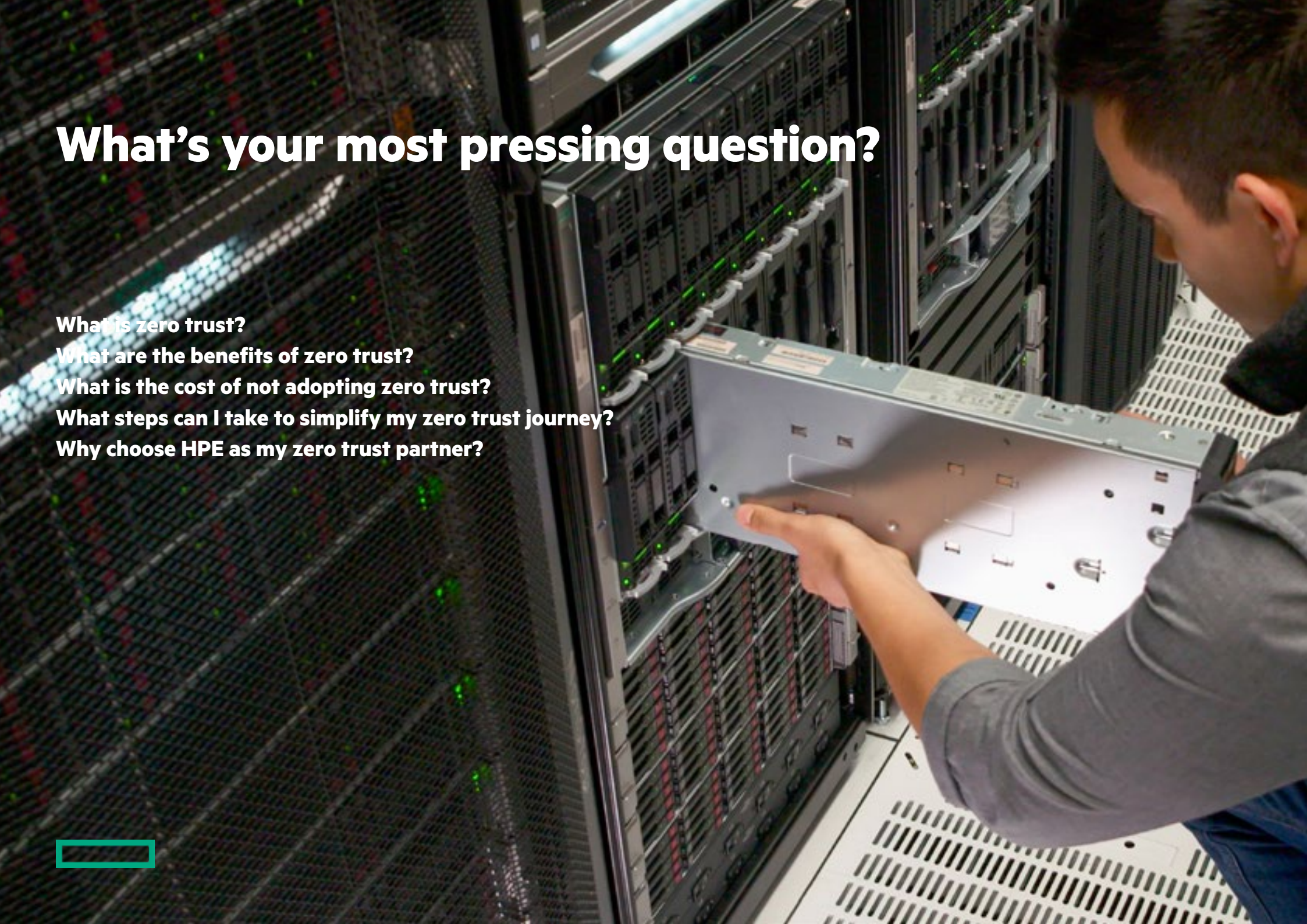
HPE aruba networking

Brochure

The simple zero trust guide for network leaders

Get started >

HPE GreenLake



What’s your most pressing question?

What is zero trust?
What are the benefits of zero trust?
What is the cost of not adopting zero trust?
What steps can I take to simplify my zero trust journey?
Why choose HPE as my zero trust partner?

