HPE GreenLake

Scale security and cyber resilience at the speed of transformation

Get security confident

Table of contents

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. Today, every organization feels at risk. With proven approaches from Hewlett Packard Enterprise, you can alleviate security doubts and move your organization to a place of security confidence. Together with HPE, you can balance operational risk with an edge-to-cloud security strategy—enabling you to continue to innovate and grow, even when facing the ever-present danger of cyberattacks.

Keeping security in lockstep with business transformation

Traditional security technologies were deployed to protect the data center and the network. Today, however, distributed enterprises operate in a hybrid world that includes private and public clouds and edge locations that must also be secured, in addition to the on-premises data center and the network.

As today's enterprises move more workloads to the cloud, they need enhanced visibility and monitoring capabilities to ensure data remains protected while in transit (from the data center to cloud and back), in use, and at rest. Adding to the mix is the push toward computing at the edge, where physical security may not be as robust as in the data center and data is literally everywhere—including manufacturing plants, retail stores, healthcare clinics, and branch offices.

With digital transformation continuing at a very rapid pace, security must keep pace to ensure the protection of any data, anywhere. HPE can help you build security into all your data-driven modernization initiatives—offering solutions and services designed to scale at the speed of your business to deliver on transformation objectives.

Security controls: Leave the 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."

– Sean Foley, Edge-to-Cloud Transformation Strategist, HPE[1]

[1] Security: The foundation for transformation success, Sean Foley, enterprise.nxt, May 2022

Digital transformation in action—retail[5]

For more than 10 years, online shopping has been a staple for many retail organizations. Today, retailers digitally transform by moving to an omnichannel strategy—enabling them to achieve more availability, drive sales and traffic, and integrate digital touchpoints.

An omnichannel retail strategy improves the customer experience and provides more channels for customer purchases—whether on a mobile device, via the web, or in a store. The availability of multiple purchasing channels leads to an increase in sales and traffic. In fact, omnichannel shoppers spend 15–30% more than single or multi-channel customers. By leveraging multiple channels, omnichannel retail not only increases revenue from online retail but also drives significant traffic to stores, further increasing revenue.

With this significant increase in digital sales activity, cybersecurity has become a top-of-mind concern for retailers adopting an omnichannel approach.

Security and data-first modernization go hand in hand

With the rate of cyberattacks at an all-time high, protecting your data, people, processes, and technologies requires constant vigilance. In 2022, ransomware breaches alone jumped by 13% year over year[2]—a greater increase than the past five years combined—and cybercrime damages are expected to cost the world economy $10.5 trillion annually by 2025.[3] Yet only 30% of businesses today feel that they are effective in closing their IT security gaps.[4]

These alarming cybersecurity statistics combined with the complexity of digital transformation and data-first modernization can create an overwhelming lack of security confidence.

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.

Taking a data-first approach to your digital transformation means that many more IT goals and priorities become aligned, due to the commonality of the data agenda applying to each. These priorities include:

- Simplifying data management and protection
- Securing your data across edge to cloud
- Achieving a cloud experience everywhere
- Creating a connected experience at the edge
- Embracing artificial intelligence (AI) and analytics at scale
- Harnessing the power of supercomputing

Closing security gaps

Regardless of the depth or breadth of your security team, most organizations 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. Through automatic and continuous monitoring, 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. All HPE systems have "designed-in" security to help ensure your apps, workloads, and data are protected within a trusted hybrid operating environment.

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

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

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

[5] "Why Businesses Must Embrace Omnichannel Retail," MuleSoft

Addressing cultural factors and risk objectives[6]

Some organizations are slow to adopt new practices to upgrade their security infrastructures due to culture and business objectives. A wall often exists between a security organization and the rest of the IT organization—creating tension and inhibiting communication and collaboration. In addition, many security organizations are resistant to change, even though the need to transform is often most acute in security organizations.

As for objectives, companies often fail to balance their business objectives with their risk objectives. Leaders need to encourage a holistic assessment of objectives for revenue, business development, and risk so that they can find a balanced approach to help the business move forward quickly, profitably, and securely.

