Customizable playbooks ensure a proactive and adaptive security posture.
- **Splunk User Behavior Analytics (UBA) –** Detect unusual behavior and potential threats with contextual insights that help security teams quickly identify and mitigate risks. Supports multiple use cases to enhance overall security visibility and operational effectiveness.

Building Zero-Trust Policies and Controls

Role-Based Access Control (RBAC)

Where zero trust provides no access until trust has been established, RBAC is that trust. It simplifies access management by assigning rights based on roles, consistent with the principle of least privilege to reduce the risk of unauthorized access. It defines access for each user and establishes trust through authentication and other real-time checks. From a nearly incomprehensible mishmash of network access, application control, and data management rules, RBAC provides a layer of abstraction that can turn into something that is not only manageable but also auditable—a key requirement for many regulatory frameworks.[19]

Assigning permissions based on job roles – When combined with strong design and modern application capabilities, identity and access management (IAM) and RBAC make a zero-trust network architecture a solid base for improving security and simplifying identity management.[19] As a user moves from one role to another, managing their security profile means reviewing the roles available to that user instead of finding every instance in which that user is mentioned in an access control list.[19]

- Dynamic access control based on contextual factors – In the context of zero trust, access control is dynamic and adaptive. It continuously evaluates trustworthiness based on factors like user behavior, device health and network location. This approach goes beyond traditional perimeter-based security measures, focusing on securing individual resources and data rather than relying solely on network boundaries.[10] Furthermore, the minimal privileges required are dynamic, that is, dependent on time and context. Elements of dynamic context can include location, security assessment of the client device, behavioral analytics and the known threats or active attacks in the environment.

Application Layer Security ›

Data Protection Measures ›

Incident Response and Recovery ›

Solutions to consider ›

Role Based Access

Building Zero-Trust Policies and Controls

Application Layer Security

In any organization, applications are valuable—and vulnerable—as they are typically easy targets for breaches. Attackers know this all too well as they actively attempt to compromise your customer's apps for easy entry to their intellectual property and data. Help them continuously protect data accessed via applications and APIs with a zero-trust strategy that helps them find the right balance between providing access and maintaining control.[20]

• **Securing APIs and microservices –** Fast-growing distributed networks use myriad microservices and application programming interfaces (APIs). In fact, API adoption is outpacing the ability to create strong governance and security tools around this layer. APIs are also being used to connect to legacy applications that lack the security of cloud-native services and architectures. To effectively manage API security, zero-trust security models need to extend beyond the user and device layers to the application, data and integration layers. To manage, control and secure APIs, your customer requires an API security platform that enables them to:

- Discover and test APIs
- Evaluate API risk posture
- Stop API attacks
- Analyze APIs for threat hunting and research

• **Implementing zero trust for cloud applications –** Most organizations today use at least some applications or infrastructure in the cloud, but these cloud apps and environments are typically operated by cloud service and SaaS providers. With multiple applications spread out across multiple locations (and multiple providers), it's difficult for your customer to see who is accessing their applications and data, with what devices and how data is being shared and used—let alone protect it all.

As your customers move to the cloud, implementing a zero-trust strategy using these steps will help to unify and protect cloud resources:[21]

1.Identify what type of applications and data your customer has, where they are and who is accessing and using them. Then, define the data, applications, assets and services most critical to their business.
2. Map the transaction flows and how your applications work.
3. Architect the new cloud infrastructure and create boundaries between users and applications.
4. Build your customer's zero-trust policies based on who should have access to what and enforce contextual access controls based on least privilege. Train users on what's expected when accessing cloud apps and data.
5. Monitor and maintain the zero-trust environment by continuously inspecting and logging all traffic to identify unusual activity and decide how to make policies more secure.

Container security and orchestration[22] **-** As container environments grow in complexity, securing containers must consider everything from the applications running in containers to the infrastructure on which those containers run. Building security into a container pipeline includes starting with trusted images, managing access with a private registry, integrating security tests to automate deployments and continuously securing the infrastructure. Containers also require different security policies. Thus, container orchestrators should be configured to define security policies for containers and only enable necessary communication. These two zero-trust solutions can take it to the next level:

• ZTNA allows organizations to enforce secure communication between containers and microservices with flexible, centralized security policies that are not dependent on the container environment itself.

• SASE allows organizations to embed security measures into the network fabric itself, ensuring that wherever containers run, they are inherently secure when they connect to the network.

Data Protection Measures

Incident Response and Recovery

Solutions to consider

Building Zero-Trust Policies and Controls

Application Layer Security

In any organization, applications are valuable—and vulnerable—as they are typically easy targets for breaches. Attackers know this all too well as they actively attempt to compromise your customer's apps for easy entry to their intellectual property and data. Help them continuously protect data accessed via applications and APIs with a zero-trust strategy that helps them find the right balance between providing access and maintaining control.[20]

• **Securing APIs and microservices –** Fast-growing distributed networks use myriad microservices and application programming interfaces (APIs). In fact, API adoption is outpacing the ability to create strong governance and security tools around this layer. APIs are also being used to connect to legacy applications that lack the security of cloud-native services and architectures. To effectively manage API security, zero-trust security models need to extend beyond the user and device layers to the application, data and integration layers. To manage, control and secure APIs, your customer requires an API security platform that enables them to:

- Discover and test APIs
- Evaluate API risk posture
- Stop API attacks
- Analyze APIs for threat hunting and research

• **Implementing zero trust for cloud applications –** Most organizations today use at least some applications or infrastructure in the cloud, but these cloud apps and environments are typically operated by cloud service and SaaS providers. With multiple applications spread out across multiple locations (and multiple providers), it's difficult for your customer to see who is accessing their applications and data, with what devices and how data is being shared and used—let alone protect it all.

