HPE GreenLake

Elevate zero trust security and close your IT security gaps

Why adopting a zero trust approach can help secure your hybrid cloud environment

Get started >

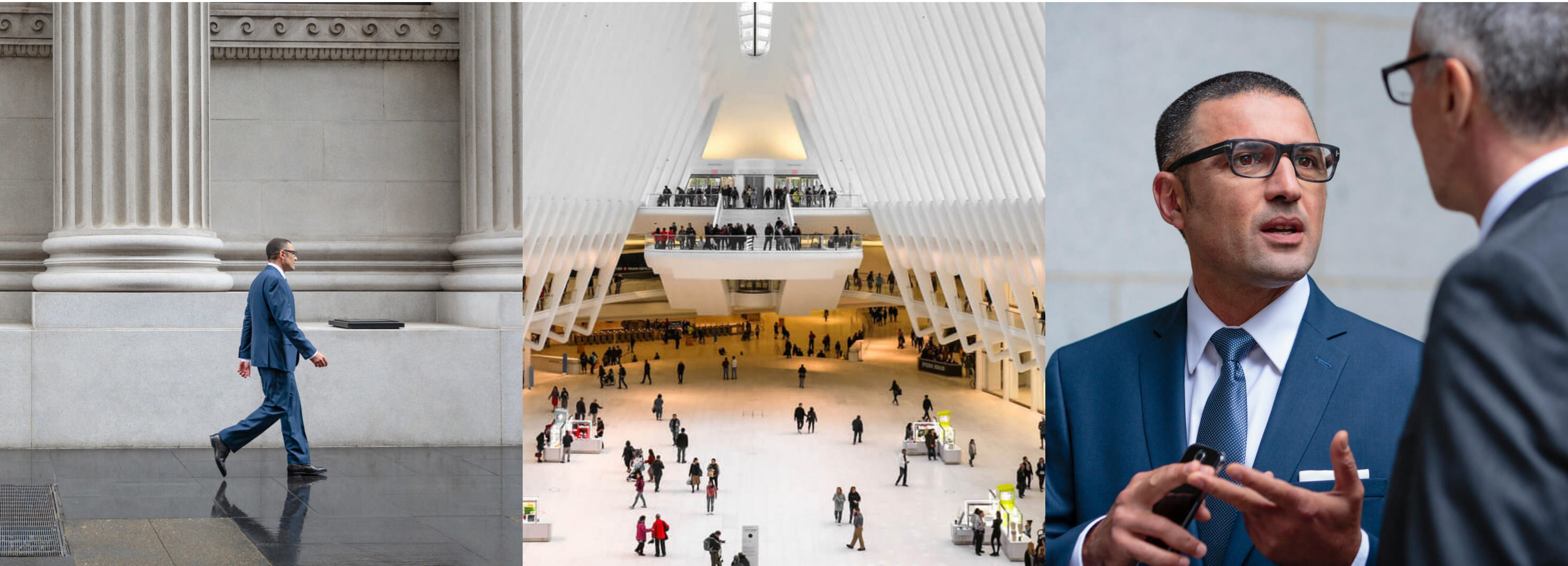


Table of contents

Cybercrime—a global threat

Preparing for the cyberattack inevitable

As the theft of digital information has become a pervasive global threat, cybersecurity has moved to center stage. Government agencies, public sector, and private sector are all impacted by cyber threats—including ransomware, phishing, data leakage, hacking, and insider threats.

So, for any organization operating in any industry, the question is not if you will be the target of cybercrime, but when and to what degree.

Considering these threats, end-user organizations have increased their focus on zero trust strategies that trust nothing—whether user, device, system, app, or data—until it has been authenticated and authorized. Additional drivers for zero trust environments include the desire to provide more secure, flexible hybrid connectivity for the increasingly mobile workforce.

Hewlett Packard Enterprise can help you design and implement a zero trust strategy and architecture that follows the basic zero trust principle that no user, device, or workload is granted IT access until it is identified and assigned the appropriate access privileges.

