HPE aruba networking

eBook

Easing zero trust security adoption

Accelerating your journey to zero trust with security-first, AI-powered networking

Get started >

HPE GreenLake

Table of contents

Shifting paradigms

Innovation is crucial to organizations. In today's digital-first world, great experiences are the hallmark of innovation.

Great experiences help organizations stand out in a crowded marketplace, draw talented workers from around the globe, and keep organizations thriving amidst uncertainty, change, and disruption.

Great experiences are powered by connectivity: connecting people to each other, retailers to customers, doctors to patients, workers to applications, devices to the cloud, and data to algorithms.

This connectivity never sleeps. It's always on and always accessible, anywhere.

Connectivity brings the promise of more personalization, satisfying user and employee experiences, advantage and, ultimately, growth.

It can also bring complexity for IT.

Network and security teams play an increasingly strategic role as connectivity and technology initiatives like generative AI rise to the top of the priority list. At the same time, the environments in which network and security teams operate are becoming more difficult to navigate. Security, privacy, governance, and compliance measures are constantly evolving, requiring more coordinated efforts, challenging teams already doing more with less.

What is zero trust?
Zero trust principles require users and devices to prove their trustworthiness to gain access to the resources they need to do their job or fulfill their function. This concept of least-privilege access is fundamental to zero trust security practices.

Zero trust security also requires continuous monitoring of users and devices. Trustworthiness is constantly re-evaluated, and if a user or device begins to act suspiciously or in a fashion inconsistent with their role, their access may be limited or revoked. This limited and dynamically assessed control can help minimize and even prevent lateral spread of attacks.

Why zero trust security?
Network security approaches focused primarily on protecting the perimeter are no longer sufficient, given rising IoT adoption, erosion of the corporate perimeter due to work-from-everywhere, and increasingly sophisticated threats that exploit "trusted" users and devices for malicious purposes.

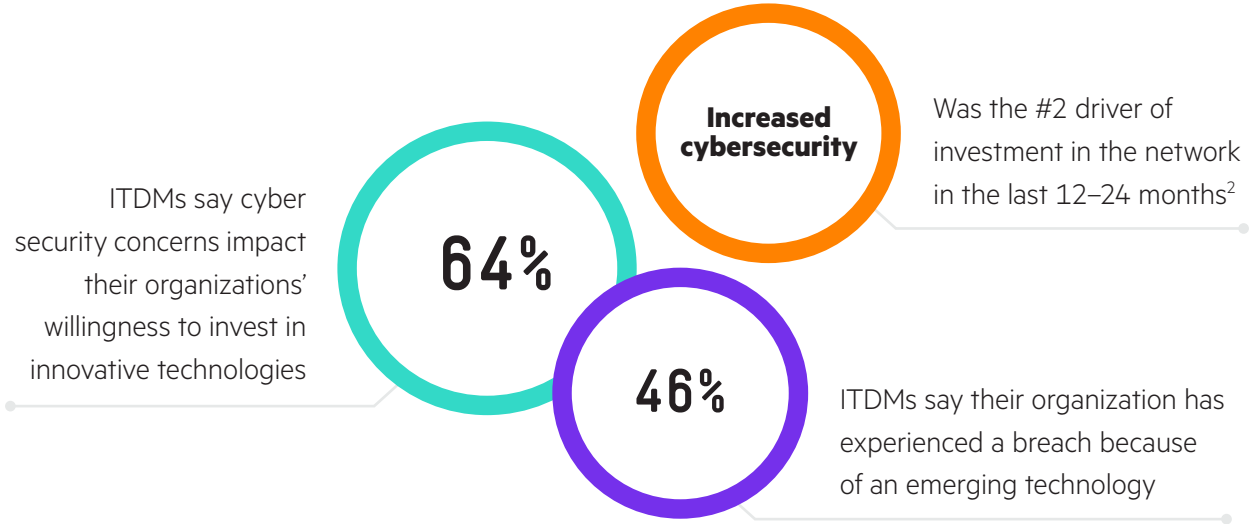
The need for zero trust

Connectivity is the key to innovation, and at the core of connectivity is the network. Whether working in the office, shopping in a store, logging in from a coffee shop, or connecting a surveillance camera to a cloud application, the network is always there.