As your customers move to the cloud, implementing a zero-trust strategy using these steps will help to unify and protect cloud resources:[21]

1.Identify what type of applications and da
is accessing and using them. Then, define t
critical to their business.
2. Map the transaction flows and how your
3. Architect the new cloud infrastructure an
4. Build your customer's zero-trust policies
enforce contextual access controls based o
when accessing cloud apps and data.
5. Monitor and maintain the zero-trust env
all traffic to identify unusual activity and deci

Container security and orchestration[22]
securing containers must consider everythi
the infrastructure on which those containe
includes starting with trusted images, man
security tests to automate deployments and
Containers also require different security p
be configured to define security policies for
communication. These two zero-trust solut

• ZTNA allows organizations to enforce sec
microservices with flexible, centralized sec
container environment itself.

• SASE allows organizations to embed secu
ensuring that wherever containers run, they
network.

Data Protection Measures

Incident Response and Recovery

Solutions to consider

Role Based Access

Role-Based Access Control (RBAC)

Where zero trust provides no access until trust has been established, RBAC is that trust. It simplifies access management by assigning rights based on roles, consistent with the principle of least privilege to reduce the risk of unauthorized access. It defines access for each user and establishes trust through authentication and other real-time checks. From a nearly incomprehensible mishmash of network access, application control, and data management rules, RBAC provides a layer of abstraction that can turn into something that is not only manageable but also auditable—a key requirement for many regulatory frameworks.[19]

Assigning permissions based on job roles – When combined with strong design and modern application capabilities, identity and access management (IAM) and RBAC make a zero-trust network architecture a solid base for improving security and simplifying identity management.[19] As a user moves from one role to another, managing their security profile means reviewing the roles available to that user instead of finding every instance in which that user is mentioned in an access control list.[19]• Dynamic access control based on contextual factors – In the context of zero trust, access control is dynamic and adaptive. It continuously evaluates trustworthiness based on factors like user behavior, device health and network location. This approach goes beyond traditional perimeter-based security measures, focusing on securing individual resources and data rather than relying solely on network boundaries.[10] Furthermore, the minimal privileges required are dynamic, that is, dependent on time and context. Elements of dynamic context can include location, security assessment of the client device, behavioral analytics and the known threats or active attacks in the environment.

Role Based Access

Building Zero-Trust Policies and Controls

Application Layer Security

Data Protection Measures

Zero-trust data protection (ZTDP) is a security framework that assumes no inherent trust and requires verification from anyone trying to access data. It emphasizes continuous authentication and strict access controls to mitigate cyber threats and safeguard sensitive information. ZTDP grants access to data on a least-privileged basis that is continually assessed, dynamically adapting access based on changing context, including users, devices, applications, threat types, geolocations, access times and data characteristics.[9]

- **Encryption and data masking –** Encryption is vital for implementing a zero-trust architecture as data is encrypted to achieve confidentiality and digital signing for integrity verification. Zero-trust data encryption not only secures your customer's data from unauthorized use, but it also ensures compliance with regulations and standards, such as General Data Protection Regulation (GDPR), that require organizations to appropriately classify and secure data.

- **Data loss prevention (DLP)[23] –** Many organizations believe their DLP deployments aren't compatible with zero trust. But the problem is legacy DLP. Legacy DLP focuses on endpoint and network security, where modern DLP—which is compatible with zero trust—protects data in SaaS-based applications.

ZTNA enables least-privileged access to data, device and identity levels and must be built into the platform's core, along with the ability to automate and orchestrate, but with the right context for a more accurate response. Building and dynamically enforcing DLP components, such as data classification and policy enforcement at all locations, is key. Your customer will benefit from DLP solutions that offer content inspection, data lineage for improved classification and visibility and incident response on a zero-trust-enabled platform. A well-defined data classification technology is at the center of a zero-trust approach to DLP, which helps to prioritize the most sensitive data and increase the effectiveness of implementing a thorough ZTNA framework.

- **Secure data handling policies[24] –** An information protection strategy needs to encompass your customer's entire digital content.

- Classify, label and discover sensitive data
- Apply encryption, access control and content markings
- Control access to data
- Prevent data leakage
- Manage insider risks
- Delete unnecessary sensitive data

Incident Response and Recovery

Solutions to consider

Building Zero-Trust Policies and Controls

Application Layer Security

Data Protection Measures

Zero-trust data protection (ZTDP) is a security framework that assumes no inherent trust and requires verification from anyone trying to access data. It emphasizes continuous authentication and strict access controls to mitigate cyber threats and safeguard sensitive information. ZTDP grants access to data on a least-privileged basis that is continually assessed, dynamically adapting access based on changing context, including users, devices, applications, threat types, geolocations, access times and data characteristics.[9]

- **Encryption and data masking –** Encryption is vital for implementing a zero-trust architecture as data is encrypted to achieve confidentiality and digital signing for integrity verification. Zero-trust data encryption not only secures your customer's data from unauthorized use, but it also ensures compliance with regulations and standards, such as General Data Protection Regulation (GDPR), that require organizations to appropriately classify and secure data.