Zero trust by the numbers

64%

of top-performing security teams are likely to adopt zero trust models.[1]

By 2025

60% of all organizations will embrace zero trust models for their security.[2]

43%

of high-performance organizations have or will implement a SASE security model[3]

[1] The 2022 Study on Closing the IT Security Gap: Global, Ponemon Institute study sponsored by HPE, January 2022

[2] Gartner Unveils the Top Eight Cybersecurity Predictions for 2022-23, Gartner, June 2022

[3] The State of SD-WAN, SASE, and Zero Trust Security Architectures, Ponemon Institute study sponsored by Aruba, April 2021

Verifying integrity, validating for security posture

Assuming every identity is bad until proven good

Traditionally, organizations have relied on a “castle and moat” approach to perimeter-based security,[4] where the only way to cross the moat to get to the castle (your data center) is to cross a bridge (your firewall). This approach has a significant drawback—it assumes everything inside the perimeter is safe and does not account for attacks on the inside.

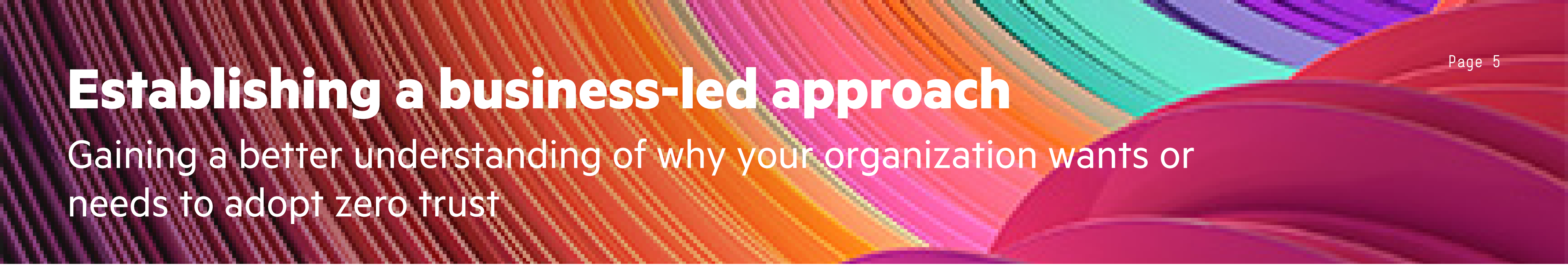
Firewalls are simply no longer sufficient to secure against the evolving and expanding threat landscape. The requirement is for security to assume that there is no perimeter. New methods are needed to protect against insider threats, malware, and ransomware intrusion—as well as more advanced and persistent threats targeting lower levels of the infrastructure, including boot kits and rootkits.

Recently, however, security strategies have been designed around the concepts of “trust verified” or zero trust. This approach is based on never trusting by default, always verifying identities, and always assuming the entity can introduce a security vulnerability unless proven otherwise. When you don’t trust by default, every identity is verified and access privileges are granted using context-based and risk-appropriate integrity verification before being allowed into the IT environment. In short, every identity is assumed bad until proven good.

HPE can help you design and implement a zero trust strategy from the inside out—designing a technology architecture that always verifies but never trusts and that also logs everything. HPE can help you to implement a zero trust model from edge to cloud with HPE GreenLake and build on reference architectures and expertise to help your organization leverage automation and improve your hybrid cloud experiences.

> **Never trust by default, always verify identities, and always assume the entity can introduce a security vulnerability unless proven otherwise.**

[4] What Is Perimeter Security In Cybersecurity, Security Forward, January 2022



Establishing a business-led approach

Gaining a better understanding of why your organization wants or needs to adopt zero trust

Adopting a business-led approach to zero trust means stepping back from the technology and first gaining a better understanding of why your organization wants or needs to adopt zero trust. HPE can start you in the right direction by identifying where you want your cybersecurity landscape to be, where you are today, and the best way to bridge that gap. Using this information, HPE can provide a clear picture of where zero trust can add value to your organization, as well as how zero trust can enable quick wins and support business use cases.

For an enterprise-wide zero trust approach to succeed, it should address six key tenets:

- Network trust
- Infrastructure trust
- Application trust
- Device trust
- Identity trust
- Data trust

Moving beyond the traditional opinion that zero trust is applied only at the network level, HPE expands the concept to state that zero trust is not simply applied at the network level alone, but that it must also address the infrastructure, applications, and workloads by defining and enforcing policies for identity and policy management.

