HPE GreenLake

Securing your distributed enterprise from edge to cloud

Standards, frameworks, and best practices to secure the complex distributed enterprise

Get started >

Table of contents

Secure your complex distributed enterprise E2C

Starting with a secure supply chain through to the edge and cloud

It's complicated

The days of an easy-to-secure perimeter have virtually disappeared. Modern IT landscapes present a host of daunting challenges, as data and infrastructure are now spread out across a mix of on-premises data centers, hybrid cloud, and edge-computing devices. This complex, distributed enterprise scenario—from edge to cloud (E2C)—is further complicated by the proliferation of software-as-a-service (SaaS) applications and remote workforces, making it difficult to achieve the high levels of security required to combat global adversarial threats from cybercriminals, who continue to innovate and wage more sophisticated attacks.

The path to success

Hewlett Packard Enterprise recommends you start with a secure supply chain, helping ensure your vendors follow a set of security standards to help minimize their risk profile, as well as your own. This applies to both private sector businesses and government entities, where infrastructure vulnerabilities can exist anywhere along the supply chain, endangering critical operations of being infiltrated and/or disrupted. The next steps involve analyzing your current maturity (security posture) to identify potential security gaps across the whole range of your digital estate—from data to systems, people, processes, and technologies. Then, go about closing any/all gaps found in your particular situation—no two are alike although we can still benefit from the experience of others.

The growing edge

It is estimated that

70%

of data now resides on-premises.[1] However, other types of data that are collected, processed, and managed at the edge—outside of public clouds—are expected to grow by up to

70% by 2025.[2]

You don't have to reinvent the wheel

There are many aids to help you get started. This eBook looks at the available cybersecurity standards and frameworks to helps ensure compliance with regulations, as well as HPE recommended best practices to learn from. A handy checklist is also provided to help you stay on track—regardless of where you are in your cybersecurity journey.

In addition, HPE offers a vast array of security solutions and services to assist you on your path to protect the distributed enterprise of today and tomorrow. Visit HPE.com for full details.

[1] "Cloud vs. on-prem? Now you can choose not to choose," HPE, May 2022

[2] "Predicts 2022: The Distributed Enterprise Drives Computing to the Edge," Gartner, October 2021

Build a modern security-first culture

A collective effort against cyber threats

Security goes beyond IT—it's everyone's business

Despite many significant advances in cybersecurity technology products, security vulnerability remains a major concern, in many cases due to staff lacking knowledge of safe cyber practices, social engineering, and negligent behaviors, not to mention more data and dispersed locations than ever before, on-premises and in the cloud.

Building a **security-first** culture is critical to thriving in a world that's rife with uncertainty. In such a culture, protecting your organization's vital assets becomes everyone's business, not just IT. HPE takes it a step further by promoting a shared security responsibility model that clearly defines the roles and responsibilities of both your staff and service providers.

Zero trust perimeter

Building a zero trust perimeter around your distributed enterprise goes hand in hand with the concept of security first.

- It begins with a zero trust-enabled architecture that is embedded in a secure supply chain and extends to hardware, apps, and workloads—one that's supported by automated and continuous integrity verification at startup and during runtime.
- These proactive security measures must be designed-in early in every data modernization and digital transformation initiative.

HPE Education Services for security

In support of this paradigm shift, HPE recommends company-wide awareness training to mitigate common sources of cyber risk and better secure your distributed enterprise, wherever data and people reside. We can help your staff develop a security-first and zero trust mindset by developing the skills and expertise needed to safeguard your business data, improve cybersecurity awareness, and learn best practices to effectively implement a robust cybersecurity risk management framework.

HPE stands by these and other proven security solutions and services to help you establish and maintain a security-first, zero trust approach across your entire IT landscape.

How the modern distributed enterprise came about

- Digital transformation—Introducing new, open technologies
- Mergers and acquisitions—Adding more personnel in geographically dispersed offices
- IT modernization—Requiring data management across a wider range of services, devices, and locations
- Migration of business-critical data to the cloud for anywhere, anytime access—Causing more security concerns
- New ways of working and doing business (for example, remote and mobile work styles)—Leading to a lack of control outside the traditional perimeter

Cybersecurity frameworks and standards

Why we need them and the important role they play

Industry-recognized guidance

Cybersecurity frameworks (CSFs), such as the NIST Cybersecurity Framework and International Organization for Standardization (ISO) certifications—for example, ISO 27001 and ISO 27002—are playing an increasingly important role. They provide:

- A set of standards to help understand your company's risk profile and those of your vendors
- Knowledge that is based on an accumulation of lessons learned
- Continual updates to address new threats, including incident-appropriate responses

HPE recommends you explore the industry-recognized CSFs for their detailed guidance on how to identify, protect, detect, respond, and recover from cyber threats. Then, decide what's right for your organization.

Designing your unique framework

The ultimate objective is to implement your cybersecurity risk management framework that best suits your needs. One that is prioritized, flexible, repeatable, and cost-effective to reduce your cyber vulnerabilities, along with policies for improved cyber resilience—capable of addressing new threats as they arise. It should consider the findings of the comprehensive cyber vulnerability analysis you conduct,[3] including actions to bridge cyber skills gaps on your security team, mitigate vulnerabilities, and prepare for more formal compliance assessments or audits.

Managed security

As an alternative, you can subscribe to security as a managed service. HPE GreenLake Management Services are designed to help you fill gaps in security, migration, and performance—even manage your entire hybrid cloud environment for you.