What's your most pressing question?

As organizations continue their shift toward a cloud-first, hybrid workforce model, traditional network security approaches are no longer enough to protect the growing array of applications, users, and devices. Legacy network infrastructures can't keep up with the speed and complexity of modern threats, leaving critical assets vulnerable. To navigate this new security landscape, network leaders must reevaluate and update their security strategies to ensure the integrity of their networks.

Zero trust is a highly effective solution to today's network security threats. It's a security model that operates on the principle of never trust, always verify, by assuming that no user, device, or application, whether inside or outside the network, should be trusted by default. This offers a more secure infrastructure, minimizes risks, and provides seamless access to authorized users.

This e-book outlines a simple, four-step approach for implementing zero trust in your network infrastructure.

What is zero trust?

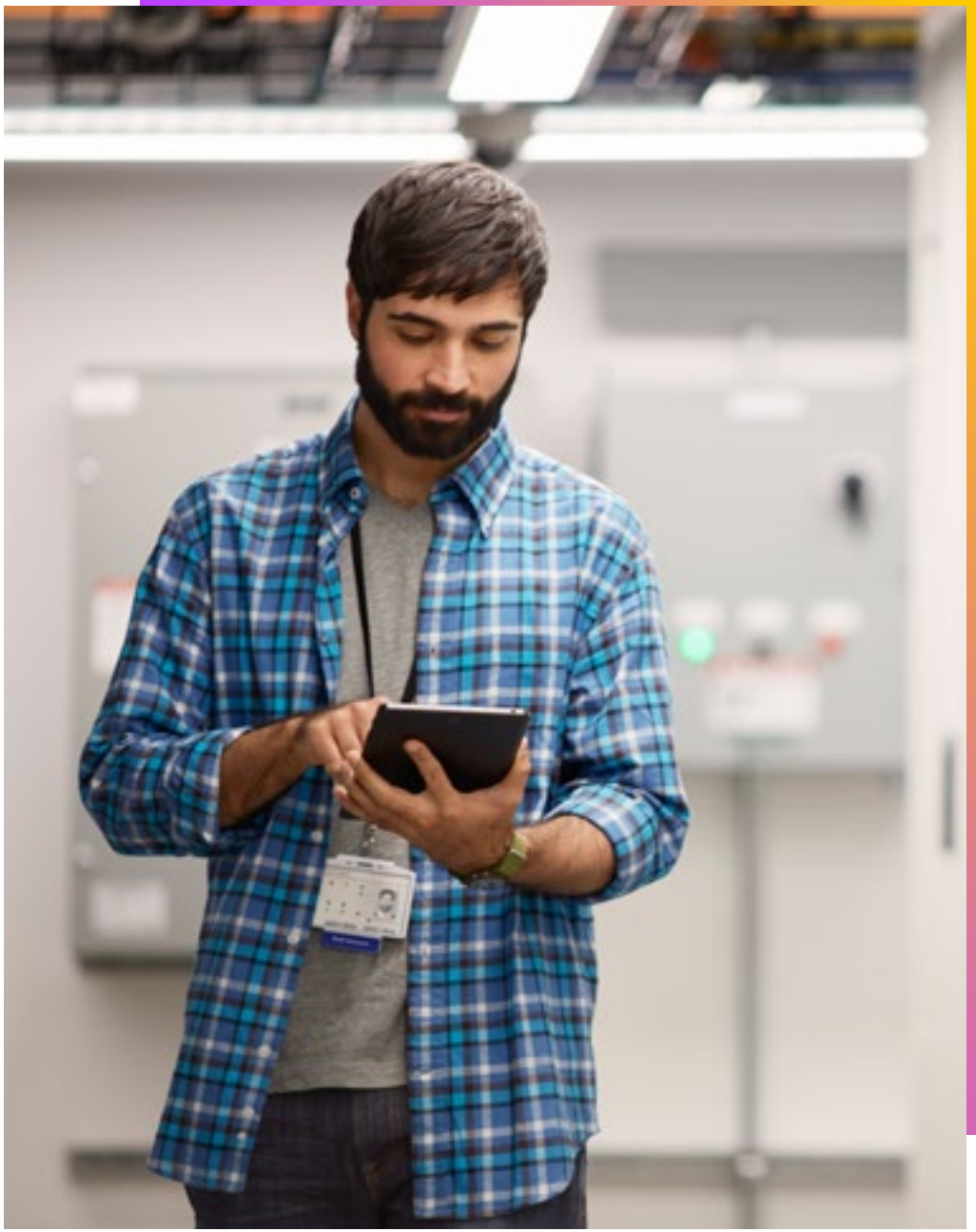
Zero trust is a security framework that addresses the vulnerabilities of traditional perimeter-based security models. Traditional models assume that users and devices inside the network are trustworthy and do not require continuous verification once they gain access. Zero trust challenges this assumption by requiring all users, devices, and applications to continuously authenticate, authorize, and verify their access. This approach helps limit exposure to cyber threats by enforcing the principle of least privilege, ensuring that users and devices only have access to the specific resources they need.