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.

[6] "Security: The foundation for transformation success," Sean Foley, enterprise.nxt, May 2022

It's never too early for security

Introducing security in the early stages of a 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. When security controls are constructed to add value to your organization's operations—rather than inhibit innovation and productivity—security can become a highly effective business enabler. Automation is also a key consideration for IT and security teams embarking on digital transformation initiatives, and the earlier that it is built into digital transformation plan the better. The growing sophistication and frequency of cyberattacks is driving a growing need for enterprises to continually evaluate how to both embed security in their architecture and then automate its use and application. Automation will continue to become increasingly more important to ensure security and IT teams can build cyber resilience and keep up with the volume and complexity of attacks and risks targeting the business.

Becoming cyber resilient

As the COVID-19 epidemic compelled entire workforces to move from their corporate offices to remote locations, an epidemic of increasingly sophisticated ransomware attacks surfaced—forcing enterprises to think about cybersecurity in a different and more comprehensive way. This transformation highlights the importance of building a cyber resilient enterprise.

Cyber resilience is the ability of an enterprise to maintain its core purpose and integrity in the face of cyberattacks. Cyber resilience brings together the formerly separate (siloed) disciplines of information security, business continuity and disaster response (BC/DR), and organizational resilience to work toward common goals. The primary difference between traditional BC/DR and cyber resilience is that, where BC/DR focuses on recoverability, cyber resilience focuses more on sustainability.

For enterprise security to be truly effective, these disciplines must work together to align their strategies, tactics, and planning to handle any type of adversity. When these teams collaborate, they can create a whole greater than the sum of their individual parts.

In terms of dealing with a zero-day attack, the following four-step plan can help improve cyber resilience:

1. **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.
2. **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.
3. **Recover**—Have a DR strategy in place that highlights the steps you should follow to neutralize the impact of a zero-day attack.
4. **Adapt**—Learn from what happened and adapt architectural capabilities so you can better withstand future events, based upon 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 key takeaways

- 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.
- Foolproof security is an unattainable goal. There will always be a weak link somewhere for hackers to exploit.
- Cyber resilience brings together information security, business continuity and disaster response, and organizational resilience to work toward a common goal.
- A siloed approach to business protection was common in the past, but COVID-19 and ransomware have demonstrated the vulnerabilities of such an approach.
- 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.

According to former U.S. Defense Secretary Donald Rumsfeld, there are three types of threats.

1. "Known known"—a threat of which you are fully aware
2. "Known unknown"—means you know something is going to happen but are unsure of what it could be
3. "Unknown unknown"—where you have no idea what is going to happen, how it will happen, or when

Dealing with unknown-unknown threats moves out of the realm of traditional cybersecurity and into the new paradigm of cyber resilience—where you have a model that keeps your end-to-end enterprise up and running (sustainable) from edge to core during an unknown-unknown attack.

Becoming cyber resilient begins with a self-examination of everything that goes into what your organization does or that can be disrupted—including power, cooling, equipment, people, highways, buildings, and environmental factors—and its ability to prevent loss of function and data compromise. You need to stress test everything and logically follow the sequence of events that might follow.

Follow-on tasks include transforming security controls that no longer work effectively; managing the cost of planning to recover from worst-case to best-case scenarios; handling data sovereignty issues posed by national or other geographical boundaries; and overcoming legal and regulatory barriers, particularly over data residency concerns, because even in an emergency, data might have to stay within a geographic region.

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 (CSF) is especially useful to help coordinate different focus areas, perform gap analyses, and identify and prioritize areas of improvement. The following best practices will help your organization effectively implement a robust cybersecurity risk management framework.

