Transforming to hybrid cloud? It's time to prioritize security.

Hybrid cloud introduces new challenges and exposes organizations to new threats. Learn six essential steps to help you thrive in this environment.

HPE GreenLake

In just a few years, hybrid cloud has become the dominant operating model for IT architecture. Recent Hewlett Packard Enterprise research found that more than 90% of large enterprises host their workloads in some mix of private and public clouds and on-premises data centers.[1]

Yet securing those workloads has become more challenging than ever. In a new study by Ponemon Institute, sponsored by HPE, only 44% of enterprises said they were confident they could secure their systems in today's constantly evolving threat environment, down from 52% a year earlier. Further, 63% of organizations said they are unable to track the activity of every user and device connected to their infrastructure, and 37% struggle to verify the security of their apps and workloads.[2]

One reason for this shift is the growing volume and sophistication of cybersecurity threats. The number of incidents in 2022 increased by just under 40%, with an average of nearly 1200 attacks occurring per organization each week.[3]

This growth in attacks has been accompanied by a change in attackers' tactics. Fewer than a third of all incidents of compromise last year were due to malware, as attackers have shifted their focus to compromising identities to gain access to sensitive systems and data. Exploits targeting cloud workloads increased 95% last year, and the number of "cloud conscious" adversaries nearly tripled.[4]

Another reason for the IT security gap is the increased complexity of hybrid cloud environments, notes Jan De Clercq, a distinguished technologist at HPE. De Clercq says today's IT departments are being asked to manage a complex environment involving multiple vendors using different cloud platforms. Additionally, they are operated by different people with different skill sets, located in different geographies using different terminology. As such, more than 40% of enterprises surveyed by Ponemon said their biggest technology challenges are securing workloads moving from the edge to the cloud or moving between on-premises and public cloud environments.

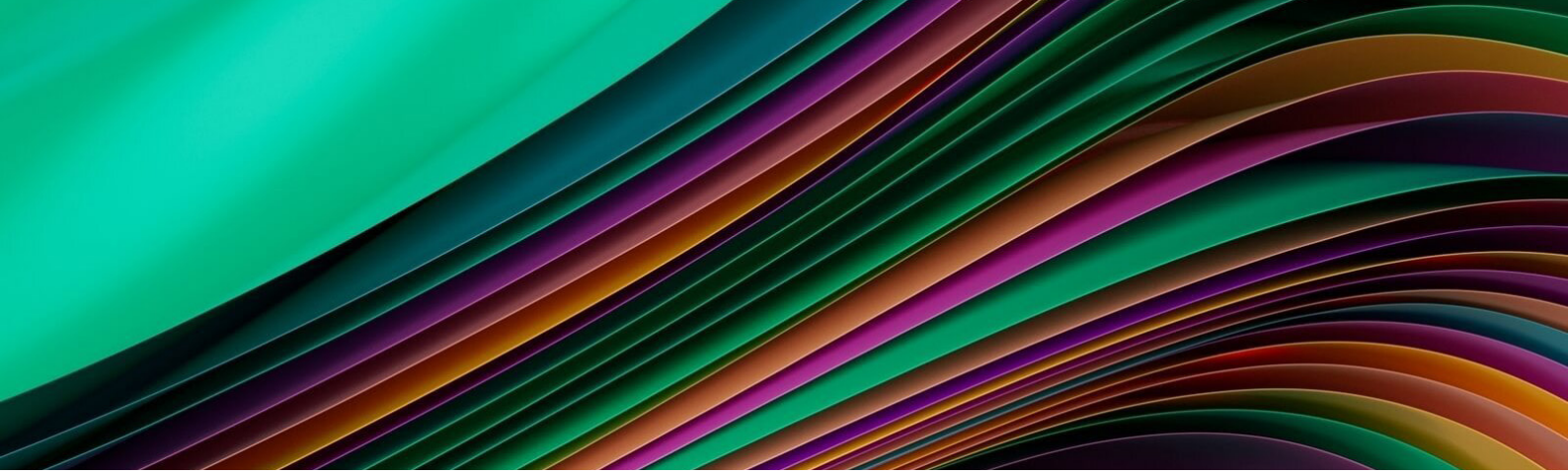
"The real challenge for security practitioners is, 'How can I uniformly and cost effectively protect my apps and data given that I've got different tooling at each cloud vendor and on-premises?'" notes Tim Ferrell, also a distinguished technologist at HPE. "How do I ensure that I have line-of-sight visibility into each of those areas? How do I manage risk in a uniform and cost-effective way? That's the holy grail everyone's trying to get to." Adds De Clercq, "Most importantly, how do I align my on-prem controls with the ones in the public cloud?"