Unlike legacy models, which focus on securing the perimeter of the network, zero trust seeks to minimize risks by enforcing strict access controls, network segmentation, and continuous monitoring for anomalies. By treating every entity as potentially compromised, zero trust reduces the likelihood of lateral movement within the network in case of a breach.

The benefits of zero trust security

Adopting a zero trust model offers a variety of benefits for organizations seeking to strengthen their network security posture and minimize risks:

- **Reduced attack surface:** By enforcing strict access controls and segmenting the network, zero trust reduces the potential entry points for attackers, preventing lateral movement and minimizing the damage caused by breaches.
- **Enhanced security for remote work:** With a hybrid or remote workforce, zero trust ensures that employees, regardless of location, access only the resources they are authorized to use. This level of security extends to Internet of Things (IoT) devices and unmanaged devices, which are often overlooked by traditional security models.
- **Improved compliance:** Zero trust enforces granular access controls, making it easier for organizations to meet regulatory requirements and avoid costly compliance violations.
- **Better visibility:** With continuous monitoring and real-time analytics, zero trust provides enhanced visibility into network activity, helping security teams quickly detect and respond to threats.
- **Cost efficiency:** By replacing legacy security solutions with a unified approach, organizations can streamline operations, reduce complexity, and eliminate the need for multiple disparate security tools.



What is the cost of not adopting zero trust

Failing to adopt zero trust can expose organizations to a variety of risks, including increased vulnerability to data breaches, ransomware, and phishing attacks—all exacerbated with the emergence of generative AI (GenAI).

"Since the proliferation of gen AI platforms, starting in 2022, phishing attacks have risen by 1,265 percent."[1]

McKinsey & Company, November 2024

Organizations are also required to comply with regulations on zero trust. In 2021, the United States introduced the Executive Order 14028[2] to improve the nation's cybersecurity. Outside of the United States, the European Union has introduced the NIS 2 directive and DORA frameworks.

Without zero trust, attackers who gain initial access to the network can easily move laterally, accessing sensitive data and critical systems. Moreover, organizations relying on outdated security models often struggle with inconsistent enforcement, inefficiencies in security operations, and an increased attack surface.

The complexity of managing legacy security solutions often leads to manual configuration errors, which can result in security gaps. Furthermore, traditional VPNs, while commonly used for remote access, can introduce latency and performance issues, negatively impacting the user experience. VPNs also give broad access to internal resources, introducing additional risks. These vulnerabilities, combined with the ever-increasing sophistication of cyber threats, make it imperative for organizations to adopt a more robust and adaptive security model like zero trust.

[1] The cybersecurity provider's next opportunity: Making AI safer, McKinsey November 2024

[2] Improving the Nation's Cybersecurity. May 2021

What steps can I take to simplify my zero trust journey?

By implementing simple steps for a zero trust architecture (see Figure 1), network leaders can reduce the risks associated with data breaches, ensure better compliance with regulations, and improve network performance—all while enhancing the user experience.

Figure 1. Four steps to simplify zero trust journey

Step 1: Modernize branch networks

The first step in embracing zero trust is modernizing WAN infrastructure. Legacy routers and traditional networking equipment were not designed with cloud-first and hybrid workforce models in mind. They lack the agility and cloud-readiness required to meet the demands of modern networks. Replacing outdated routers with a secure SD-WAN solution is key to a high-performing, secure, and scalable network.

