HPE aruba networking

eBook

The simple zero trust guide for security leaders

Get started →

HPE

What's your most pressing question?

Today's security teams are superheroes, facing more digital transformation in the last 10 years than in the previous 30 combined. Applications are migrating to the cloud, users are more mobile and demanding than ever before, and increasingly sophisticated attacks are coming from all directions, even internally. As if things weren't complex enough, we are now entering the world of AI, bringing a new set of challenges and opportunities.

Your accomplishments are extraordinary, yet you are still being asked to do more with less. To offer more security, at lower cost, with fewer obstacles to users, less networking requirements, at scale.

This may feel insurmountable, but you've already proven your ability to achieve what once was impossible. The key to overcoming many of these challenges lies in adopting a zero trust approach to secure connectivity. We're here to support you in making this task manageable.

The goal of this e-book is to help you optimize the digital transformation journey you have already been on and help unify these initiatives under one zero trust umbrella.

What is zero trust?

Zero trust means a lot of different things to different people. We view zero trust as a strategy, not a product — something to be pursued as organizations evolve in their digital transformation journey.

Zero trust is defined as a security model where you "never trust and always verify." It presumes no device, user, network, or piece of data is inherently trustworthy and all should be treated as a potential threat. Zero trust works under a couple of assumptions:

— Security threats can be inside or outside your network.

— Every device and person accessing resources on your network must be authenticated and authorized.

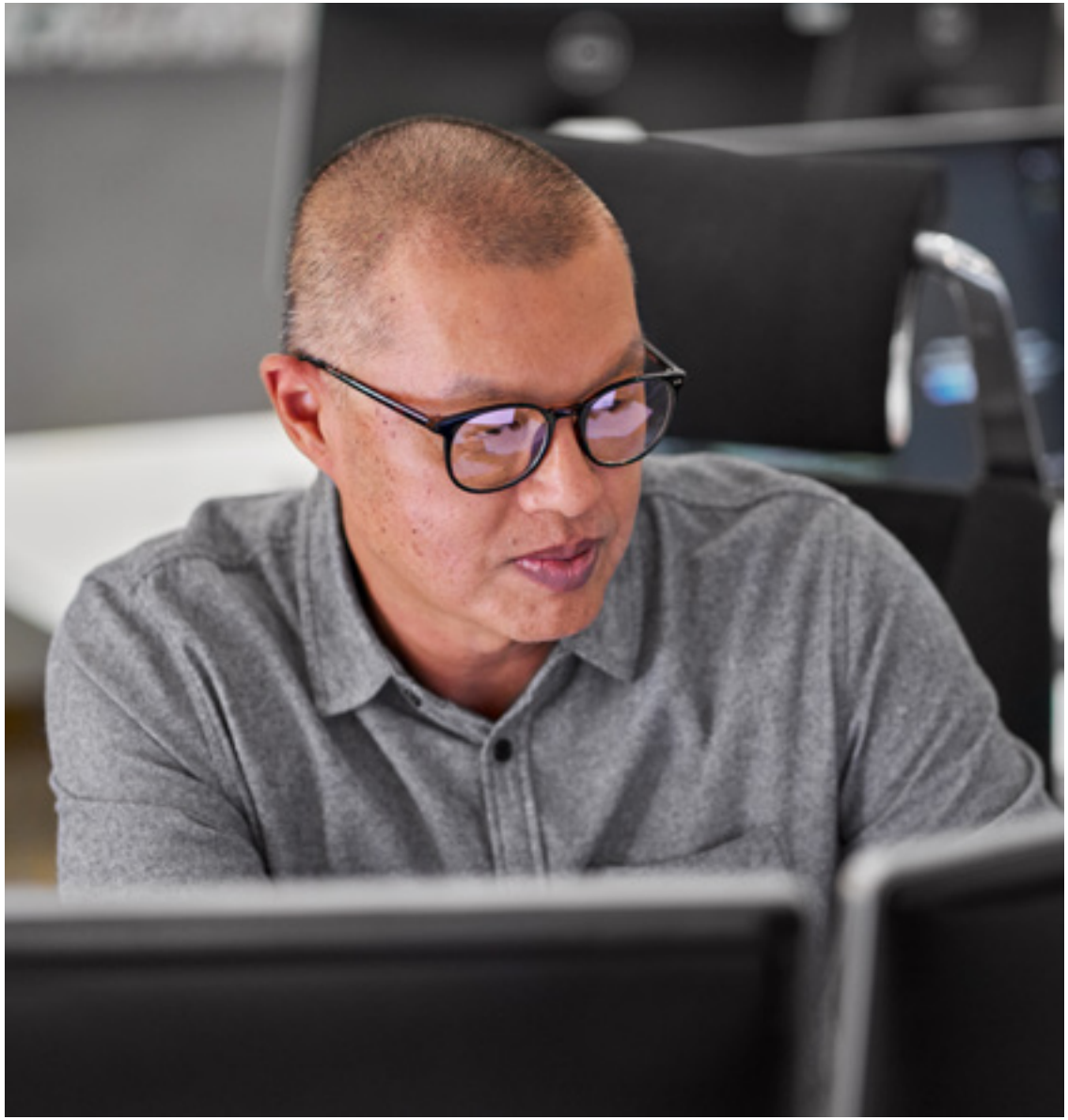
— By default, no person or device is trusted.