After ascertaining a comprehensive view of your current environment—reviewing business processes, current asset inventory, security controls, architecture, security governance model, IT security strategy, and any future business and growth initiatives—HPE tailors a zero trust strategy that can help protect your organization while also helping your business take a risk-based approach to growth that is enabled by security.

Key pillars of a zero trust strategy:

[Future proof]

[Risk aware]

[Flexible]

[Proven design]

[Integrated]

Global push toward zero trust

Understanding the guidelines provided in the U.S. government's executive order for improving the world's cybersecurity posture

In May 2021, the United States government issued an executive order for improving the nation's cybersecurity posture.[5] The order provides guidelines on how to better address the persistent and increasingly sophisticated malicious cyber campaigns that threaten the public sector, the private sector, and ultimately the security and privacy of people around the world. These guidelines include details on how companies can improve their efforts to identify, deter, protect against, detect, and respond to malicious actions and actors. The order also requires agencies and organizations to:

- Adopt security best practices
- Advance toward zero trust
- Accelerate movement to secure cloud services, including software as a service, infrastructure as a service, and platform as a service
- Centralize and streamline access to cybersecurity data to drive analytics for identifying and managing cybersecurity risks
- Invest in both technology and personnel to match these modernization goals

This order prompted enterprises in the U.S. and around the world to consider zero trust as the preferred approach for improving global cybersecurity and to address the concerning expectation that cybercrime is estimated to cost the world economy $10.5 trillion/year in damages globally by 2025.[6]

New guidelines include details on how companies can improve their efforts to identify, deter, protect against, detect, and respond to malicious actions and actors.

[5] Executive Order on Improving the Nation's Cybersecurity, The White House, May 2021

[6] Cybercrime To Cost The World $10.5 Trillion Annually By 2025, Cybercrime Magazine, November 2020

Getting to success with a zero trust framework

Overcoming the lack of in-house expertise and supporting infrastructure to implement zero trust

HPE looks at zero trust differently than other vendors. We feel that zero trust is certainly part of the network construct but it also applies equally to everything else in the technology stack—including people, data, apps, infrastructure, and operating systems. In short, HPE can deliver a zero trust-ready IT stack. Our security experts can help design and assign zero trust policies to each level of the technology stack to drive the benefits of zero trust across your enterprise, from edge to cloud.

Success with a zero trust framework starts with assuming a business-led approach. This means gaining a clear understanding of why your organization needs to adopt zero trust and then identifying where you want your cybersecurity landscape to be, where you are today, and the best way to bridge that gap.

The business-led approach also requires cooperation between your security and business teams. If the security team understands what the business team is doing, then the security team can design a security architecture that enables the business to successfully meet its objectives.

The first step in a zero trust business-led initiative is to define the business case, starting with understanding which parts of the IT environment are going to be most appropriate to consider for adopting zero trust. The next step is to identify some use cases to demonstrate zero trust to the rest of the organization.

Adopting zero trust can deliver important business and financial benefits:

Reduced organizational risk

Decreased potential of a security breach

Better control of the security stack

Improved quality of security alerts

Enhanced user experience

Enabling an effective zero trust framework

Designing a unique zero trust framework, based on each organization and its security goals

Though unique, every HPE designed zero trust strategy interoperates with the control plane that includes the security governance, orchestration, and all the other capabilities built into an organization. In addition, every zero trust strategy and architecture from HPE addresses a zero trust approach to networking, infrastructure, and workloads—helping ensure that identity and integrity are verified as key elements. Without automation—which HPE provides—implementing a zero trust model can be significantly more challenging.

Networking

Hybrid workplace initiatives, including IoT and edge computing, dissolve the traditional IT perimeter. The goal for organizations is to provide anytime, anywhere connectivity without sacrificing security while maintaining visibility and control without impacting the user experience. HPE can help you reach this goal with Aruba ClearPass network access control and Aruba ClearPass Policy Manager.

Infrastructure

HPE delivers secure zero trust-enabled cloud-native building blocks with integrity verification initiated in the secure supply chain and anchored in the silicon root of trust—starting from the time of manufacture in a secure supply chain. Throughout the manufacturing process until delivery, zero trust-based confirmation is initiated at first boot before anything connects to the network.

