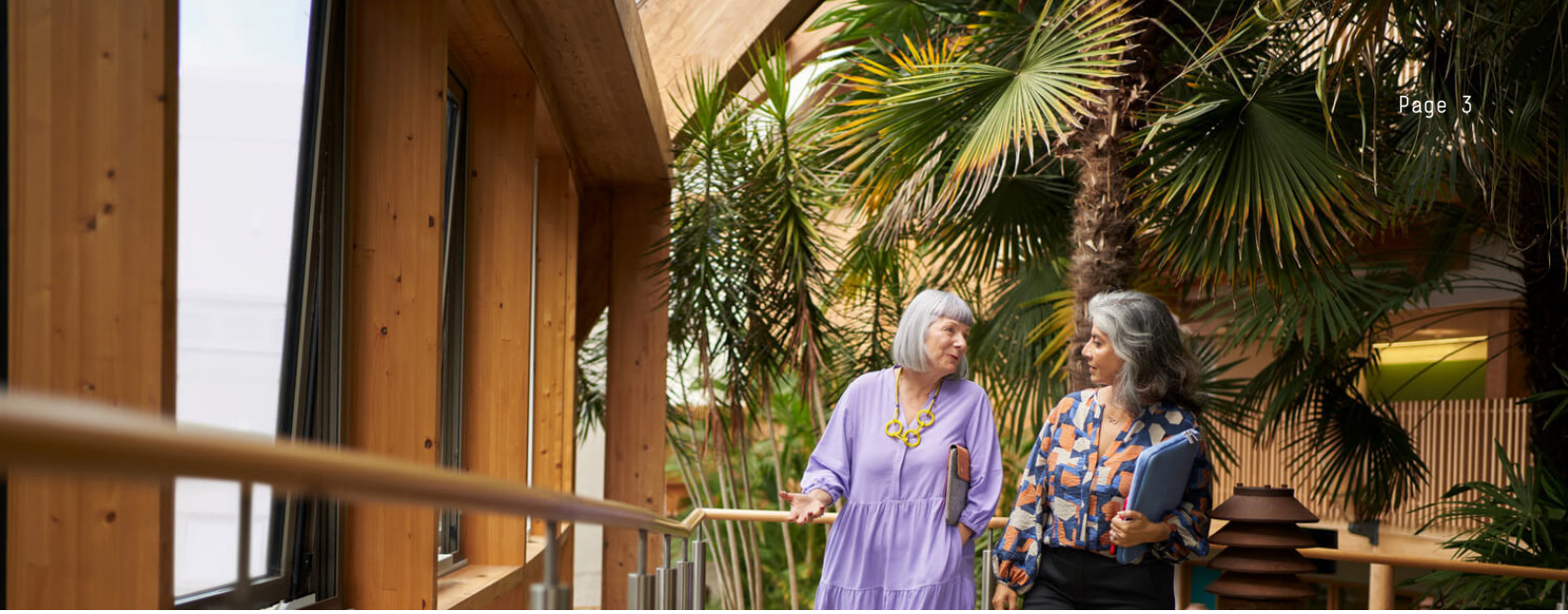
HPE GreenLake

Securing the complex, distributed enterprise

The importance of protecting your IT landscape, from edge to cloud

Table of contents



Executive summary

Security goes beyond IT—it's people and processes, too. A proven framework for data-informed threat assessment includes an evaluation of current talent and processes and a road map for implementation and improvements.

As new business strategies reinvent the IT landscape through modernization efforts and digital transformation initiatives, the resulting distributed environment is full of new, sometimes unknown cyber risks with more points of vulnerability. Data and infrastructure are now spread out across a mix of on-premises data centers, hybrid clouds, and edge-computing devices. Securing the distributed enterprise from edge to cloud presents a host of daunting challenges. Software-as-a-service (SaaS) applications and remote work scenarios add further complexity and obstacles to achieving high levels of security, particularly in an adversarial global environment where cyber threats are more serious than ever, and cybercriminals continue to innovate and wage more sophisticated attacks.