Often, vendors will say, “we sell zero trust in a box,” or “buy my zero trust product,” but the reality is that zero trust is more than a single product — it often requires a cybersecurity mesh of technologies that make up an overarching strategy. What’s needed is a holistic zero trust strategy that covers:

- **Users —** Identity must be consistently verified for every user.
- **Devices —** Devices must be frequently authorized and audited.
- **Applications —** Access to applications and resources must be specific to each user.
- **Data —** The movement of data must be consistently inspected.
- **Network —** Networks must be segmented to prevent lateral movement.

However, zero trust isn’t a one-time application; it’s a continuous process. Verifying a user’s identity just once isn’t enough — ongoing verification is crucial. Device posture can change rapidly, creating security gaps if only checked at initial connection. Both network and application access should be segmented based on user roles and authorization, ensuring least-privilege access. Additionally, data flow must be constantly monitored to prevent leaks and detect intrusions.

Your zero trust strategy will likely span multiple domains and should continually adapt over time as industry trends evolve. By consistently improving your zero trust approach, you ensure robust protection against emerging threats and maintain a resilient security posture.



The high cost of complacency

— $4.88M[1] — The average cost of a data breach in 2024

— 194 days[2] — The average amount of time it takes to detect a breach.

— 64 days[3] — The average amount of time it takes to remediate a breach.

Failing to modernize your security infrastructure against evolving threats can have severe consequences, such as:

— **Significant financial losses:** The total cost of a data breach can include both direct costs such as fines, legal fees, and remediation expenses, and indirect costs like lost business opportunities. The average cost of a data breach in 2024 was a staggering $4.88 million, underscoring the financial risk of inadequate security measures.

— **Risk of non-compliance:** Regulatory requirements are becoming increasingly stringent. Non-compliance can result in hefty fines and legal repercussions. Moreover, failing to meet internal and external compliance standards can hurt your organization's credibility.

— **Lost trust and opportunity with customers, partners, and vendors:** Trust is a critical currency in today's digital economy. A security breach can shatter the trust you've built with customers, partners, and vendors, leading to broken trust, damaged brand reputation, lost business, and strained relationships. Rebuilding this trust can be a long and costly process, and some organizations may never recover.

[1, 2, 3] "Cost of a Data Breach Report 2024," 2024, IBM.