Secure SD-WAN integrates networking and security into a single platform, combining routing, firewalling, and WAN optimization. With advanced SD-WAN capabilities like dynamic path selection and tunnel bonding, organizations can leverage any type of link, including multiprotocol label switching (MPLS), broadband, and 5G, and combine them while selecting the best path (Figure 2).

And it's possible to deploy a virtual instance of SD-WAN in cloud service providers such as AWS, Azure, and Google Cloud™, to optimize the first mile from the branch to the cloud service provider. Network modernization can eliminate dependency on rigid and often costly and inflexible MPLS networks. SD-WAN enables the use of broadband internet for traffic, reducing backhaul to the data center and improving performance for cloud-destined applications. This not only boosts network performance but also reduces latency, making it easier for users to access critical applications without disruptions.

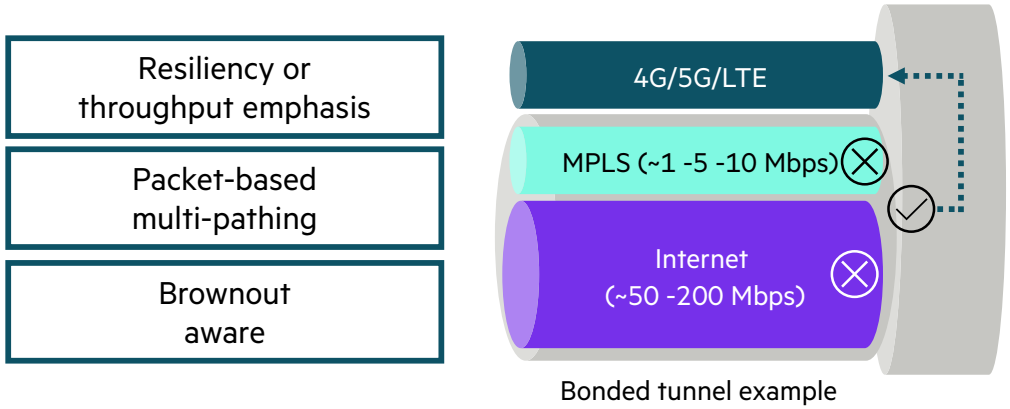


Figure 2. Bonded tunnels with SD-WAN using failover to 4G/5G/LTE links

Step 2: Simplify zero trust with secure SD-WAN and ZTNA

As applications move to the cloud, branch office networks must evolve to support secure, direct connectivity to cloud apps and other resources. Traditional firewall models and VPNs no longer provide the agility or security needed for modern work environments. A secure SD-WAN solution with a built-in next-generation firewall (NGFW) and zero trust network access (ZTNA) effectively addresses these challenges.

In branch offices, secure SD-WANs provide essential security features such as micro segmentation (Figure 3), intrusion detection system (IDS) and intrusion prevention system (IPS), and distributed denial-of-service (DDoS) attack defense. These capabilities enhance security while reducing complexity by replacing outdated firewalls with an integrated solution.