Today's edge-to-cloud computing environment requires that enterprise security spans the whole range of your digital estate to protect everything—from data to systems, people, processes, and technologies. New and unified approaches to data security are critical to reduce risk, improve regulatory compliance, and protect your most valuable asset: data. Now that traditional security perimeters are gone, the question we must ask ourselves is, what can be done to mitigate cyber risks and shore up vulnerabilities for today's edge-to-cloud world?

Introduction

Organizations around the world are embracing digital transformation while many are being forced to reexamine the ability of their existing technology infrastructure to meet the demands of data growth, edge expansion, the Internet of Things (IoT), distributed (remote) workforces, and security. As data is generated and consumed across clouds, edges, data centers, and colocations, IDC research suggests that organizations face a significant risk of information silos and security vulnerabilities forming across the enterprise, limiting an organization's ability to make effective, data-driven decisions based on trusted sources.[1]

Organizations can no longer make compromises when running their mission-critical apps and crucial enterprise data services without risking their ability to ensure a trusted operating environment. They can leverage value delivered by both on-premises resources and the public cloud. However, for this value to be realized securely, certain key considerations must be addressed. This white paper discusses those considerations and more. It offers recommendations and best practices drawn from the considerable experience Hewlett Packard Enterprise has in providing cybersecurity solutions and services to distributed enterprise customers.

The modern distributed enterprise

Many IT organizations are still saddled with legacy applications and infrastructure. Add to that the newer technologies and work styles—such as the shift to hybrid cloud, the proliferation of data mobility (that is, moving from location to location and cloud to cloud), devices and data at the edge, IoT, and today's remote workforces that are now dispersed around the world in many cases—fueled by the need to generate insights from data wherever it lives. So, it's no wonder the existing resources are overwhelmed by managing and securing such expansive operations. To further complicate matters, the modern distributed enterprise not only encompasses the hybrid cloud and edge infrastructure but also includes SaaS subscriptions and API-driven machine-to-machine integration with external entities.

[1] "Using Data Protection as a Service to Address Modern Data Threats," IDC, November 2021

All this came about because of:

- 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

Importance of cybersecurity frameworks

Increasingly, enterprises are struggling to assess their cybersecurity maturity and identify their security gaps while meeting critical obligations to comply with cybersecurity regulations. Cybersecurity frameworks (CSFs) such as the NIST Cybersecurity Framework and certifications such as ISO 27001 and ISO 27002 certifications and many more—are playing an increasingly important role. These frameworks provide a common language and set of standards for security leaders to understand their company's risk profile and those of their vendors, as well. This is especially true for governments, public sector agencies, and organizations operating in critical infrastructure market sectors that require verifiable cyber assurance and zero trust assurance.

Frameworks are needed to ensure the organization complies with the evolving and emerging security, governance, and privacy regulations and, importantly, can apply lessons learned from major cyber incidents. Now, protecting national security for many governments worldwide requires their entities and agencies to partner with the private sector. Together, they must adapt to the continuously changing threat environment, ensuring that critical infrastructure and technology solutions are built and operated securely.

With a CSF in place, it becomes much easier to define the processes and procedures that your organization must have to assess, monitor, and mitigate cybersecurity risk. It also outlines a structured approach to applying best practices when determining where to focus time, develop talent, and build road maps for resources and budgets to develop a comprehensive cybersecurity protection plan. Additionally, such frameworks provide a benchmark against which your organization can measure the effectiveness of its security investments and the success of its efforts.