What else is expected? Undetected threats.

The expectation is so pervasive that it gave rise to a new model of security architecture: zero trust. Zero trust security models assume an attacker is present in the environment, and thus an owned network is no more secure than a non-owned network.[1]

How do organizations balance the need for high performance and uninterrupted access across their network with the need for robust security?



The challenges of zero trust

While adoption of zero trust has grown in recent years, its implementation is still challenging for many organizations. There are several reasons for this.

1. **A paradigm — not a product.** Zero trust is not a single product or solution that can be purchased off the shelf. It is a set of guiding architectural principles that must be consistently refined and carried out through infrastructure and policy decisions; as such, it's not a "once and done" initiative. Advancing maturity toward a vision of zero trust can take time as security mindsets change and processes adapt.

2. **Cross-domain requirements.** Zero trust spans technology domains within an organization, touching not just networking but users, devices, applications, and workloads across campuses, branch offices, data centers, cloud, and beyond. Coordination, control, and consistency are critical but difficult to achieve given the diversity among environments.
3. **Fragmented capabilities.** The access control capabilities that support zero trust architectures typically span multiple technology solutions, which are often cobbled together in a disjointed fashion. Over time, this patchwork approach not only increases architectural and operational complexity, it also exposes the organization to security gaps, inconsistencies in policies and enforcement, and potential cyber security risk from inadvertent gaps.[4]
4. **Team collaboration.** Delivering successful innovation that meets zero trust security requirements often requires network and security teams to work together to pursue common goals and objectives — providing superior experiences while keeping the organization safe from increasingly prevalent and sophisticated attacks. Disparate tooling and lack of shared controls and data can create siloed operations that hinder efforts to reach joint business outcomes.

The new role of the network

Infusing innovation with zero trust principles is key, and innovation is built on connectivity. That means the network now has an essential role as part of an overall zero trust security ecosystem.

Now is the time for IT leaders to think about the network as a zero trust security solution.

While no single vendor or solution can deliver all the cyber protection an organization needs, starting with a network that provides a built-in foundation for zero trust security can make it easier to implement security requirements while adding protection at critical digital entry points. And, in its dual role as connectivity enabler and cybersecurity defender, the network naturally becomes a place of collaboration and cooperation between network and security teams.

Your choice of network matters when it comes to protecting your organization.

Easing the path to zero trust adoption

Security-first, AI-powered networking

Accelerate your journey to zero trust adoption with security-first, AI-powered networking from HPE Aruba Networking. Built with zero trust principles, HPE Aruba Networking security-first, AI-powered networking solutions provide a common foundation for networking and security teams to power distinctive experiences and innovative business results without sacrificing cybersecurity protection.

A security-first, AI-powered network from HPE Aruba Networking eases adoption of zero trust security and supports compliance with cybersecurity standards and regulations by allowing teams to use the network as a security solution. The network can now provide advanced visibility and insights, centralized policy management, data protection, threat defense, and access control in a single platform. With these built-in zero trust security capabilities, the network itself becomes a critical line of defense that integrates with the elements of the security ecosystem to enhance protection without the added complexity that comes from multiple disparate tools, or the costly and disruptive requirement of a rip-and-replace of existing infrastructure.

AI-powered networking also multiplies an organization's human power — a crucial factor as regulatory frameworks expand, talent gaps widen, and cyber threats increase. With HPE Aruba Networking security-first, AI-powered networking, teams can benefit from intelligent automation that reduces manual effort, improves visibility and anomaly detection, and enhances monitoring and diagnostics, all of which ensure the organization is not exposed to unnecessary risk.