Simplify your journey to edge-to-cloud zero trust with Hewlett Packard Enterprise

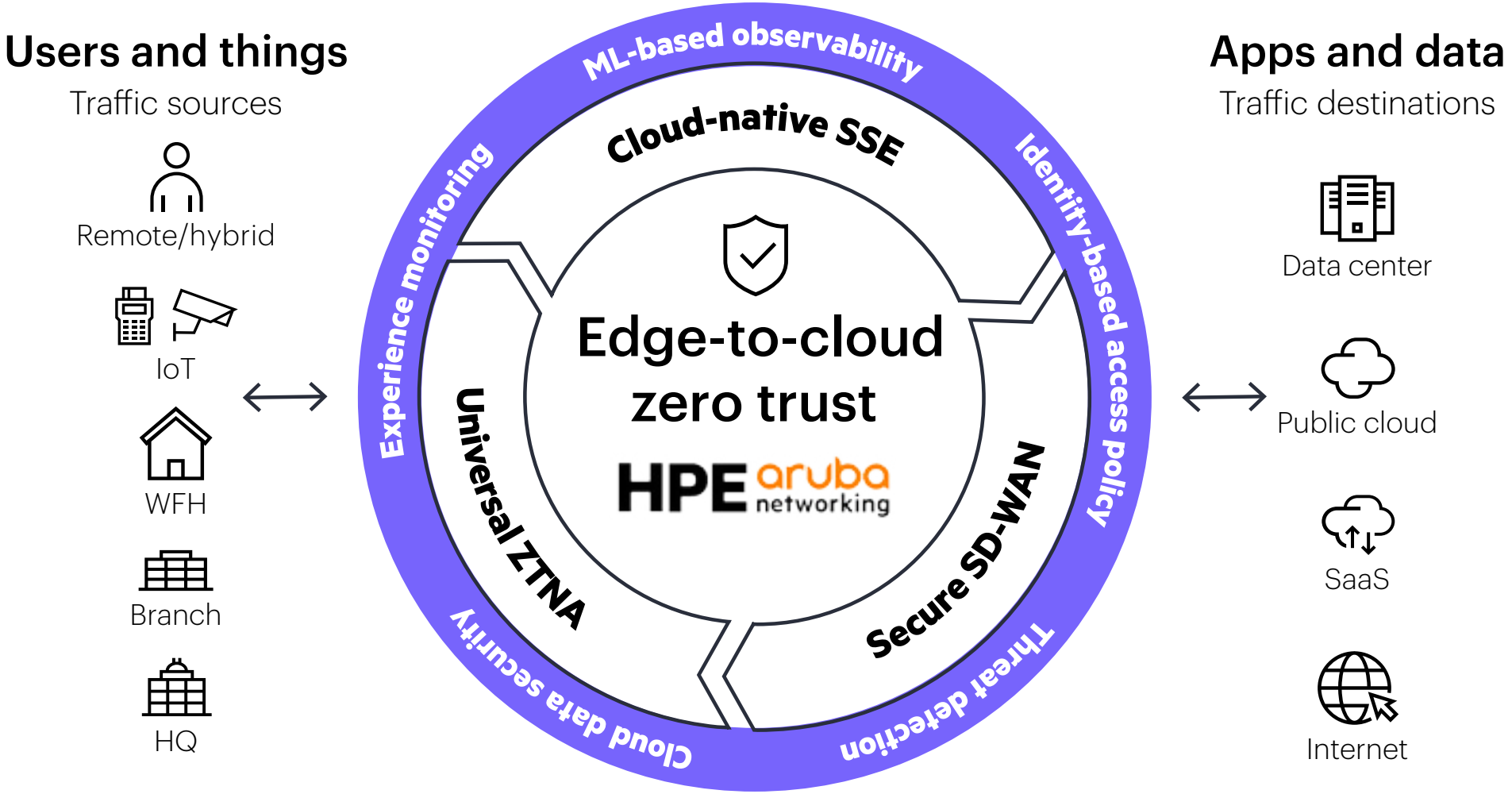


Figure 1. Components of the edge-to-cloud zero trust platform from HPE

HPE offers a robust suite of zero trust elements designed to modernize and optimize security and networking environments:

- **HPE Aruba Networking Security Service Edge (SSE)** provides seamless and secure access for users, devices, and applications from anywhere, offering zero trust networking access (ZTNA), secure web gateway (SWG), cloud access security broker (CASB), and digital experience monitoring (DEM) functionalities in a cloud-delivered solution.
- **HPE Aruba Networking EdgeConnect SD-WAN** enhances network performance and security by unifying SD-WAN, firewall, routing, and WAN optimization, offering high-quality application performance and secure connectivity.
- **HPE Aruba Networking ClearPass Policy Manager** delivers comprehensive network access control with role-based policies, enabling visibility, policy control, and attack response across wired, wireless, and WAN networks.

Together, these solutions create a comprehensive edge-to-cloud zero trust offering, providing a scalable and efficient security and networking infrastructure that's ready for the future. But it's important to understand that adopting zero trust is a process. It doesn't happen all at once.

Here are four recommended steps on the journey to a holistic zero trust strategy.

Step 1: Minimize third-party risk with ZTNA

Many of today's enterprises still rely on VPNs to secure third-party access. This is a big security risk, because VPNs provide unfettered access to untrusted users and devices, increasing the chance of exposing sensitive data.

Additionally, onboarding a third party to a VPN is laborious and resource intense, requiring users to download a VPN client and then wait for admins to manually update access control list (ACL) and firmware (FW) policies.