Benefits of adopting the NIST Cybersecurity Framework (CSF)

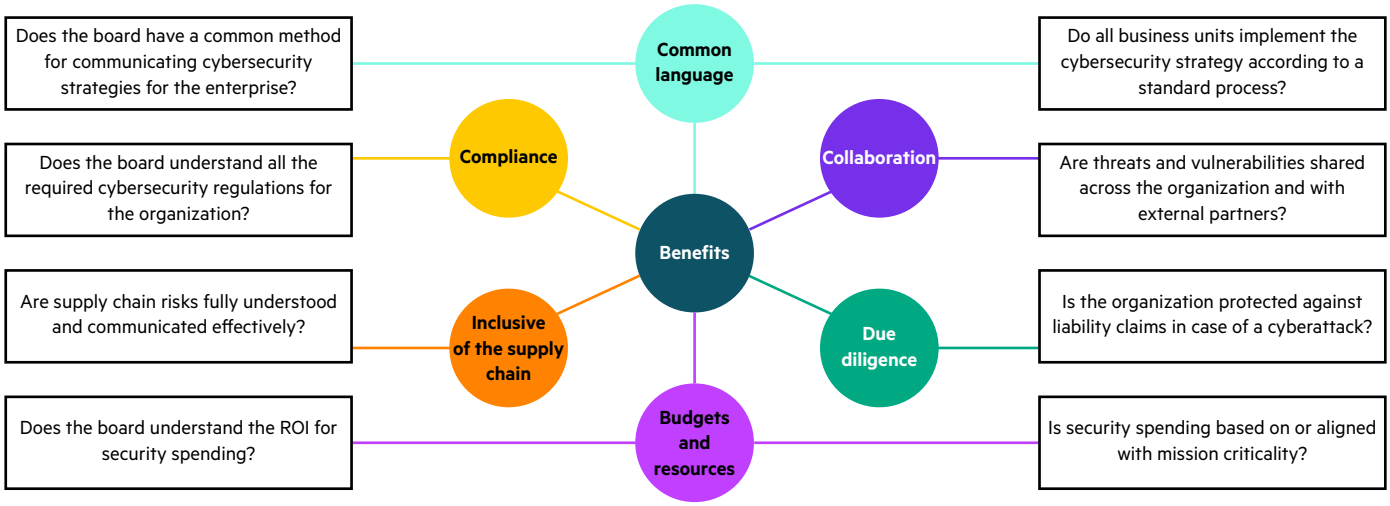

Figure 1. The benefits of adopting the NIST Cybersecurity Framework (NIST CSF)

Align all levels of your organization, beginning at the top

The primary objective of adopting a model such as the NIST CSF should be to facilitate meaningful conversations among all stakeholders across your organization—including the board of directors, executive leadership, and senior management, as well as the line of business teams and other stakeholders with a vested interest. Doing so ensures that the appropriate levels of visibility and awareness are consulted as your organization makes informed decisions about cyber risk investments and commitments.

Use the NIST CSF core functions

The NIST CSF acts as a comprehensive set of steps your organization can take to ensure that cyber risk is assessed. The framework uses functional and straightforward best practices, explained with easy-to-interpret business language, to outline the core functions of your organization's unique cybersecurity risk management framework.

Core functions address the following:

- 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**?

Using these core functions, you can facilitate discussions about different sets of cyber risk controls, better understand your organization's cyber risk profile, ensure that you have a sufficient balance of controls, and gain greater security confidence.

Build awareness

A robust playbook of responses or policies to address the most likely types of cyber incidents, including remedial actions, is required. A good precursor or parallel activity is to implement an effective awareness program. By improving security awareness, employees are empowered to move from being a source of vulnerability to becoming the first line of defense. A security aware workforce can become an asset and is an essential building block of your cyber defense.

Understand, assess, and prioritize

The first step for your cybersecurity team is to understand your organization's needs and desired outcomes. Then, the team must assess various risks and consider the controls needed to mitigate those risks, while at the same time evaluating the impact of the controls on your organization's ability to achieve desired outcomes. Finally, the team needs to define a program of improvements that prioritizes actions identified as most important to your organization, such as protecting revenue streams or reducing the risk to growth initiatives.

Be agile, unconstrained, and innovative

Because cybercrime is a constantly moving target, your organization must not look upon cybersecurity as a one-time project with one-time funding. You need to include security as an inherent part of your business strategy.