The perimeter is gone

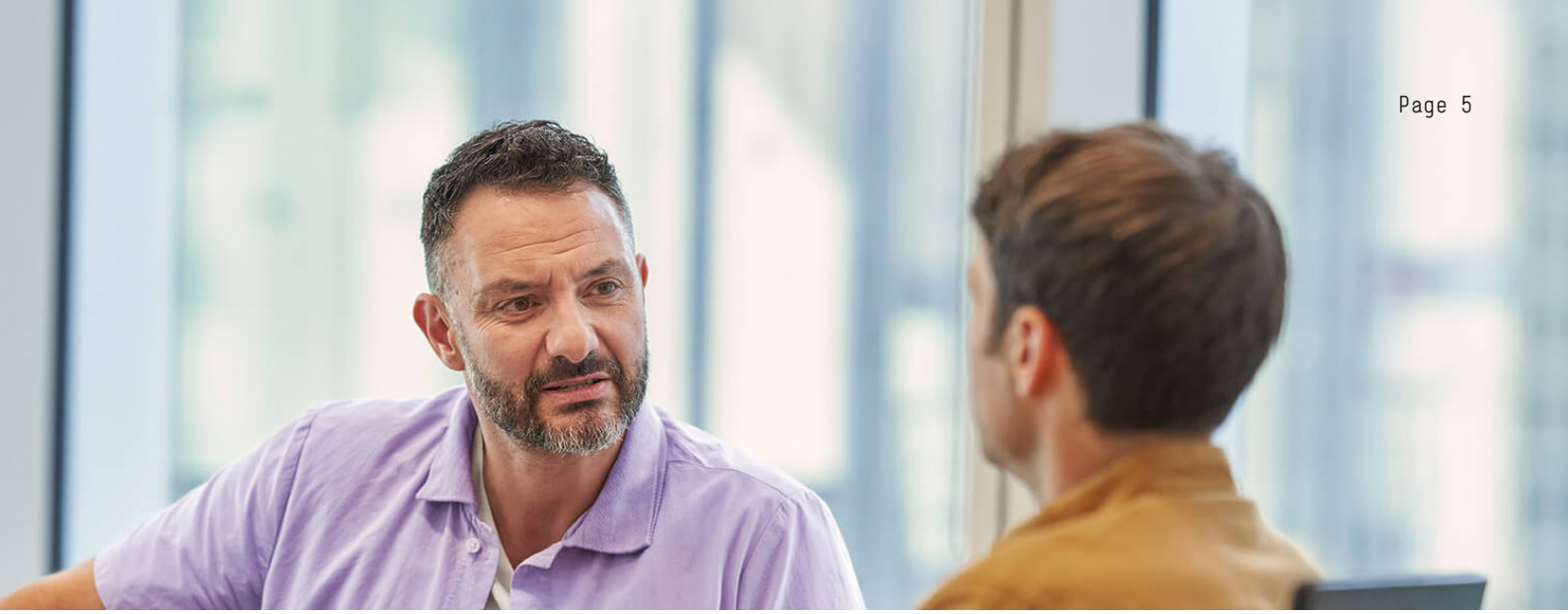
With digital assets everywhere, the days of an easy-to-secure perimeter have virtually disappeared. We find ourselves in varying stages of maturity—particularly who is responsible for enterprise-wide security and how that security will be effectively accomplished. The best time to define these roles and responsibilities is in the early stage of planning your digital transformation project, which is typically comprised of the public cloud, colocation, and data center elements that need to be kept secure.

The velocity at which cloud models change, however, requires security efforts to keep pace with transformation, by continually assessing the current security plan, aligning it to business priorities and risk profiles, and making modifications as needed. The growing complexity and lack of visibility into every layer of the technology stack—from edge to cloud and throughout the technology lifecycle—present unique challenges that impact organizational staffing, especially with industry-wide cybersecurity skills and experience scarcity at present time.

Visibility issues
Today, it is estimated that 70% of data resides on-premises.[2] 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.[3] Managing workstreams across these remote sites where physical security cannot be verified, in addition to workstreams on-premises, while ensuring always-on connectivity, compliance, and security are managed most cost-effectively, is no easy task.