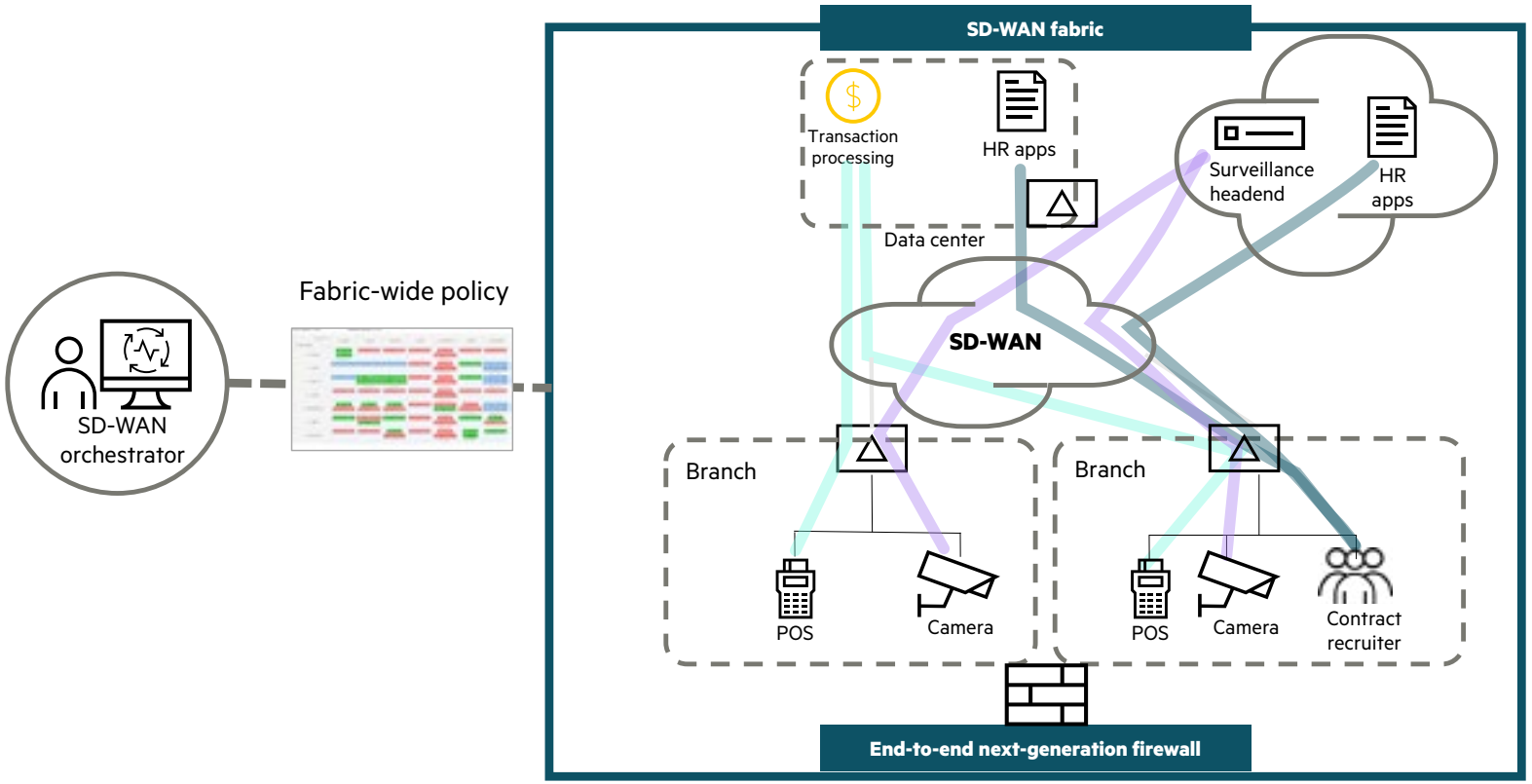


Figure 3. End-to-end segmentation with secure SD-WAN

VPNs typically require users to be connected to the corporate network to access applications, which can introduce latency and performance issues. ZTNA, on the other hand, complements SD-WAN by allowing users to securely access applications from any location, based on strict least-privilege access policies. This approach enhances security while providing a better user experience.

As applications are moving to the cloud and hybrid working is becoming the norm, organizations may no longer need complex branch infrastructure. This is similar to a coffee shop experience, using a simple architecture and assuming no device is safe until it has been properly authenticated and authorized. With this new paradigm, organizations can streamline their branch equipment by leveraging ZTNA with a lightweight SD-WAN—shifting traditional security equipment and functionalities to the cloud, and ensuring all devices are treated as untrusted by default. However, for more advanced needs such as branch-to-data center connectivity or advanced WAN optimization, organizations may implement a full-fledged secure SD-WAN solution.

Step 3: Achieve universal ZTNA across your infrastructure

Universal ZTNA extends zero trust beyond remote users to all parts of your infrastructure. This includes campus and branch locations where IoT devices may be deployed and even data centers, providing consistent security across the entire network.