- **Data loss prevention (DLP)**[23] **–** Many organizations believe their DLP deployments aren't compatible with zero trust. But the problem is legacy DLP. Legacy DLP focuses on endpoint and network security, where modern DLP—which is compatible with zero trust—protects data in SaaS-based applications.

ZTNA enables least-privileged access to data, device and identity levels and must be built into the platform's core, along with the ability to automate and orchestrate, but with the right context for a more accurate response. Building and dynamically enforcing DLP components, such as data classification and policy enforcement at all locations, is key. Your customer will benefit from DLP solutions that offer content inspection, data lineage for improved classification and visibility and incident response on a zero-trust-enabled p
technology is at the center of a zero-trust ap
the most sensitive data and increase the effi
ZTNA framework.

- **Secure data handling policies**[24] **–** An i
encompass your customer's entire digital co

- Classify, label and discover sensitive data
- Apply encryption, access control and cont
- Control access to data
- Prevent data leakage
- Manage insider risks
- Delete unnecessary sensitive data

Incident Response and Recovery

Solutions to consider

Role Based Access

Role-Based Access Control (RBAC)

Where zero trust provides no access until trust has been established, RBAC is that trust. It simplifies access management by assigning rights based on roles, consistent with the principle of least privilege to reduce the risk of unauthorized access. It defines access for each user and establishes trust through authentication and other real-time checks. From a nearly incomprehensible mishmash of network access, application control, and data management rules, RBAC provides a layer of abstraction that can turn into something that is not only manageable but also auditable—a key requirement for many regulatory frameworks.[19]

Assigning permissions based on job roles – When combined with strong design and modern application capabilities, identity and access management (IAM) and RBAC make a zero-trust network architecture a solid base for improving security and simplifying identity management.[19] As a user moves from one role to another, managing their security profile means reviewing the roles available to that user instead of finding every instance in which that user is mentioned in an access control list.[19]• Dynamic access control based on contextual factors – In the context of zero trust, access control is dynamic and adaptive. It continuously evaluates trustworthiness based on factors like user behavior, device health and network location. This approach goes beyond traditional perimeter-based security measures, focusing on securing individual resources and data rather than relying solely on network boundaries.[10] Furthermore, the minimal privileges required are dynamic, that is, dependent on time and context. Elements of dynamic context can include location, security assessment of the client device, behavioral analytics and the known threats or active attacks in the environment.