How does security-first, AI-powered networking make it easier to adopt zero trust security?

1. Delivers **shared visibility** for a common source of truth between teams and tools.
2. Provides **global policy management** for simplified policy definition and application.
3. Enables **edge-to-cloud enforcement** for optimized performance and consistent control.
4. Is **AI-powered** to improve efficiency and security.

Seeking to adopt zero trust security? Consider its basic requirements.

“Ideally, you should be able to answer a few questions of every user or device on your network: Who are you? What should you be allowed to do on this network? And how can I enforce that through policy control?”

– Jon Green, Chief Technology Officer and Chief Security Officer, HPE Aruba Networking, Hewlett Packard Enterprise[5]

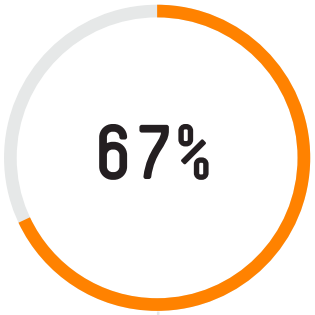
HPE Aruba Networking zero trust security foundation

Unlike other approaches that require a collection of disjointed security solutions bolted on to the network infrastructure, HPE Aruba Networking security-first, AI-powered networking delivers built-in zero trust solutions that are planned, designed, and operationalized as a natural part of a standard network implementation. HPE Aruba Networking solutions also seamlessly integrate with the rest of the security ecosystem to both inform and act on information from across the security environment, helping to enhance protection while simplifying operations.

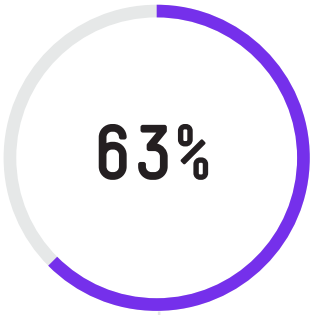
Shared visibility

Operate from a common truth

Zero trust security starts with visibility of connected users and devices. Yet security gaps caused by lack of visibility and control into user and device activities persist for many organizations[6]. Much of the gap is driven by the growing number of IoT devices connected to enterprise networks, which represent a significant expansion of the organization's attack surface. Exacerbating the issue, IoT devices are often installed and managed by lines of business other than IT, contributing to lack of visibility.



Respondents said that identifying and authenticating IoT devices accessing their network is critical to their organizations' security strategy



Respondents said their security teams lack visibility and control into all the activity of every device connected to their IT infrastructure[7]

Security-first, AI-powered networking makes it easier for teams to implement zero trust security controls by delivering shared visibility and control. Making trust decisions based on a combined source of data streamlines networking and security operations, so teams can make informed decisions about how to monitor and manage risk.

The benefits of shared visibility

- Know with confidence who and what is on your network, and continuously monitor behavior and status
- Share data with other elements of the security ecosystem, such as SIEMs, to deliver alerts and insights from across the infrastructure
- Leverage built-in network traffic analysis and behavioral baselines for early attack detection, potentially stopping or preventing spread of attacks

HPE Aruba Networking solutions

Cloud-based network management solution HPE Aruba Networking Central includes AI-powered visibility and profiling with Client Insights. Client Insights analyzes native infrastructure telemetry directly from access points, switches, gateways, and clients, without requiring installation of physical collectors or agents. Client Insights provides accurate AI/ML device profiling with up to 99% profiling accuracy of known clients with < 5% rate of unknowns across a wide variety of endpoints connecting to the network[8], including a diverse set of IoT devices across the entire wired and wireless infrastructure. For environments not managed by cloud-based HPE Aruba Networking Central or with third-party network devices, HPE Aruba Networking ClearPass Device Insight provides ML-based identification and profiling of clients.

Gain up to 99% profiling accuracy for network-connected devices, including IoT

How do role-based policies simplify the adoption of zero trust security frameworks?
Roles enable policy definitions to be carried across networks irrespective of geographic location or point of connectivity to the network. Appropriate policies can follow users and devices consistently as they travel throughout the enterprise, from campus to branch to home office and beyond.