In a zero trust model, every device and every user are continuously monitored for unusual behavior, and access is automatically adjusted based on real-time intelligence. AI-driven technologies, such as machine learning and behavioral analytics, are key to zero trust, by identifying and authenticating devices in real time (Figure 4). This ensures that only authorized devices are granted access to the network, reducing the likelihood of compromised devices being used as entry points for attackers.

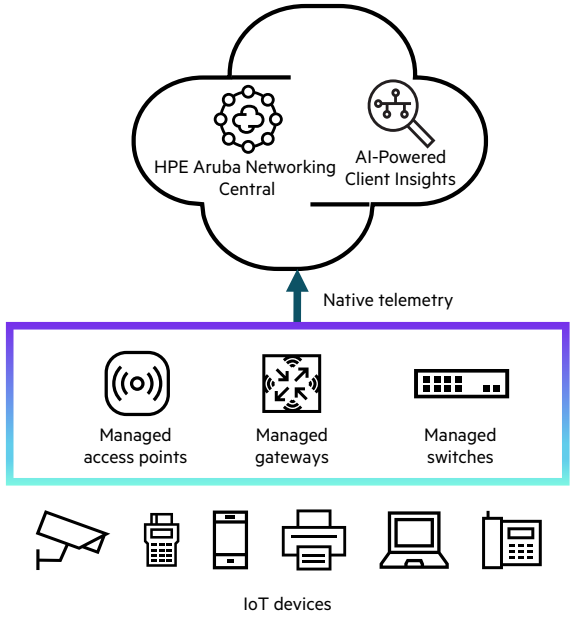


Figure 4. Accurately identify and authenticate devices using machine learning

Zero trust segmentation plays a critical role in restricting network traffic to only those users, devices, and applications that require access to specific resources. By enforcing strict access controls, organizations can reduce the risk of lateral movement in the event of a breach.

By embedding security within core network components such as switches, access points, and SD-WAN, organizations can define and enforce global zero trust policies that extend across the enterprise. This also applies to data centers, where advanced switching solutions provide zero trust segmentation and east west firewalling, eliminating unnecessary traffic routing through hardware appliances.

Extending zero trust across infrastructure ensures that everything on the network is visible, identifiable, and secure. A unified security model with global policies effectively segments the network, reducing the attack surface and preventing unauthorized access. Centralized management simplifies security enforcement, making it easier to maintain compliance and operational efficiency.

Step 4: Transform and unify secure connectivity with SASE

The final step in implementing zero trust is to unify security and networking through a secure access service edge (SASE) solution. SASE is a cloud-native framework that integrates networking and security functions into a single service, providing a consistent and scalable security model for the modern enterprise.

By combining SD-WAN and universal ZTNA with integrated security services such as secure web gateway (SWG), cloud access security broker (CASB), and data loss prevention (DLP), SASE ensures that all users, devices, and applications are protected regardless of location. The integration of these security features into a single platform simplifies management and ensures consistent policy enforcement across all parts of the network.

SWG, for example, blocks access to malicious websites and provides content inspection to protect against threats like phishing and malware. It can also leverage SD-WAN deployments to protect all devices, managed and unmanaged, without the need to install a security service agent (SSE) agent on each device, using dedicated tunnels to the SWG solution (Figure 5).

CASB adds an extra layer of protection by securing software-as-a-service (SaaS) applications, discovering shadow IT and ensuring that sensitive data is not inadvertently leaked or accessed by unauthorized users. DLP helps prevent data loss by enforcing strict data access and transfer policies.

When implementing zero trust, it is crucial to monitor the network and adjust trust in real time, with tools such as IDS/IPS and network detection and response (NDR). AI-powered NDR can detect abnormal behavior and identify threats such as ransomware attacks.