[1] "From hybrid cloud by accident to hybrid cloud by design," Hewlett Packard Enterprise, May 2023

[2] "The 2023 Global Study on Closing the IT Security Gap: Addressing Cybersecurity Gaps from Edge to Cloud," Ponemon Institute, March 2023

[3] "Check Point Research Reports a 38% Increase in 2022 Global Cyberattacks," Check Point Software Technologies Ltd., January 5, 2023

[4] "2023 Global Threat Report," CrowdStrike, February 2023



To tackle this challenge, enterprises need to update their controls, governance, and skill sets. Most important, they need to make security, for both on-premises systems and those in the cloud, a key priority moving forward.

Here are six essential steps you can take to transform your security function from a barrier to an accelerator of innovation.

1 Be proactive, not reactive

The key to developing an effective security strategy is to be proactive, not reactive. Leading companies don't just buy a set of tools and wait for incidents to happen. Instead, they put the right processes in place, train their personnel on how to use them, and continuously update them as new threats arise.

"Most of the big breaches we've seen were not failures of technology," says Ferrell. "They were human or process failures."

2 Break down information silos

In many companies, responsibility for security is left to individual teams on a project-by-project basis. Or it's the sole province of the cybersecurity team but with little communication with the business units responsible for applications, networking, infrastructure, and so on, notes De Clercq. In the Ponemon study, 40% of enterprises cited turf and silo issues as the greatest challenge to achieving a secure hybrid cloud environment — higher than any other barrier.

"When you want to create a set of coherent security controls that link together well, you need to make sure people talk to each other and everyone knows what everyone else is doing," says De Clercq. "And that includes communication between technical people and the C-suite."

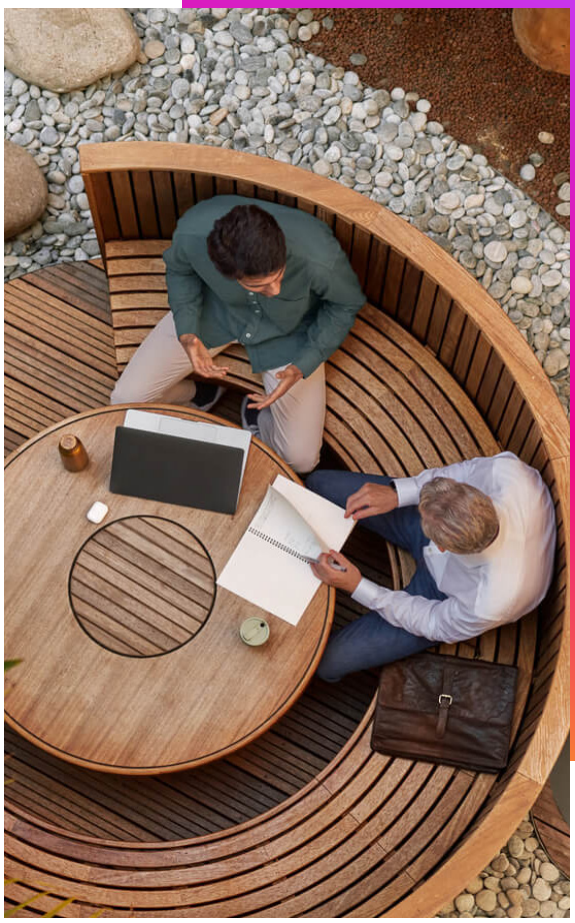
3 Prioritize security from the start

In many enterprises, security is often seen as a barrier to innovation, an impediment to the speed of agile teams. But security is the one thing you don't want to break. And it's not something you can easily bolt onto a project after it's nearly complete. Security controls that might have taken a few hours to implement at the beginning of a project can take weeks to add in at the end, which can be very disruptive, says Ferrell.