Global policy

Policies that follow the user

Once a user or device is known and profiled, the next step in a zero trust security framework is to authenticate its identity each time it connects and assign it appropriate access control policies. Defining and managing policies can be challenging, however, as business dynamics change, workers log in from anywhere, and IoT devices are added to the mix. Approaches that rely on location- or network-specific constructs, such as IP addresses or subnets, can lead to complexity and inflexibility in the network, and create security risk associated with inconsistencies in definition and application.

Global policy capabilities within security-first, AI-powered networking help organizations extend their reach, with high-level policies defined and applied based on identity and roles. Roles span the entire enterprise, eliminating painstaking maintenance of access controls for every device in the organization. Policies expressed in terms of business intent simplify policy workflows by abstracting them from the complexity and changes of the underlying physical network, so both network and security teams can manage by intent.

Benefits of global policy

- Define policy once and apply everywhere, eliminating painstaking maintenance of access controls and inconsistencies that increase risk
- Continuously monitor and enforce policies for users, devices, data, and apps with no gaps — no matter where they are or what they are connected to
- Provide network and security teams a “shared toolbox” to optimize network performance and enforce granular security policies

HPE Aruba Networking solutions

HPE Aruba Networking ClearPass authenticates users and devices against a wide variety of identity sources, such as Active Directory. Using a rich policy engine that enables precision access privileges, ClearPass controls what users and what devices can access what resources. Policies follow the user and device seamlessly across wired, wireless, and wide area networks — even within multi-vendor environments.

For networks managed by HPE Aruba Networking Central, cloud-native network access control (NAC) solution Cloud Auth enables frictionless on-boarding of end users and client devices either through MAC address-based authentication or through integrations with common cloud identity stores to automatically assign the right level of network access.

For hybrid and remote users, as well as third parties such as contractors and temporary workers, HPE Aruba Networking SSE Zero Trust Network Access (ZTNA) limits access, via a trust broker, to only specific applications or microsegments that have been approved for the user as defined via a single global policy interface. Continuous monitoring ensures that policies automatically adapt based on changes in identity, location, and device health — context that makes it easier to ensure zero trust for every access event.

Edge-to-cloud enforcement

Consistent policy enforcement for users, apps, data, and devices

Zero trust security frameworks rely on policy enforcement to enforce trust and ensure that users and devices have access just to the resources they need, as long as they are not suspected of participating in an attack.

With HPE Aruba Networking security-first, AI-powered networking, organizations can implement zero trust, role-based enforcement at every control point. Security-first, AI-powered networking enforces role-based policy for all users, devices, data, and apps, no matter where or how they are connected or what they are connecting to. Inline policy enforcement within switching infrastructure avoids hair-pinning traffic to implement security policies, improving performance, enhancing user experience, and consuming fewer resources along the way — without compromising access or protection.

Benefits of edge-to-cloud enforcement

- Enforce policy anywhere, including endpoint, access point, access switch, SD-WAN gateway, data center top-of-rack switch, on campus and via cloud
- Support network and security team cooperation and collaboration as policies help deliver optimal network performance while protecting the organization
- Reduce the amount of external security solutions required to enforce access controls required for zero trust and compliance frameworks, as well as associated complexity

HPE Aruba Networking solutions

HPE Aruba Networking's Dynamic Segmentation separates network traffic based on identity and associated access permissions, enforcing zero trust least-privilege access to applications and data from edge to cloud. Dynamic Segmentation supports multiple enforcement models — centralized and distributed — allowing IT to use one or both models based on the needs of their environment. Centralized enforcement is provided by Policy Enforcement Firewall, a full application firewall embedded in HPE Aruba Networking network infrastructure. Distributed enforcement inline within gateway and switching infrastructure is delivered by HPE Aruba Networking Central NetConductor, a full-stack solution that uses widely adopted technology, such as EVPN/VXLAN, to produce an intelligent network overlay suitable for rapid enterprise network deployment and massive scalability for network and security automation.