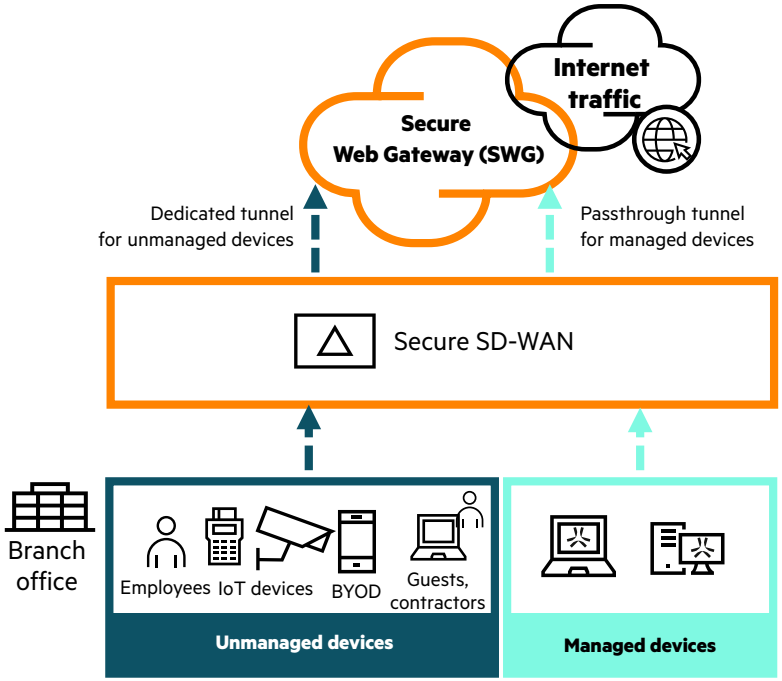


Figure 5. Protect all devices managed and unmanaged from web-based threats with SD-WAN augmented with SWG

SASE SWG site license

User-based SWG license

More tips on getting started with zero trust

Implementing zero trust is a strategic decision that can significantly strengthen your organization's network security. Here are some more important considerations as you get started.

- **Assess your current security posture:** Evaluate your existing security infrastructure and identify areas where zero trust can enhance protection. Focus on vulnerable points such as remote access, legacy firewalls, and network segmentation.
- **Adopt a cloud-first strategy:** As you transition to the cloud, consider adopting a secure SD-WAN solution that can enable zero trust principles across your network, ensuring that security and performance are optimized.
- **Select the right tools:** Choose security solutions that integrate seamlessly with zero trust frameworks, such as next-generation firewalls, ZTNA, and SASE platforms.
- **Break silos:** Work with your security teams to develop a comprehensive policy framework that includes access controls, segmentation, monitoring, and authentication procedures.
- **Implement gradually:** Start with a pilot project, applying zero trust principles to a limited set of users or applications. Gradually expand the scope as you refine your processes and gain experience.

By taking these steps, you can build a zero trust network architecture that will protect your organization from evolving cyber threats, improve compliance, and enhance user experience.

Why choose Hewlett Packard Enterprise as my zero trust partner?

HPE provides a comprehensive, holistic zero trust platform (Figure 6) that goes beyond traditional approaches, which often focus on isolated aspects of protection such as remote user access or network access control (NAC). Our platform enables organizations to enforce universal zero trust principles across devices, whether remote or on-premises.