Role Based Access

Building Zero-Trust Policies and Controls

Application Layer Security

Data Protection Measures

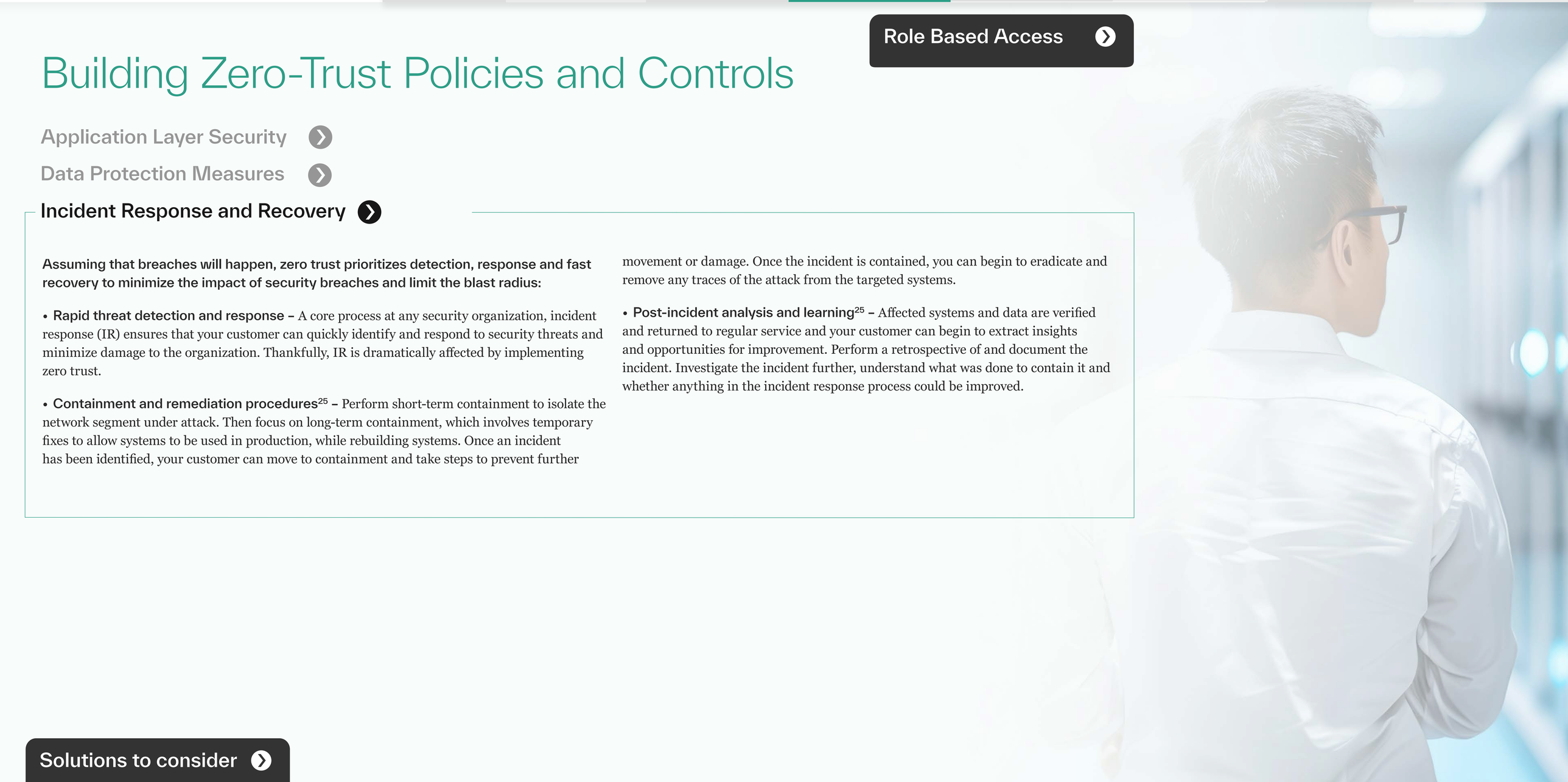
Incident Response and Recovery

Assuming that breaches will happen, zero trust prioritizes detection, response and fast recovery to minimize the impact of security breaches and limit the blast radius:

- **Rapid threat detection and response –** A core process at any security organization, incident response (IR) ensures that your customer can quickly identify and respond to security threats and minimize damage to the organization. Thankfully, IR is dramatically affected by implementing zero trust.

- **Containment and remediation procedures[25] –** Perform short-term containment to isolate the network segment under attack. Then focus on long-term containment, which involves temporary fixes to allow systems to be used in production, while rebuilding systems. Once an incident has been identified, your customer can move to containment and take steps to prevent further movement or damage. Once the incident is contained, you can begin to eradicate and remove any traces of the attack from the targeted systems.

- **Post-incident analysis and learning[25] –** Affected systems and data are verified and returned to regular service and your customer can begin to extract insights and opportunities for improvement. Perform a retrospective of and document the incident. Investigate the incident further, understand what was done to contain it and whether anything in the incident response process could be improved.



Solutions to consider

Building Zero-Trust Policies and Controls

Application Layer Security

Data Protection Measures

Incident Response and Recovery

Assuming that breaches will happen, zero trust prioritizes detection, response and fast recovery to minimize the impact of security breaches and limit the blast radius:

• **Rapid threat detection and response –** A core process at any security organization, incident response (IR) ensures that your customer can quickly identify and respond to security threats and minimize damage to the organization. Thankfully, IR is dramatically affected by implementing zero trust.

• **Containment and remediation procedures**[25] **–** Perform short-term containment to isolate the network segment under attack. Then focus on long-term containment, which involves temporary fixes to allow systems to be used in production, while rebuilding systems. Once an incident has been identified, your customer can move to containment and take steps to prevent further movement or damage. Once the incident is
remove any traces of the attack from the ta

• **Post-incident analysis and learning**[25] **–**
and returned to regular service and your cu
and opportunities for improvement. Perfor
incident. Investigate the incident further, u
whether anything in the incident response p

Solutions to consider

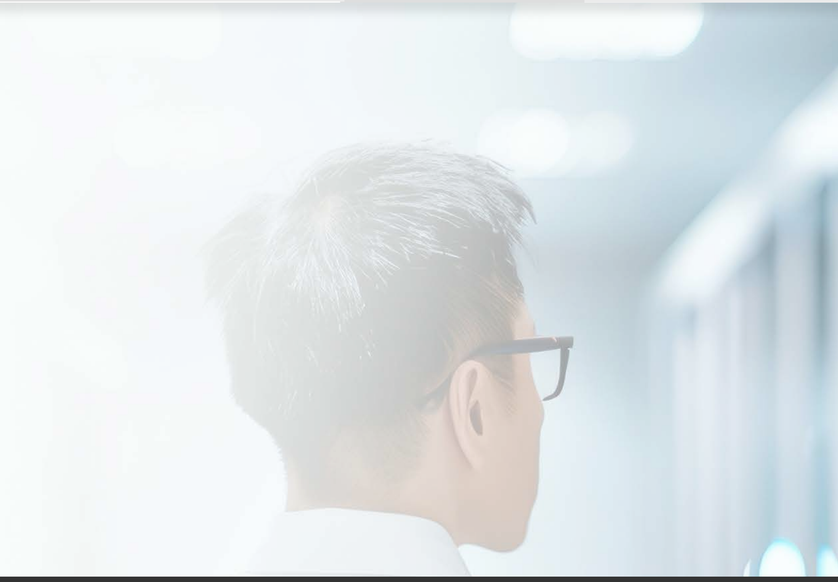
Role Based Access

Role-Based Access Control (RBAC)