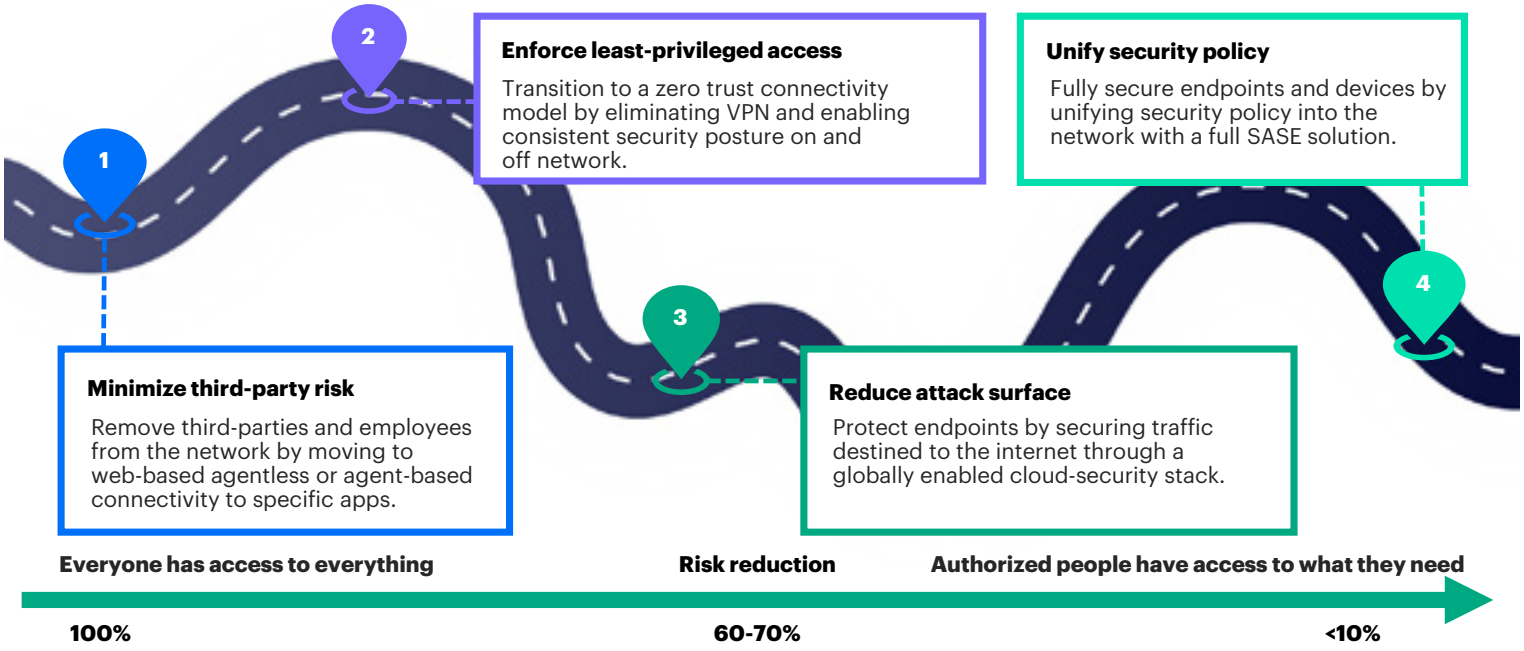


Figure 2. An image of a road depicting a four-step journey to a holistic zero trust strategy

With ZTNA, security teams can directly address the risks of third-party access by keeping users off the corporate network, enforcing granular zero trust policies to specific applications, and enhancing security through better visibility and control. Onboarding with ZTNA is significantly easier and more efficient, as it eliminates the need for VPN clients, allowing the use of bring your own devices (BYODs), and minimizing manual policy updates with centralized access management. ZTNA balances strong security with user-friendly access, minimizing third-party risks while improving collaboration with your partner, contractor, or supplier ecosystem.

Step 2: Enforce least-privileged access with ZTNA for remote and hybrid employees

As mobility increases, businesses are continually moving away from VPNs not only for third-party users, but also by leveraging ZTNA to fully replace VPNs for remote and hybrid employees. According to the 2024 SSE Adoption Report, nearly 80% of businesses now operate on a hybrid work model. This frequent transition between home and office introduces significant risks. Cybercriminals have exploited VPN design flaws to target businesses. Therefore, organizations must ensure business continuity, enhance user experience, and secure connectivity regardless of the work location.

ZTNA offers a more secure and efficient alternative to VPNs by granting least-privileged application access without bringing users on to the corporate network. This approach reduces attack surface and mitigates security risks, such as the impacts of insider threats and ransomware, by minimizing lateral movement through application-level segmentation. Additionally, ZTNA is far more user-friendly, providing always-on security paired with a better access experience and resulting in fewer IT tickets to manage.

Step 3: Reduce the attack surface with SSE

Once you've limited network third party and internal user/device access with ZTNA, the next step to a robust security posture is to reduce attack surfaces. Expanding from ZTNA to the full SSE cloud-security suite allows you to secure web traffic with a SWG, protect data with a CASB, and monitor user performance with DEM.

With a single SSE platform, security teams can deliver a holistic security approach, ensuring that your security measures are consistent and effective. It eliminates security gaps across all types of business traffic, regardless of where your users are located. As a result, you can deploy global security that follows your users wherever they go, providing peace of mind and robust protection in an increasingly complex digital environment.

Step 4: Unify security posture with SASE

Today more than ever, it's crucial that security and networking teams work in harmony, ensuring their functions and solutions complement and optimize each other. So often this is not the case, and teams can be at odds with different roles and different goals. The wrong technology exacerbates this issue, but the right technology fosters unity. A secure access service edge (SASE) framework enhances your network security by combining the value of a robust SD-WAN and cloud-delivered SSE platform. SASE combines WAN and security services into one framework, improving security, boosting performance, and making management easier, all at a global scale.

This integration ensures robust and adaptable security measures, offering comprehensive protection for users and devices. The SASE framework also fosters collaboration between security and networking teams, breaking down silos and optimizing network performance. These strategies are critical for maintaining a strong security posture and supporting overall business objectives in a dynamic digital environment.

