HPE GreenLake

Balance security, speed, and complexity with data-first modernization

Get security confident

Get started >

Table of contents

Keeping security in lockstep with business transformation

Building security into your data-driven modernization initiatives

With digital transformation continuing to accelerate, security must also scale to keep pace to ensure the protection of any data, anywhere. Hewlett Packard Enterprise can help you build security into your data-driven modernization initiatives—offering solutions and services designed to scale at the speed of your business to deliver on transformational objectives.

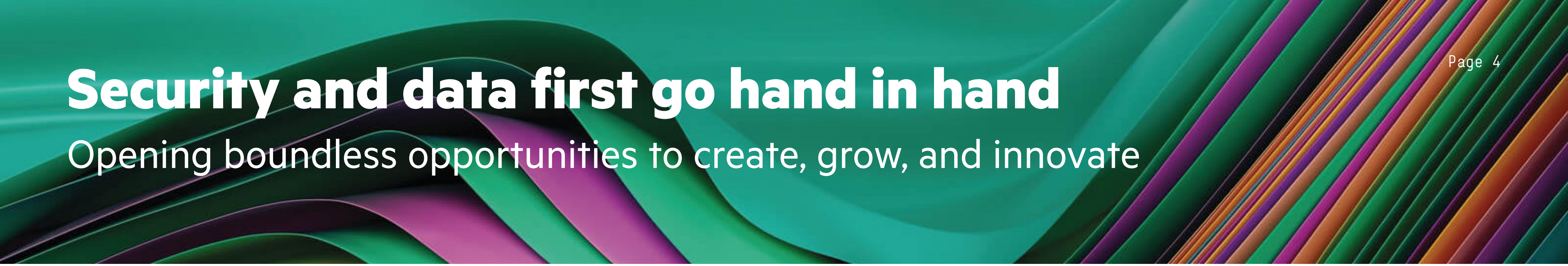
As you move more workloads to the cloud, HPE can provide solutions to enhance your visibility and monitoring capabilities—enabling you to help ensure your data remains protected while in transit (from the data center to the cloud and back), in use, and at rest.

And if you are capitalizing on the benefits of securing data even at the edge—manufacturing plants, retail stores, healthcare clinics, or branch offices where physical security cannot always be guaranteed—you can now benefit from a wide range of HPE solutions and services designed to deliver the same level of security at edge locations as in the data center.

Leave legacy processes behind

“With security controls, enterprises are running into problems because they’re not adapting to their new environments. While the controls themselves don’t change, how they’re implemented likely will. Enterprises are attempting to use traditional on-premises tools and approaches in a hybrid, cloud-native estate. This doesn’t work, and companies that don’t appreciate the architectural difference will take more time on their overall transformations and have to spend more money.”[1]

[1] “Security: The foundation for transformation success,” Sean Foley, chief technology and strategy officer at HPE, May 25, 2022.



Security and data first go hand in hand

Opening boundless opportunities to create, grow, and innovate

The alarming cybersecurity statistics shown, combined with the complexity of data-first modernization, can create an overwhelming lack of security confidence. The security and data-first experts at HPE can suggest systems, solutions, and approaches to help alleviate your fear of cyberattacks, so you can become security confident.

What is data-first modernization?

Becoming data first means providing seamless access to the data you rely on for insights to run and grow your business and giving your data science teams the tools they need to analyze the data. Becoming data first opens boundless opportunities to create, grow, and innovate—which are vitally important when your business wants to be nimbler and more flexible in the use of your data.

The HPE advisory and professional services teams can suggest ways to take a secure data-first approach at every step of your digital transformation journey—enabling you to align IT goals and priorities according to one common data agenda. For instance, HPE can help you build your cyber resilience to address these priorities, and more:

- Simplify data management and protection
- Secure your data across edge to cloud
- Achieve a cloud experience everywhere
- Create a connected experience at the edge
- Embrace artificial intelligence (AI) and analytics at scale
- Harness the power of supercomputing

13%

higher ransomware breaches in 2022, a greater increase than the past 5 years combined[2]

$10.5T annually

The cost of global cybercrime damages by 2025[3]

Only 30%

of businesses today feel they are effectively closing their IT security gaps.[4]

[2] "Ransomware threat rises: Verizon 2022 Data Breach Investigations Report," Verizon, May 2022.

[3] "2022 Cybersecurity Almanac: 100 Facts, Figures, Predictions and Statistics," Cybercrime Magazine, January 2022.

[4] "The 2022 Study on Closing the IT Security Gaps: Global," Ponemon Institute study, sponsored by HPE, January 2022.