Where zero trust provides no access until trust has been established, RBAC is that trust. It simplifies access management by assigning rights based on roles, consistent with the principle of least privilege to reduce the risk of unauthorized access. It defines access for each user and establishes trust through authentication and other real-time checks. From a nearly incomprehensible mishmash of network access, application control, and data management rules, RBAC provides a layer of abstraction that can turn into something that is not only manageable but also auditable—a key requirement for many regulatory frameworks.[19]

Assigning permissions based on job roles – When combined with strong design and modern application capabilities, identity and access management (IAM) and RBAC make a zero-trust network architecture a solid base for improving security and simplifying identity management.[19] As a user moves from one role to another, managing their security profile means reviewing the roles available to that user instead of finding every instance in which that user is mentioned in an access control list.[19]• Dynamic access control based on contextual factors – In the context of zero trust, access control is dynamic and adaptive. It continuously evaluates trustworthiness based on factors like user behavior, device health and network location. This approach goes beyond traditional perimeter-based security measures, focusing on securing individual resources and data rather than relying solely on network boundaries.[10] Furthermore, the minimal privileges required are dynamic, that is, dependent on time and context. Elements of dynamic context can include location, security assessment of the client device, behavioral analytics and the known threats or active attacks in the environment.

Building Zero-Trust Policies and Controls



Solutions to consider

Dell Technologies

- **Dell EMC PowerEdge Servers –** These servers provide a cyber-resilient infrastructure with built-in security features that support zero trust principles. They offer secure boot, system lockdown and firmware protection.
- **Dell EMC OpenManage –** This suite includes tools for managing and automating server infrastructure, ensuring consistent security configurations and compliance with zero trust policies.
- **Dell EMC PowerScale –** This scale-out NAS solution follows the zero trust model and can be deployed across the enterprise, from edge to core to cloud, handling demanding file-based workloads securely.

HPE Aruba

- **HPE Aruba Networking Zero Trust Network Access (ZTNA) –** This advanced ZTNA service uses identity, policy and context to broker secure, one-to-one connections to private apps (even VoIP, AS400 and ICMP)—replacing VPN without network access or exposure.
- **Secure web gateway (SWG) –** Using advanced SSL inspection, URL filtering and DNS filtering, this SWG ensures that authorized users get fast, secure internet access—while protecting the business from Internet- based threats.
- **Cloud access security broker (CASB) –** This solution mediates the connections between users and cloud applications, helps discover shadow IT to apps and ensures sensitive data in motion remains protected, while helping prevent cyberthreats.

Palo Alto Networks

Palo Alto's portfolio of platforms consolidates best-in-class capabilities under a single, unified cybersecurity solution to outpace cyberthreats with:

- **Network Security –** Leverage an industry-leading firewall platform and comprehensive Prisma SASE solution available across hardware, software and cloud-based form factors.
- **Cloud Security –** Comprehensive security through Prisma Cloud from development to runtime across multicloud and hybrid environments
- **Security Operations –** A new approach to SOC with Cortex XDR, XSOAR and XSIAM providing advanced visibility, data, analytics and automation capabilities.

Splunk

- **Splunk Enterprise Security (ES) –** Get real-time monitoring, advanced threat detection, and data-driven security insights for fast response to potential threats. Robust analytics capabilities enhance visibility for easier management of tasks to complex cyber threats.
- **Splunk SOAR (Security Orchestration, Automation, and Response) –** Streamline security operations across security tools and accelerate incident response, helping teams efficiently resolve threats while freeing time for strategic activities. Customizable playbooks ensure a proactive and adaptive security posture.
- **Splunk User Behavior Analytics (UBA) –** Detect unusual behavior and potential threats with contextual insights that help security teams quickly identify and mitigate risks. Supports multiple use cases to enhance overall security visibility and operational effectiveness.

Challenges and Considerations

While ZTE completely disrupts traditional network security practices, it also brings significant challenges and considerations that will require significant planning and agility. These challenges and considerations include:

Integration with Existing Structure[26]

User Experience and Productivity

Scalability and Performance

Compliance and Regulatory Requirements

Solutions to consider

Challenges and Considerations

While ZTE completely disrupts traditional network security practices, it also brings significant challenges and considerations that will require significant planning and agility. These challenges and considerations include:

Integration with Existing Structure[26]

There are multiple challenges in integrating an existing infrastructure into a ZTE framework, particularly if it's a legacy network. The thousands of incompatible IT, operational technology (OT) and IoT devices can complicate integration into an existing network and may require a significant infrastructure overhaul as a result. In fact, some components may need to be modernized and some legacy hardware may not meet ZTE requirements at all, forcing replacement of those devices for a smoother transition to a ZTE network.

Another integration challenge concerns applications and services built on non-web protocols—such as RDP/VDI for remote access and SIP/VoIP for voice—and without standardized ZTE procedures. These applications would either need to be modernized for the cloud or replaced for a successful ZTE implementation.