Workloads

The HPE zero trust workload solution leverages the Secure Production Identity Framework for Everyone (SPIFFE) and SPIFFE Runtime Environment (SPIRE) open source projects from the Cloud Native Computing Foundation. These projects enable HPE to apply zero trust principles to its services delivered in a cloud environment with implementations, including high-performance computing systems, end-to-end data fabric, and edge-to-cloud platform. With the HPE zero trust approach, each identity is verified continuously—to help ensure that two reciprocal organizations can collaborate using trusted identities. This level of zero trust validation is possible only through continuous monitoring.

With HPE, you can:

Identify and remediate security gaps with the right mix of integrated security design and constant monitoring

→

Reduce the costs and brand impact of cybercrime by proactively identifying and resolving threats while freeing up IT and security staff to focus on business priorities

→

Bridge security skills gaps by augmenting your skills with HPE experts

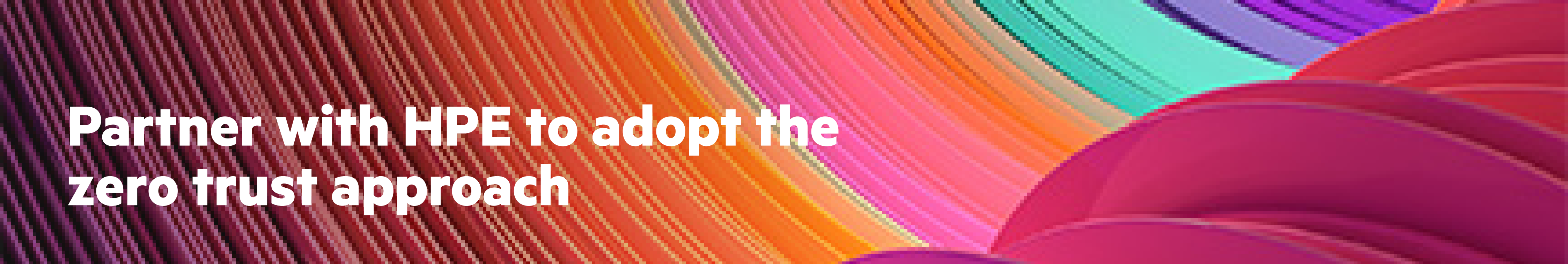
Ready to adopt the zero trust approach?

Stop cyberattacks before they occur

Adopting a business-led approach to zero trust will add value at every level of your organization. With the right mix of integrated security design and constant monitoring, your organization can reduce the costs and brand impact of cybercrime by proactively identifying and resolving threats while freeing up IT and security staff to focus on business priorities. HPE can help you:

- **Ensure security is designed into your business use cases from edge to cloud**
- **Reduce organizational risk through a better understanding of your environment**
- **Significantly improve control over your security stack**
- **Lower your CAPEX and OPEX**
- **Make security transparent to your users**
- **Reduce the scope of compliance through continuous monitoring and inspection of your environment**

With **HPE Managed IT Compliance services**, HPE experts can help you to identify and remediate security gaps with the right mix of integrated security design. Keep up to date with the changing regulations and compliance controls that are needed to protect and optimize your security risk and compliance across your multicloud environment as you adopt and enhance your zero trust approach.



Partner with HPE to adopt the zero trust approach

Visit **HPE GreenLake**

As you face the inevitable occurrence of a cyberattack, a business-led zero trust approach can help you stop the attack before it occurs. Learn how HPE can help you gain full visibility, granular control, and enforcement with a built-in foundation for zero trust designed to protect your data while also mitigating risks, filling skills and resource gaps, and lowering your operating costs.

Learn more at

Connect with your HPE representative today to learn more about adopting a business-led zero trust approach. Discover how your organization can:

- Gain full visibility, granular control, and enforcement with a built-in foundation for zero trust and SASE frameworks: Aruba ClearPass Policy Manager
- Protect your data and mitigate risks with HPE Managed IT Compliance, delivered as a managed service

Make the right purchase decision.
Contact our presales specialists.

Chat now (sales)

Call now

Get updates

Hewlett Packard
Enterprise

a50007343ENW, Rev. 1