Closing security gaps

Augmenting your security landscape with trusted HPE personnel, powering your IT with proven HPE systems

Regardless of the depth or breadth of your security team, you most likely have gaps that need to be filled. By augmenting your security team with HPE personnel, you benefit from a team of experts armed with comprehensive knowledge and understanding of today's cybersecurity landscape—as well as digital transformation and data-first modernization. With HPE on your team, your people will be available to work on strategy or train other in-house personnel on security products and approaches.

While HPE personnel closes knowledge gaps within your team, HPE systems close security gaps in your IT by leveraging embedded security technologies such as the silicon root of trust and a secure supply chain that extends from manufacturing through initial boot at your data center or edge location.

Through automatic and continuous monitoring with HPE Integrated Lights-Out (HPE iLO), our systems can verify the integrity of the software and IT operating systems processing your data workloads from silicon to the cloud, wherever the data lives. HPE systems have designed-in security anchored in the silicon root of trust to help ensure your apps, workloads, and data are protected within a trusted hybrid operating environment.

It's never too early for security

Introducing security and how you can automate it in the early stages of your digital transformation project is critical to ensuring that the project follows secure-by-design principles. Early introduction can also identify security issues in the development lifecycle before they impact production and time to market.

HPE experts can help you construct security controls that add value to your organization's operations—rather than inhibit innovation and productivity. This way, security can become a highly effective business enabler across your organization.

Organizations that have taken measured steps to address cultural and goal alignment have made good progress toward improving their security confidence. These organizations are ultimately more effective at putting in place the people, process, and tool changes necessary to deliver modern security across their entire estate.

Becoming cyber resilient

A four-step plan to improve cyber resilience

Similar to many organizations, yours might have moved to a hybrid work model—if not remote—thanks to the fallout of the COVID-19 epidemic. Accompanying this mass migration of workers to remote locations was an epidemic of increasingly sophisticated ransomware attacks. The result: organizations operating in all industry sectors across the globe are thinking about cybersecurity differently and more comprehensively. A critical part of the new thinking is how to become more cyber resilient.

Cyber resilience is the capacity for your enterprise to maintain its core purpose and integrity in the face of cyberattacks. For enterprise security to be truly effective, information security, business continuity and disaster response (BC/DR), and organizational resilience must work together as a unified strategy, and with plans and programs in place, ready to handle any type of adversity.

In terms of dealing with a zero-day attack, HPE security experts can help you implement a four-step plan for improving your cyber resilience:

Anticipate—Perform holistic risk assessments across your entire organizational estate to understand where risk exists. This is a critical first step in becoming cyber resilient and being prepared to deal with any state of adversity.

Withstand—Ensure you have the right cybersecurity architecture in place so you can maintain business-critical functions / business continuity during a zero-day attack. A cyber resilient organization follows principles such as zero trust in segmenting the infrastructure and has a mature level of security hygiene to efficiently reduce the impact of a zero-day attack.

Recover—Have a DR strategy in place that highlights the steps you should follow to neutralize the impact of a zero-day attack.

Adapt—Learn from what happened and adapt architectural capabilities so you can better withstand future events, based on changes to either the operational environment or the threat landscape. Handled correctly, the adapt phase can be considered as ongoing threat modeling following the agile concept of continuous improvement.

Cyber resilience requires a team effort

Maintain your organization's core purpose and integrity when faced with cyberattacks

Cyber resilience key takeaways

1. Cyber resilience is like any other enterprise program—how you address it comes down to cost and priorities. Some organizations will take a high-risk and high-reward approach while others will run more conservatively.
2. Fool-proof security is an unattainable goal. There will always be a weak link somewhere for hackers to exploit.
3. Cyber resilience brings together information security, BC/DR, and organizational resilience to work toward a common goal.
4. A siloed approach to business protection was common in the past, but COVID-19 and ransomware have demonstrated the vulnerabilities of such an approach.
5. One of the great benefits of cyber resilience is that it helps organizations recognize that hackers have an advantage. Organizations now see security as a full-time job and embed security best practices in day-to-day operations.

Adopting a cybersecurity risk framework

Gaining the benefits of transformation while managing the associated risks

Building in security from the very beginning of any digital transformation and data-first modernization project is a critical step toward success. Part of the building-in process is to develop an overarching cyber risk framework that extends across your organization. Such a framework will provide a holistic approach to pulling together all the pieces of your security landscape.

Many frameworks are available, but HPE has found the NIST Cybersecurity Framework (NIST CSF) especially useful to help coordinate different focus areas, perform gap analyses, and identify and prioritize areas of improvement. HPE suggests the following best practices to help your organization effectively implement a robust cybersecurity risk management framework.