Finally, capacity constraints can also wreak havoc on a ZTE implementation. Your customer may need to consider additional workarounds or make significant upgrades if they are near |capacity limits—or pursue a cloud migration strategy before implementing ZTE. Both actions would further complicate a transition to ZTE.

User Experience and Productivity

Scalability and Performance

Compliance and Regulatory Requirements

Solutions to consider

Challenges and Considerations

While ZTE completely disrupts traditional network security practices, it also brings significant challenges and considerations that will require significant planning and agility. These challenges and considerations include:

Integration with Existing Structure[26]

User Experience and Productivity

One of the key challenges for users is ensuring that they can access the network with little trouble and have the bandwidth needed to be productive throughout the day, regardless of where they're working. In terms of security, a fine balance needs to be struck between stringency and convenience or users will tire of re-authenticating themselves at every turn and seek their own workarounds—which may then unearth yet another security issue. Users also require top network performance throughout the day to be at their most productive. Sending traffic to a central data center and backhauling it out to a remote location can cause frustrating delays that impact productivity.

ZTE facilitates an enhanced user experience and productivity by improving network performance and throughput and eliminating the need for multiple authentications. Globally available internet on-ramps reduce the need for backhauls, driving latency down and significantly accelerating application performance for a comprehensive digital experience.

Scalability and Performance

Compliance and Regulatory Requirements

Solutions to consider

Challenges and Considerations

While ZTE completely disrupts traditional network security practices, it also brings significant challenges and considerations that will require significant planning and agility. These challenges and considerations include:

Integration with Existing Structure[26]

User Experience and Productivity

Scalability and Performance

Where traditional VPNs typically backhaul remote users' traffic through centralized data centers, ZTE uses cloud on-ramps for global connectivity, eliminating bandwidth congestion and the need for backhauling traffic and boosting performance. Zero trust can be scaled. Gradually introducing zero-trust security does not disrupt the continuity of an existing cybersecurity strategy. Organizations may begin by locking down crucial assets, but because they are not entirely abandoning one system for another, they are exposed to fewer threats.

Compliance and Regulatory Requirements

Solutions to consider

Challenges and Considerations

While ZTE completely disrupts traditional network security practices, it also brings significant challenges and considerations that will require significant planning and agility. These challenges and considerations include:

Integration with Existing Structure[26]

User Experience and Productivity

Scalability and Performance

Compliance and Regulatory Requirements

Zero trust helps reduce risk, simplify governance and increase maturity within the compliance framework. By employing security protocols and a zero-trust method, your customer can gain visibility into risk at all levels. By enforcing strict access controls and continuously monitoring a user's activities, zero trust helps maintain regulatory compliance—particularly salient for those industries with a high regulatory burden.

Solutions to consider

Challenges and Considerations

While ZTE completely disrupts traditional network security practices, it also brings significant challenges and considerations that will require significant planning and agility. These challenges and considerations include:

Integration with Existing Structure[26]

User Experience and Productivity

ce

Solutions to consider

Dell Technologies

- **Dell EMC PowerEdge Servers –** These servers provide a cyber-resilient infrastructure with built-in security features that support zero trust principles. They offer secure boot, system lockdown and firmware protection.
- **Dell EMC OpenManage –** This suite includes tools for managing and automating server infrastructure, ensuring consistent security configurations and compliance with zero trust policies.
- **Dell EMC PowerScale –** This scale-out NAS solution follows the zero trust model and can be deployed across the enterprise, from edge to core to cloud, handling demanding file-based workloads securely.

HPE Aruba

- **HPE Aruba Networking Zero Trust Network Access (ZTNA) –** This advanced ZTNA service uses identity, policy and context to broker secure, one-to-one connections to private apps (even VoIP, AS400 and ICMP)—replacing VPN without network access or exposure.
- **Secure web gateway (SWG) –** Using advanced SSL inspection, URL filtering and DNS filtering, this SWG ensures that authorized users get fast, secure internet access—while protecting the business from Internet- based threats.
- **Cloud access security broker (CASB) –** This solution mediates the connections between users and cloud applications, helps discover shadow IT to apps and ensures sensitive data in motion remains protected, while helping prevent cyberthreats.

Palo Alto Networks

Palo Alto's portfolio of platforms consolidates best-in-class capabilities under a single, unified cybersecurity solution to outpace cyberthreats with:

- **Network Security –** Leverage an industry-leading firewall platform and comprehensive Prisma SASE solution available across hardware, software and cloud-based form factors.
- **Cloud Security –** Comprehensive security through Prisma Cloud from development to runtime across multicloud and hybrid environments
- **Security Operations –** A new approach to SOC with Cortex XDR, XSOAR and XSIAM providing advanced visibility, data, analytics and automation capabilities.

Splunk

- **Splunk Enterprise Security (ES) –** Get real-time monitoring, advanced threat detection, and data-driven security insights for fast response to potential threats. Robust analytics capabilities enhance visibility for easier management of tasks to complex cyber threats.
- **Splunk SOAR (Security Orchestration, Automation, and Response) –** Streamline security operations across security tools and accelerate incident response, helping teams efficiently resolve threats while freeing time for strategic activities. Customizable playbooks ensure a proactive and adaptive security posture.
- **Splunk User Behavior Analytics (UBA) –** Detect unusual behavior and potential threats with contextual insights that help security teams quickly identify and mitigate risks. Supports multiple use cases to enhance overall security visibility and operational effectiveness.