Adopt and adapt

Adopting and adapting the framework to suit your organization are keys to your success. Keep in mind that a framework is a guidance—not a law. Best practices such as the NIST CSF are proven to work for many organizations, but you will need to continuously scrutinize and review the framework/process to decide what works best for your organization both now and in the future.

Create competitive advantage

A robust and pragmatic cybersecurity risk management program creates an opportunity to gain a competitive advantage, as well as boost security confidence. For example, an organization that has, or is part of, a supply chain that decides to adopt the Cybersecurity Supply Chain Risk Management (C-SCRM) security controls can be independently audited using the Cybersecurity Maturity Model Certification (CMMC). This certification provides a level of comfort to customers and fellow suppliers, generating a competitive edge and, ultimately, more business.

HPE can get you started in the right direction by helping develop 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.

Trusted assistance from planning to deployment and beyond

Offering capabilities across the security spectrum, HPE offers a portfolio of Enterprise Security and Digital Protection 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,[7] and understand how to become cyber resilient.[8]

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

The HPE GreenLake edge-to-cloud platform delivers integrity verification capabilities that automatically and continuously detect threats and unauthorized changes to your infrastructure, applications, and workloads. Initiated in the HPE secure supply chain and anchored in the silicon root of trust from HPE, the integrity verification capabilities cryptographically measure the HPE GreenLake operating environment. It also includes the compute infrastructure, 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. These capabilities provide robust capabilities to help you to implement NIST CSF controls and identify, protect, detect, respond, and recover from attacks.

From silicon to the cloud, HPE can help your organization build resiliency. With HPE iLO, you can initiate hardened security features and securely configure, monitor, and update your compute infrastructure from anywhere in the world—helping you gain consistent insights into the health and operation of your servers. HPE iLO provides the latest security and remote management capabilities to simplify operations and improve performance with security capabilities that are initiated in the supply chain and rooted in the 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. Complex server management unnecessarily consumes valuable IT resources and slows innovation. HPE GreenLake for Compute Ops Management solves these challenges by simplifying and unifying operations across the server lifecycle, for the entire environment, no matter where your compute infrastructure lives. The service provides a consistent, secure cloud experience that scales elastically and unifies compute management to help you securely monitor and control your distributed compute lifecycle tasks using a cloud-native architecture.

Regardless of your final security solution, you can rest assured that any system you choose will include hardened security features that enable you to securely configure, monitor, and update your servers from anywhere in the world. You benefit from 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 the silicon.

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

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

In addition, HPE 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.

Ready to get security confident?

Generally, today, no one is confident about data security. Everyone is afraid of cyber threats and they make every organization feel at risk. Thankfully, there are proven approaches to alleviating that insecurity and moving your organization to a place of security confidence.

First, as your enterprise grows, you need a resilient security landscape that can scale right along with your transformation projects. To meet this goal, you need a comprehensive strategy for identifying threats, protecting against them, detecting them, knowing where and how they are going to attack, and remaining ready to resolve them.

Second, you need to set security expectations based on skills and knowledge gaps within your organization, and then be open to filling those gaps with outsourced personnel well-versed in security and digital transformation. These experts can help you navigate the complexity of today's security landscape to ensure you can reach a state of resilience.

You need to create a balance between operational risk across your enterprise so that security doesn't become the land of "no." Instead, security can become the land of "yes" when you receive expert guidance to manage your operational risk as you scale your digital transformation projects.

Your organization can overcome the fear of cyber threat and reach the goal of security confidence by working with HPE to design a tailored security strategy from edge to cloud, fill your skills and knowledge gaps, and suggest systems and solutions to manage your operational risk.

Connect with your HPE representative today to learn more about getting security confident. Discover how your organization can configure, monitor, and update your servers from anywhere in the world with HPE iLO.

Learn more at

HPE Integrated Lights-Out (HPE iLO)

Visit **HPE GreenLake**

Make the right purchase decision.
Contact our presales specialists.

Chat now (sales)

Call now

Get updates

Hewlett Packard Enterprise

a50007253ENW