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

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



Recommended best practices

The following best practices are recommended to get you started with designing and launching your enterprise security program:

- **Use a secure-by-design approach**—Security must be designed in early for every data modernization and digital transformation initiative. It begins with an architecture enabled by zero trust and 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. Hybrid cloud platforms must also be comprehensively secured.
- **Clearly define who is responsible for security**—A shared security responsibility model that clearly defines the roles and responsibilities, of both the consumer and the service provider, is needed to govern the security obligations of a cloud provider and its users to ensure accountability. Defining the line between your responsibilities and those of your service providers helps mitigate the risk of introducing vulnerabilities into your public, hybrid, and multicloud environments.
- **Align your security strategy with your business priorities**—By understanding the gaps between business and cybersecurity priorities, your corporate board or executives can start aligning both strategies to ensure key priorities are focused on and resources and budgets are allocated accordingly. It is very important that business leaders reach a state of agreement on the priorities and fully understand risk profiles. This process may be complex, but it is vitally important to ensure the support of all stakeholders and to determine ongoingly the acceptable risk thresholds for your business in a constantly changing environment. It is essential to protect data, intellectual property, and revenue streams, as these are often the primary targets of attackers.
- **Build a security-first culture**—Creating a security-first culture is a critical step to being able to thrive in a world that's rife with uncertainty. In such a culture, protecting your organization's vital assets becomes everyone's business. Despite many significant advances in cybersecurity technology products, a lack of staff awareness of safe cyber practices, social engineering, and negligent behaviors remains a major source of security vulnerability. It is important to make sufficient investment in staff awareness training, given these prominent sources of cyber risk, and because a collective effort against cyber threats will better serve your enterprise.
- **Understand your risks and fix vulnerabilities before hackers find them**—Cyber vulnerability analysis, also called security testing or pen testing, is a process to assess your organization's security posture and identify your vulnerabilities before an attacker has the chance to exploit them. This process provides insights into the risks that organizational assets are exposed to, from both an internal and external perspective. It can also help you identify potential security gaps in preparation for more formal compliance assessments or audits. To enhance the security posture of your organization, it is also important to develop actionable plans to help bridge any cyber skills gaps on your security team and mitigate vulnerabilities.

- **Implement or optimize your cybersecurity framework**—Explore industry-recognized CSFs, such as NIST Cybersecurity Framework, as they offer detailed guidance on how to identify, protect against, detect, respond to, and recover from cyber threats. Cybersecurity frameworks are based on an accumulation of lessons learned and are continually modified to address new threats, including an incident-appropriate response. The objective is to use a framework that is prioritized, flexible, repeatable, and cost-effective to reduce cyber vulnerabilities, along with policies for improved cyber resilience.
- **Manage risk and improve compliance**—Managing operational risks can be optimized with elements of your security managed as a service, including security information and event management (SIEM) and vulnerability monitoring, with an approach that spans technologies, people, and processes. Gaining a comprehensive view of your IT compliance, corporate governance, and regulatory compliance controls can provide a single source of truth across the security, risk, and compliance (SRC) workstream with real-time monitoring and remediation recommendations.
- **Educate and grow expertise**—To strengthen the organization's cybersecurity, it is also important to invest in a comprehensive mix of end-user training and educational programs that fit your corporate culture. Educate teams on how to target relevant threats and understand key security concepts—including risk assessment and management, threat identification, compliance, governance, and managing information assets.

A road map to follow

It helps to have a road map when embarking on your journey to achieve distributed enterprise security. In addition to cybersecurity standards and frameworks, there are practical steps you can take or use as a checklist along the way.

Step-by-step process

The following steps provide a high-level guide to implementing an enterprise security plan:

1. Assess your cybersecurity maturity.
2. Embrace an edge-to-cloud security 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 risks 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 (that is, 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 risks 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.

How HPE helps secure the distributed enterprise

Even with increased awareness of the risks mentioned in this technical white paper, combined with an increase in security and compliance-related spending, managing IT security still presents an array of challenges, including gaps in cyber skills and expertise, siloed tools, a lack of automation, and other complexities. These challenges grow larger when you consider outsourcing IT operations to a third-party service provider. While certain operations can be safely outsourced, the organizational risks of security and compliance failure cannot.