- Align all levels of your organization, beginning at the top—facilitate meaningful conversations among all stakeholders across your organization
- Build awareness to empower your employees to move from being a source of vulnerability to becoming the first line of defense
- Understand, assess, and prioritize your organization’s needs and desired outcomes
- Be agile, unconstrained, and innovative as you include security as an inherent part of your business strategy
- Adopt and adapt the NIST CSF to suit your organization
- Create a competitive advantage with a robust and pragmatic cybersecurity risk management program

HPE can get you started in the right direction by developing a NIST framework tailored to your unique organizational requirements. You can participate in a world-class program that covers cybersecurity awareness, cloud security, data protection, risk assessment, threat identification, and more.

HPE can help you answer critical questions about your security landscape:

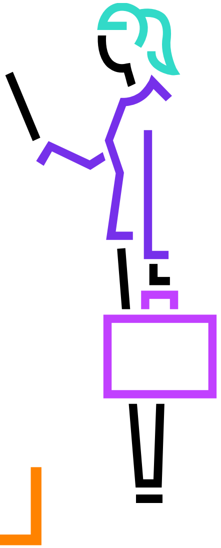
How do we **identify** what requires protection?

How and what do we **protect** to mitigate the risk?

How quickly can we **detect** that our protections have failed?

How quickly can we **respond** to limit or avoid damage?

How quickly can we fully **recover**?



Trusted assistance from planning to deployment and beyond

Reinforcing and enhancing (rather than replacing) your current security

With capabilities across the security spectrum, HPE offers a portfolio of Enterprise Security Services and Advisory and Professional Services designed to help you reach your security goals with confidence. HPE security capabilities reinforce and enhance (rather than replace) your current security framework. Together, we can integrate new processes into your existing security strategy—across your people, processes, and technology—to help minimize risk and maximize the effectiveness of the investments you already made.

Depending on your needs, you can work with HPE to assess your security vulnerabilities, plan for edge-to-cloud adoption of your new security strategy, help ensure platform security through a zero trust approach,[5] and understand how to become cyber resilient.[6]

And to ensure you can quickly recover from a security event if it were to occur, HPE can help you design your security strategy from edge to cloud.

- Initiated in the HPE secure supply chain and anchored in the silicon root of trust, the HPE GreenLake delivers integrity verification capabilities that automatically and continuously detect threats and unauthorized changes to your infrastructure, applications, and workloads.
- With HPE iLO, you can initiate hardened security features and securely configure, monitor, and update your servers anywhere in the world. Gain consistent insight into the health and operation of your servers with the latest innovations in simplified operations, performance, and security initiated in the supply chain and rooted in silicon.
- HPE GreenLake for Compute Ops Management helps to further eliminate complexity and improve confidence by addressing security risks with features that help you operate more efficiently. HPE GreenLake for Compute Ops Management simplifies and unifies operations across the server lifecycle, for the entire environment, no matter where your compute infrastructure lives.

HPE GreenLake offers a consumption-based business model that enables you to pay for what you deploy and allows you to grow to what you need. With extended deployment, you can acquire your forecasted compute and storage capacity in advance of the actual need and align payments with your usage—giving you flexibility and budget efficiency.

[5] The zero trust approach is based on never trusting by default, always verifying identities, and always assuming breach. Every identity is verified before being allowed into the IT environment. In short, every identity is assumed bad until proven good.

[6] Cyber resilience refers to an entity's ability to continuously deliver the intended outcome, despite cyberattacks.

Ready to get security confident?

Preventing and overcoming cyber threats

Generally, no one is ever 100 percent confident about data security. However, you can build confidence in your security when you take a security-first approach to your digital transformation. When security is aligned to business objectives it is possible to transform security to an enabler of business risk to enable innovation and growth. With HPE's proven approaches you can start alleviating the risks and improve your cyber resilience. HPE can help you:

Build a resilient security landscape designed to scale right along with your transformation projects

Set security expectations based on skills and knowledge gaps within your organization, and then work with HPE to fill them

Create a balance between operational risk and security across your enterprise

Partner with HPE to get security confident

Visit **HPE GreenLake**

Cyber threats are becoming increasingly sophisticated as attack surfaces continue to expand to include a proliferation of interconnected platforms, services, and systems that widen security gaps. With proven approaches from HPE, you can alleviate security doubts and move your organization to a place of security confidence.

Learn more at

Learn how HPE can help you:

- Configure, monitor, and update your servers from anywhere in the world with HPE iLO
- Automatically and continuously detect threats and unauthorized changes to your infrastructure, apps, and workloads with the HPE GreenLake platform
- Simplify and unify operations across the server lifecycle with HPE GreenLake for Compute Ops Management

**Make the right purchase decision.
Contact our presales specialists.**

Chat now (sales)

Call now

Get updates

Hewlett Packard
Enterprise

a50007337ENW