Opportunities for MSPs and 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 6

Solutions to consider ›

Opportunities for MSPs and 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 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 craft a zero-trust vision.
- 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.
- Identify interdependencies between the zero-trust implementation and other IT and business projects.

2 3 4 5 6

Solutions to consider ›

Opportunities for MSPs and 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 Refine the Business Continuity Plan** | 3 | 4 | 5 | 6

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.

Solutions to consider ›

Opportunities for MSPs and 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 6

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.

Solutions to consider ›

Opportunities for MSPs and 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 6

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 801-171, ISO 27001, NERC-CIP, SOC 1and2, 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.
  - **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.

Solutions to consider ›

Opportunities for MSPs and 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

6

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.

Solutions to consider ›

Opportunities for MSPs and 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

6 Sell and Build SASE and XDR into the Security Stack

According to Gartner, "by 2025, at least 60% of enterprises will have explicit strategies and timelines for SASE adoption encompassing user, branch, and edge access, up from 10% in 2020."[15] Security leaders will also want to consolidate their products/vendors, be more proactive in their response to threats, and drive greater efficiency—and they're increasingly turning to MSPs and MSSPs who truly understand their security challenges.

- Perform a gap analysis and establish a high-level SASE strategy and roadmap that's closely aligned with business goals and wider organizational strategic initiatives (such as cloud migration, cybersecurity policies, and IT strategy plans). Ensure the plan leverages the customer's existing assets and enables them to transition to a SASE model over time.
- Assess your client's current network and security environment, and the resources they have available, to determine which services they need, the processes to be used, what technologies will be deployed, and the training required.
- If your customer already has an SD-WAN, they may only need SSE capabilities. If they don't, determine whether they can benefit from SASE now or whether SSE can be an on-ramp for SASE.
- Evaluate the point solutions your customer has and any underutilized functionality, as well as the level of automation and integration between them, and consider a consolidation strategy anchored with XDR.
- Help your customer understand the synergistic value offered by XDR—for example, underlying data lake foundation with lower-cost and flexible data storage, functional orchestration and automation, and advanced security analytics—and not just in how you can pare down the number of solutions and/or vendors.
- Deliver XDR as a service to minimize maintenance for you and your customer.
- Cut time to sale by packaging up or bundling solutions you've already vetted—or provide a menu of pre-vetted vendor solutions from which to choose.

Solutions to consider ›

Opportunities for MSPs and 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 6

Solutions to consider

Dell Technologies

- **Dell EMC PowerEdge Servers –** These servers provide a cyber-resilient infrastructure with built-in security features that support zero trust principles. They offer secure boot, system lockdown and firmware protection.
- **Dell EMC OpenManage –** This suite includes tools for managing and automating server infrastructure, ensuring consistent security configurations and compliance with zero trust policies.
- **Dell EMC PowerScale –** This scale-out NAS solution follows the zero trust model and can be deployed across the enterprise, from edge to core to cloud, handling demanding file-based workloads securely.

HPE Aruba

- **HPE Aruba Networking Zero Trust Network Access (ZTNA) –** This advanced ZTNA service uses identity, policy and context to broker secure, one-to-one connections to private apps (even VoIP, AS400 and ICMP)—replacing VPN without network access or exposure.
- **Secure web gateway (SWG) –** Using advanced SSL inspection, URL filtering and DNS filtering, this SWG ensures that authorized users get fast, secure internet access—while protecting the business from Internet- based threats.
- **Cloud access security broker (CASB) –** This solution mediates the connections between users and cloud applications, helps discover shadow IT to apps and ensures sensitive data in motion remains protected, while helping prevent cyberthreats.

Palo Alto Networks

Palo Alto's portfolio of platforms consolidates best-in-class capabilities under a single, unified cybersecurity solution to outpace cyberthreats with:

- **Network Security –** Leverage an industry-leading firewall platform and comprehensive Prisma SASE solution available across hardware, software and cloud-based form factors.
- **Cloud Security –** Comprehensive security through Prisma Cloud from development to runtime across multicloud and hybrid environments
- **Security Operations –** A new approach to SOC with Cortex XDR, XSOAR and XSIAM providing advanced visibility, data, analytics and automation capabilities.