Bonus step! Embrace universal ZTNA

As the number of Internet of Things (IoT), operational technology (OT), and unmanaged devices grow, and user devices frequently connect and disconnect from the network, it's crucial to maintain visibility over who and what is on your network. This visibility enables better access control and risk mitigation.

Universal ZTNA is a comprehensive solution that combines remote access ZTNA with an on-premises NAC to your zero trust strategy. This integration allows you to extend network and identity policies to both remote users and on-site employees seamlessly. Prioritize solutions that enhance user experience and simplify daily management. Ideally, the solution should feature a "centralized policy engine" that aligns policies based on user or device location. This engine will support both remote access and on-premises systems, addressing critical IoT/OT requirements.

Zero trust benefits the business and ROI

- Up to 78% decreased risk of data breach[4]
- Up to 91% time saving with zero trust[5]
- Up to 85% reduction in infrastructure costs[6]

Implementing a zero trust approach can deliver significant business benefits.

Increased security

By embedding the foundations of zero trust into your environment, you can prevent unauthorized access to applications and data. This proactive approach reduces the attack surface, and the risk of breaches, and enforces a universal security posture.

Improved user experience

Delivering fast, reliable (yet secure) access to all business resources, whether in the cloud, on-premises, or on the open internet, enhances productivity by reducing IT friction. Users can work more efficiently and increase business productivity with always-on security that doesn't hinder their ability to work.

Greater efficiency

Centralizing the management of network and security policies reduces the overhead associated with managing multiple systems across multiple geographies. A unified SASE framework offers a streamlined approach allowing your IT team to focus on strategic initiatives rather than day-to-day maintenance.

Ability to scale and adapt

A zero trust approach allows businesses to adapt to growth and the evolving technological and industry landscape. Support your digital transformation initiatives, like cloud adoption and a remote and hybrid work model, at the scale of cloud, ensuring that your security measures are future-proof and agile.

[4, 5, 6] Analysis from the HPE Aruba Networking Value Assessment Tool, 2025. Figures are based on assumptions and potential outcomes.

Start your journey with a strong use case

Secure third-party and contractor access

Give external users access to required business applications without bringing them onto the network using agentless ZTNA. This approach minimizes the risk of unauthorized access and ensures that third-party interactions are secure.

Modernize and secure employee connectivity

Replace legacy VPN solutions with always-on ZTNA, ensuring that users are secure whether they are inside or outside of the network. This modern approach enhances security and user experience.

Streamline IT M&A and divestiture processes

Rapidly provide users with access to the applications they need across companies using agentless ZTNA. This streamlined approach simplifies IT processes during mergers, acquisitions, and divestitures.

Improve performance while enhancing security

Modernize network edge infrastructure by leveraging SD-WAN and deliver security at scale with SWG. This approach ensures that your network is both secure and performant, supporting your business needs.

Take the next step towards zero trust

The journey to zero trust is not just a strategic imperative: it's a critical step towards securing your organization's future in an increasingly complex digital landscape. By adopting a zero trust approach, you can enhance your security posture, improve operational efficiency, and support your organization's growth and transformation.

Begin by assessing your current security measures, identifying gaps, and prioritizing areas for improvement. Leverage the insights and strategies outlined in this e-book to develop a comprehensive zero trust road map tailored to your organization's unique needs.

Ready to get started? Connect with a zero trust expert today to learn how we can support you every step of the way, ensuring that your zero trust journey is smooth, effective, and aligned with your business goals.

Learn more at

HPE.com/networking

Visit HPE.com

Chat now

© Copyright 2025 Hewlett Packard Enterprise Development LP. The information contained herein is subject to change without notice. The only warranties Hewlett Packard Enterprise products and services are set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. Hewlett Packard Enterprise shall not be liable for technical or editorial errors or omissions contained herein.

a00146025ENW, Rev. 1

HEWLETT PACKARD ENTERPRISE

hpe.com