For your cloud transformation initiatives, HPE has developed the **HPE Edge-to-Cloud Adoption Framework**—built upon the experience of hundreds of successful customer engagements where HPE has identified several critical areas that enterprises should evaluate and measure to run an effective cloud operating model and meet the right standards. These domains—which include strategy and governance, security, people, operations, innovation, applications, DevOps, and data—have formed the core of the HPE Edge-to-Cloud Adoption Framework.

The framework allows organizations to assess their maturity level for security across key domains to provide benchmarks against peers and other industry models. In addition, it provides organizations with a common vernacular and aids in developing an actionable road map to meet critical digital imperatives to support a path to secure modernization.

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

Managed security from HPE GreenLake Management Services is designed to help you fill gaps in areas such as security, migration, and performance, or even manage your entire hybrid environment for you. Managed security enhances the HPE GreenLake Management Services customer environment by offering services that include security monitoring, privileged access management, vulnerability management, and security hardening with the attention and accountability of an account security officer.

Managed security delivered as a managed service helps your organization with the additional expertise you need to help identify and mitigate security threats across your distributed cloud environment—from edge to cloud. With our long history of managed services experience, the capability to deliver end-to-end security management, and recent innovations in remote infrastructure management, you'll have the confidence of knowing that the security of your data, applications, and infrastructure is in capable hands with HPE.

Benefits of working with HPE to secure your distributed enterprise

- **Security innovations for your organization**—HPE GreenLake has been designed with security top of mind. We secure the HPE GreenLake edge-to-cloud platform with integrity verification that automatically and continuously detects threats and unauthorized changes to the infrastructure, apps, or workloads. Initiated in our secure supply chain and anchored in the silicon root of trust from HPE, our integrity verification capabilities cryptographically measure the HPE GreenLake operating environment to establish trusted security building blocks that enable our cloud-native, zero trust architecture from edge to cloud—without performance trade-offs or reliance on signatures.
- **Secure by design**—HPE provides 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. All management activities are logged for audit purposes, and we understand that for as-a-service environments from HPE GreenLake, we are a custodian for your data in use, at rest, and in motion. So, we support customers "bring your own key (BYOK)" to help ensure you retain ownership of your data.

- **Comprehensive view of your ecosystem**—The HPE GreenLake security shared responsibility model includes a delineated view of where security responsibility lies—with you, HPE, or your colocation provider—defined by resource location, usage, management, and operation.
- **Close your IT security gaps**—HPE helps improve your security monitoring, privilege access management, vulnerability management, and security hardening—by providing ways to mitigate against risks to your outsourced resources with the right security expertise and experience, simplified processes, and holistic management solutions—all aimed at reducing organizational risk.
- **Establish a single source of truth**—Protect your business from evolving threats with the right tools and skills, leveraging **HPE GreenLake for SRC**. Gain control of IT compliance, corporate governance, and regulatory compliance with real-time monitoring and remediation recommendations. HPE can help your security and IT teams identify and remediate IT security gaps and provide ongoing monitoring and management.[4]
- **Learn to recognize and prevent cyber threats**—Enable your staff with a security-first mindset and grow 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 with **HPE Education Services for security**.

Conclusion

In today's distributed enterprise environment, the path to a mature state of security—where cyber threats are prevented and vulnerabilities are eliminated—takes planning, committed and skilled IT resources, and insights from experts. The security frameworks, standards, and best practices presented in this white paper are meant to assist you in that ever-evolving process, so your business survives and thrives in this time of heightened risks and uncertainty. HPE stands by its proven security solutions and services to help you develop and maintain a security-first, zero trust approach across your entire IT landscape. A reimagined, modernized cybersecurity plan, when properly designed-in and implemented, will protect your organization's data, people, processes, and IT systems everywhere—beyond the traditional perimeter, from edge to cloud—and enable you to address new threats as they arise.

Learn more at

HPE GreenLake for security, risk and compliance

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

Hewlett Packard Enterprise

a50007376ENW