And for all your digital transformation initiatives...

We offer **HPE Edge-to-Cloud Adoption Framework** to help you assess your organization's maturity level for security—and key domains, such as strategy and governance, people, operations, innovation, applications, DevOps, and data. It provides benchmarks against peers and other industry models while helping you develop an actionable road map to meet critical digital imperatives to support a path to secure modernization.

[3] "HPE Vulnerability Analysis Services," HPE data sheet, July 2020

Apply best practices

Following proven methods to achieve your security goals

The following list of six best practices is based on HPE's experience in providing cybersecurity solutions and services to customers with distributed hybrid cloud environments:

- **Use a secure-by-design approach**—Security must be designed-in early in every data modernization and digital transformation initiative.
- **Understand your risks and fix vulnerabilities before hackers find them**—This analysis provides insights into the risks your organizational assets are exposed to and how to mitigate them.
- **Implement or optimize your cybersecurity framework**—After assessing your cybersecurity current state, design or enhance the process required to manage your unique IT landscape.
- **Clearly define who is responsible for security**—Defining the line between your responsibilities and those of your service providers helps avoid the risk of introducing vulnerabilities into your public, hybrid, and multicloud environments.
- **Align your security strategy with your business priorities**—Your corporate board or executives need to align business and cybersecurity plans to help ensure focus on the right priorities.
- **Manage risk and improve compliance**—This can be optimized through security managed as a service, including security incident and event monitoring (SIEM) and vulnerability monitoring.
- **Educate and grow expertise**—To strengthen your organization's cybersecurity, it is important to invest in a mix of end-user training and educational programs that fit your security-first corporate culture.

Security checklist

1. Assess your cybersecurity maturity.
2. Embrace a secure edge-to-cloud strategy.
3. Adopt a shared responsibility model for security to ensure governance and accountability for your hybrid cloud assets.
4. Apply best practices.
5. Take a secure-by-design approach.
6. Modernize by adopting infrastructure that is enabled for zero trust.
7. Assess organizational risk and vulnerabilities.
8. Clearly define roles and responsibilities for security.
9. Align security and risk profiles with business priorities.
10. Design security into the technology platform (forming a zero trust perimeter).
11. Scale security to everywhere data lives.
12. Centralize the management of security operations.
13. Build a security-first culture.
14. Understand risk and fix vulnerabilities before hackers find them.
15. Implement or optimize a cybersecurity framework.
16. Implement a DevSecOps approach.
17. Manage risk and improve compliance.
18. Educate and invest in employees and grow expertise.

Your trusted source for E2C security

Benefits of working with HPE to secure your distributed hybrid cloud ecosystem

HPE GreenLake edge-to-cloud platform

We secure our platform with integrity verification that automatically and continuously detects threats and unauthorized changes to the infrastructure, apps, and workloads. Initiated in our secure supply chain and anchored in the silicon root of trust, our integrity verification capabilities cryptographically measure the HPE GreenLake operating environment to establish trusted security building blocks. And that enables our cloud-native, zero trust architecture from edge to cloud—without performance trade-offs or reliance on signatures.

HPE GreenLake security managed as a service

We provide a secure cloud experience with infrastructure and services based on zero trust principles. We use identity and privilege as foundational principles and separate service provider operations from customer workloads by default. Management activities across your distributed environment are logged for audit purposes—we act as the custodian of your data in use, at rest, and in motion. By supporting customer "bring your own key (BYOK)," however, you retain ownership of your data.

HPE GreenLake security shared responsibility model

This model delivers a clearly delineated view of where security responsibility lies—with you, HPE, or your colocation provider—defined by resource location, usage, management, and operation. It helps ensure governance and accountability for your hybrid cloud assets.

A single source of truth

Protect your business from evolving threats with the right tools and skills, by leveraging **HPE GreenLake for security, risk, and compliance**. These services help you gain control of IT compliance, corporate governance, and regulatory requirements with real-time monitoring, remediation, and recommendations. HPE can also help your security and IT teams identify IT security gaps through ongoing monitoring and management.[4]

With on-premises infrastructure—including resources and cloud services supplied in a consumption model—organizations still control their applications and data. That includes compliance and security risk mitigation. HPE has the expertise to help you to meet these requirements and serve as an extension of your IT and security teams.

[4] "Mitigating risk with managed security from HPE GreenLake Management Services," HPE brochure, 2022

Ready to enhance your E2C security?

Meet the security challenges of today and beyond

Managing workstreams across remote sites where physical security cannot be verified, in addition to multidomain workstreams on-premises—while ensuring always-on connectivity, compliance, and security are managed cost-effectively—is no easy task. HPE has proven methods and strategies to help your organization achieve a security-first, zero trust environment. Find out how HPE can help you:

- Identify your current security vulnerabilities and work to close gaps
- Build a robust cybersecurity risk management framework
- Mitigate common sources of cyber risks to better secure your whole enterprise
- Apply lessons learned from major cyber incidents
- Educate the workforce to raise security awareness
- Ensure cybersecurity resilience to be ready for known, and unknown, types of adversarial attacks—especially on the edge where they often occur

Partner with HPE for security

HPE offers organizations innovative ways to protect their ever-expanding, distributed IT estate, to secure their data, people, processes, and technology—from the edge to the cloud, and everywhere in between.

Learn more at

HPE GreenLake managed security

Make the right purchase decision.
Contact our presales specialists.

Chat now (sales)

Call now

Get updates

Visit **HPE GreenLake**

Hewlett Packard
Enterprise