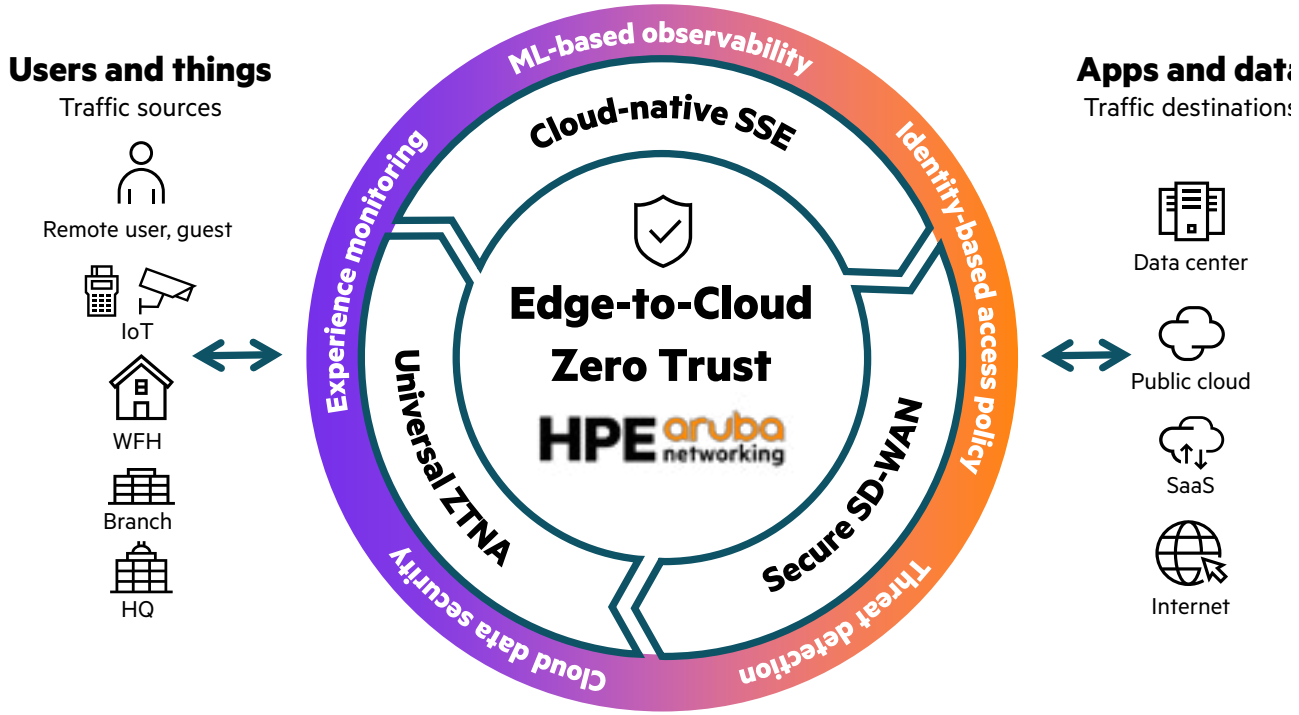


Figure 6. Enforce zero trust from edge to cloud with HPE Aruba Networking

HPE Aruba Networking EdgeConnect SD-WAN is a secure SD-WAN solution that enables edge-to-cloud architecture as the secure backbone between the edge and the hybrid cloud. With advanced capabilities such as path conditioning, tunnel bonding and WAN optimization, it optimizes traffic across any network links including MPLS, broadband and 5G.

The solution enables multi cloud networking by deploying its virtual instances into cloud service providers. With a built-in NGFW, organizations can seamlessly replace legacy branch firewalls by leveraging IDS/IPS and adaptive DDoS to protect against DDoS attacks with machine learning. By combining HPE Aruba Networking ClearPass Policy Manager with HPE Aruba Networking EdgeConnect SD-WAN, organizations can segment the network based on role and identity, enforcing zero trust principles, so that users and devices—including IoT—can reach destinations consistent with their role in the business.

HPE Aruba Networking SSE is a cloud-native platform that includes advanced cloud-delivered security features such as ZTNA, SWG, CASB and DLP managed with a single policy engine. For remote users, the solution replaces legacy VPNs with modern ZTNA, providing secure and seamless access to private resources while mitigating third-party risks through an agentless solution. Additionally, it integrates SWG functionality to protect endpoints from web-based threats, alongside CASB and DLP features to safeguard access to SaaS applications and prevent data leaks.

Universal ZTNA with HPE Aruba Networking allows organizations to extend zero trust security into branch and campus locations. With local edge capabilities, the solution helps ensures that on-premises ZTNA traffic remains local while reducing inefficient hairpin routing to the cloud. This enforces the same granular access control policies for on-premises traffic, creating a consistent security posture throughout the organization. With embedded AI-powered NAC capabilities, our platform uses machine learning that helps provide visibility into all connected devices, including IoT, achieving up to 99% profiling accuracy for comprehensive threat detection and mitigation. Administrators can define and enforce a global zero trust policy through HPE Aruba Networking Central, using firewalls embedded in HPE Aruba Networking CX switches, access points, and HPE Aruba Networking EdgeConnect SD-WAN to protect every endpoint. In data center environments, the HPE Aruba Networking CX 10000 Switch Series introduces advanced zero trust segmentation and east-west firewalling, mitigating inefficiencies and enhancing protection for critical workloads by avoiding hairpin routing to external appliances.

Learn more at

hpe.com/networking

Visit HPE.com

Chat now (sales)

a00146024ENW