Organizations can also use HPE Aruba Networking EdgeConnect SD-WAN to enforce consistent security policies spanning the WAN and LAN with built-in, end-to-end, next-generation firewall capabilities including IDS/IPS, DDoS protection, and enterprise-wide micro segmentation. Built-in NGFW services enable organizations to consolidate branch network and security functions by eliminating legacy firewalls and routers in branches.

Within the data center, the HPE Aruba Networking Fabric Composer eases implementation of zero trust security by simplifying and automating the micro segmentation process with an easy-to-use, point-and-click user interface. The HPE Aruba Networking CX 10000 switch delivers distributed micro segmentation, east-west firewalling, encryption, and telemetry services inline, across every port, closer to critical enterprise applications, eliminating the need for additional firewalls

“Leading enterprises will adopt zero trust architectures where the network’s job is defined not in terms of connecting anything to anything, but rather as being an enforcement layer for security policy.”

– David Hughes, Chief Product & Technology Officer, HPE Aruba Networking, Hewlett Packard Enterprise[9]

What is AI networking?
AI networking is a new term introduced to specifically target how artificial intelligence for IT operations (AIOps) applies to Wi-Fi, switching and WAN environments.

AI-automated operations

Manage and protect at scale

Today's business landscape has become more complex and challenging to navigate than ever before. Maintaining and securing a zero trust network today requires full-time visibility and automation. AI promises to multiply human potential, so organizations can mitigate risk at scale to improve security and free teams to create business advantage.

Security-first, AI-powered networking gives teams the power of machine learning combined with full network and user-centric telemetry that captures data from every user, device, and network. Security teams can use this data to support zero trust security implementation and continuous monitoring to help prevent and contain attacks. Networking teams benefit from the ability to automate mundane onboarding, provisioning, and policy orchestration tasks.

The benefits of AI-automated operations

- Automate network management and security operations tasks to reduce the manual effort required to secure and manage the network
- Improve visibility and control of users and devices on the network and detect anomalies to improve attack detection and prevention
- Enhance monitoring and diagnostics to deliver relevant, actionable insights network and security teams can use

HPE Aruba Networking AI-automated operations

HPE Aruba Networking Central is a cloud-native network and security management console for all HPE Aruba Networking infrastructure. As the single point of visibility and control for HPE Aruba Networking Security-First, AI-Powered networking, HPE Aruba Networking Central delivers AIOps, workflow automation, and advanced security features to unify operations across campus, branch, data center, and remote work environments.

HPE Aruba Networking Central leverages AI and advanced analytics to automate common network and security management and operations activities, with 24x7 intelligent monitoring of networks, applications, and devices that form a part of the data lake. These features are based on ML models that are consistently trained with network performance data of varied and global HPE Aruba Networking customer base. HPE Aruba Networking Central's AI-powered capabilities include:

- Automatic detection and diagnosis of issues using dynamic baselines, with built-in anomaly detection for precise problem identification, root cause, and remediation with close to 95% accuracy[10]
- ML models coupled with deep packet inspection to accurately identify and profile clients across wired and wireless infrastructure without physical collectors or agents
- Firmware recommendations to eliminate the overhead of manually tracking firmware upgrades and reduce the risk of non-compliance due to security vulnerabilities

HPE Aruba Networking Central's AI-powered capabilities are driven by the industry's largest data lake[11]

3.8
Million devices

1+
Billion clients

30+
Industry verticals

eBook

Bethesda Health Group

Security-first, AI-powered networking at work

Customer story

By offering vibrant and diverse retirement communities that uniquely reflect the neighborhoods of Greater St. Louis, as well as highly personalized in-home care, Bethesda Health Group has built a national reputation as a trusted resource for senior citizens and their families for 135 years. The organization's 1,100 employees supply individualized, quality, innovative, and compassionate care across 16 locations.