Splunk

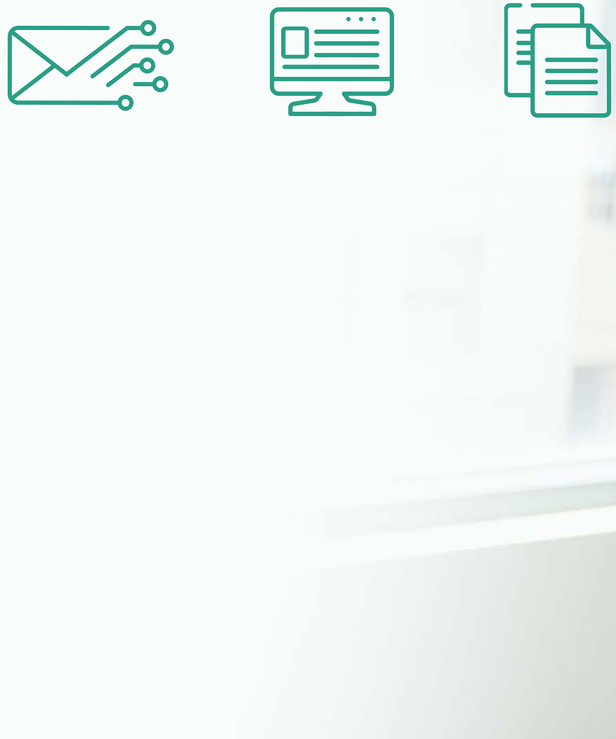
- **Splunk Enterprise Security (ES) –** Get real-time monitoring, advanced threat detection, and data-driven security insights for fast response to potential threats. Robust analytics capabilities enhance visibility for easier management of tasks to complex cyber threats.
- **Splunk SOAR (Security Orchestration, Automation, and Response) –** Streamline security operations across security tools and accelerate incident response, helping teams efficiently resolve threats while freeing time for strategic activities. Customizable playbooks ensure a proactive and adaptive security posture.
- **Splunk User Behavior Analytics (UBA) –** Detect unusual behavior and potential threats with contextual insights that help security teams quickly identify and mitigate risks. Supports multiple use cases to enhance overall security visibility and operational effectiveness.

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 address your most critical cybersecurity needs.

Our sponsors are listed on the next page, along with contact information to reach a TD SYNNEX security professional. Contact us … we're here to help.

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.

DELL Technologies AUTHORIZED DISTRIBUTOR

Visit our portal today at https://www.tdsynnex.com/na/us/cybersolv/dell-technologies

HPE aruba networking

Need help quoting HPE Aruba Networking security solutions or have questions? Contact Kristen.Vargo@tdsynnex.com, your HPE Aruba Networking EdgeConnect and SSE Sales Representative at TD SYNNEX.

paloalto NETWORKS

For more information, please reach out to panwbd@tdsynnex.com.

splunk> a CISCO company

For more information, email SplunkBD@tdsynnex.com .

References and Further Reading

1.Gartner Glossary. “Secure Access Service Edge (SASE).”

2.VMware. “What is Zero Trust Edge?,” Retrieved May 13, 2024.

3.Palo Alto Networks. “What is Zero Trust Edge (ZTE)?,” Retrieved May 8, 2024.

4.Forrester. “Introducing the Zero Trust Edge Architecture for Security and Network Services.” August 02, 2021.

5.StrongDM.com. “Zero Trust vs. the Principle of Least Privilege: What’s the Difference?”

6.“Harnessing Zero Trust Security,” ISACA.org. Nov. 18, 2020.

7. “ZeroTrust, ZTA, and ZTNA: What’s the Difference?” CSOOnline.com, March 15, 2021.

8. “Top Management Considerations for Zero Trust,” ISACA.org, Dec. 26, 2023.

9.Generated by AI, 05/15/2024.

10. “Access Control in Zero Trust Ensuring Robust Security,” ISMS.online, Oct. 3, 2023.

11. “Software-Defined Perimeter (SDP) and Zero Trust,” CloudSecurityAlliance.org, May 27, 2020.

12.What Is Zero Trust Network Access (ZTNA)?,” VMware.com, retrieved May 15, 2024.

13. “What is a Secure Web Gateway?,” PaloAltoNetworks.com, retrieved May 15, 2024.

14.“Enhancing Security with Multi-Factor Authentication in Zero Trust Model,” ISMS.online, Oct. 9, 2022.

15.“Advancing Zero Trust Maturity Throughout the User Pillar,” Defense.gov, PP-23-0208, April 2023.

16. “What Is Network Traffic Analysis?,” Cisco.com. Retrieved May 15, 2024.

17.“SOAR, SIEM, SASE and zero trust: How they all fit together,” SecurityIntelligence.com, March 7, 2023.

18.“A Deep Dive into The Forrester Wave™: Zero Trust Edge Solutions, Q3 2023,” Forrester.com, Aug. 29, 2023.

19. “What Is Role-Based Access Control (RBAC) and What Does It Have to Do with Zero Trust?” EdTechMagazine.com. Oct. 26, 2023.

20. “Secure applications with Zero Trust,” Microsoft.com. Retrieved April 30, 2024.

21.“What Is Zero Trust for the Cloud?,” PaloAltoNetworks.com. Retrieved May 14, 2024.

22.“Securing Containers with Zero-Trust Tools,” CloudNativeNow.com. Aug. 3, 2022.

23.“Why Data Loss Prevention (DLP) is Important in a Zero-Trust Environment,” ITSecurityWire.com, Oct. 25, 2022.

24.“Secure Data with Zero Trust,” Microsoft.com, retrieved May 14, 2024.

25.“Incident Response in a Zero Trust World,” SANS Institute, Jan. 15, 2020.

26.“What is Zero Trust? Principles, Benefits, and Use Cases,” Veeam.com. Jan. 8, 2024.

27.“2021 Strategic Roadmap for SASE Convergence,” Gartner.com. March 24, 2021.