In support of its increasingly mobile and tech-savvy workforce and resident population, Bethesda transformed its operations to adopt a cloud-first strategy. It leverages high-performance connectivity to deliver services, provide access to a host of applications, and enable residents to stay in touch with their care teams, family, and friends. With this transformation also came the need for improved cybersecurity, as well as the need to adopt zero trust.

Already partnered with HPE Aruba Networking for wired, wireless, and SD-WAN (software-defined WAN) networking, Bethesda decided to enhance its infrastructure by adopting the fully cloud-delivered Secure Access Service Edge (SASE) platform and HPE Aruba Networking Security Service Edge (SSE). It consolidates multiple secure access capabilities into a single, easy-to-use cloud service that automatically adapts policies based on changes in user, device, and application context.

After deploying SD-WAN, Bethesda sought to improve access security and satisfy audit requirements. HPE Aruba Networking ClearPass enabled Bethesda to modernize its access control with a granular, policy-based solution for wired and wireless networks, and their lean IT staff found it intuitive and easy to use.

Bethesda also appreciated HPE Aruba Networking Central for supplying AI-powered cloud-based management for further unifying its wired and wireless infrastructure.

"We've gained comprehensive and secure networking infrastructure that enables us to manage a large wired, Wi-Fi, and SD-WAN footprint with a lean IT staff."

– Michael Keller, Director of Information Technology, Bethesda Health Group[12]

Read **the full story**

Implementing zero trust security

Adopting a zero trust security model is a journey. Not sure where to start? Consider this checklist of capabilities to help prioritize next steps:

- ✓ Do you have visibility into every device on your network, even if you do not manage it?
- ✓ Do you have consistent methods for assigning privileges to users and devices?
- ✓ Are you enforcing standards of security compliance before a device is allowed on the network?
- ✓ Are you enforcing role-based access security policies consistently everywhere throughout the network?
- ✓ Are you able to continuously monitor a subject's security state using all available data?

Find out how security-first, AI-powered networking from HPE Aruba Networking can help you fill the gaps.

arubanetworks.com/products/security/

Visit **ArubaNetworks.com**

Make the right purchase decision.
Contact our presales specialists.

Contact us

Hewlett Packard Enterprise

[1] Rose, S.; Borchert, O.; Mitchell, S.; Connelly, S. Zero Trust Architecture. NIST Special Publication 800-207. National Institute of Standards and Technology. August 2020.

[2] The innovation vs. risk conundrum. Hewlett Packard Enterprise. 2023.

[3] The 2023 Global Study on Closing the IT Security Gap: Addressing Cybersecurity Gaps from Edge to Cloud. Ponemon Institute. March 2023.

[4] The 2023 Global Study on Closing the IT Security Gap: Addressing Cybersecurity Gaps from Edge to Cloud. Ponemon Institute. March 2023.

[5] What's the state of Zero Trust Security? HPE Aruba Networking. April 2023.

[6] The 2023 Global Study on Closing the IT Security Gap: Addressing Cybersecurity Gaps from Edge to Cloud. Ponemon Institute. March 2023.

[7] The 2023 Global Study on Closing the IT Security Gap: Addressing Cybersecurity Gaps from Edge to Cloud. Ponemon Institute. March 2023.

[8] AI-powered Network Infrastructure: The answer to IT Efficiency. 2022.

[9] Hughes, D. Five top networking and security trends for 2024. January 2024.

[10] HPE Aruba Networking Central AI-powered, cloud-managed networking for branch, campus, remote, and data center networks. 2023.

[11] HPE Aruba Networking Central AI-powered, cloud-managed networking for branch, campus, remote, and data center networks. 2023.

[12] Bethesda Health Group. 2024.

EBK_Security-First-AI-Powered-Networking_RVK_082724 a00137590ENW