Yet, 25% of enterprises surveyed said security is not considered early enough in project plans. Trying to plumb in security after a project is nearly complete becomes much more difficult and more expensive, agrees De Clercq. "And even then, you end up creating holes."

At the same time, security professionals need to work closely with project developers to minimize disruption as an app or service is being developed and embrace flexibility in how they manage risk as the project moves forward, De Clercq notes. Collaborating early and often is the key to enabling innovation while minimizing vulnerabilities.

4 Automate processes and tools to reduce the potential for human error



In the Ponemon study, organizations that ranked themselves as top performers in cybersecurity had several characteristics in common. For one, they are more likely to have adopted a zero trust security model for managing access for users and devices. And roughly half have deployed or plan to deploy secure access service edge (SASE) or network access control (NAC) solutions for continuous monitoring of network traffic to identify and stop malicious Internet of Things (IoT) activity.

They also devote more resources to security staffing and are more likely to centralize architecture decisions within the security or networking teams. In addition, many have adopted tools that automate the verification of infrastructure integrity.

"A lot of the controls organizations have in place today are still acting in a purely reactive mode," says De Clercq. "What's needed are proactive tools that automatically close down gates based on the behavior they are seeing in the environment. By relying more on automation and machine intelligence, we can get rid of some of the human error and make security more proactive."

5 Choose the right security framework

The most common way to assess the robustness of an organization's cyber-posture is by measuring it against an existing security framework. Adopting an accepted guideline also helps to ensure compliance, since many regulatory requirements are subsets of the most common security frameworks. In the Ponemon study, implementing a cybersecurity framework ranked as the top priority for minimizing risk, along with modernizing IT security processes.

"Essentially, a security controls framework is a list of the key security controls that should be in place in any modern cybersecurity enterprise," says Ferrell. "Some are mandated by law, some by industry, and some are voluntary. But, if you follow the appropriate security standards or frameworks for your enterprise, you will likely meet most compliance requirements."

Some of the most common frameworks include:

- **ISO 27001:** Created by the International Organization for Standardization, ISO 27001 is similar to System and Organization Controls 2 (SOC 2) in that it requires proof that you've implemented security controls to protect customer data. But compliance is typically more challenging and time consuming, and it requires organizations to have an information security management system in place to manage and update cybersecurity operations on an ongoing basis.
- **SOC 2:** Created by the American Institute of CPAs, SOC 2 is a voluntary compliance standard for how service organizations should handle customer data. Its five key principles are security, availability, processing integrity, confidentiality, and privacy. SOC 2's requirements are considered slightly easier to meet for smaller organizations with less mature security operations.
- **NIST 800-53:** A series of security and privacy controls for federal information systems created by the National Institute of Standards and Technology (NIST), NIST 800-53 covers 20 areas, including access control, audit and accountability, risk assessment, incident response, business continuity, and disaster recovery. With few exceptions, U.S. agencies and contractors that work with them are typically required to meet these standards.

- **FedRAMP:** The Federal Risk and Authorization Management Program (FedRAMP) relies on NIST 800-53 guidelines as applied to the use of cloud services. Cloud service providers are evaluated on a three-point impact scale: low, moderate, and high. The higher the impact rating, the more baseline controls a communications service provider (CSP) must provide to meet federal agency standards.
- **Cloud Controls Matrix:** Created by the Cloud Security Alliance, the Cloud Controls Matrix (CCM) is composed of nearly 200 controls across every domain of cloud technology, including audits and applications, identity and access management, and threats and vulnerabilities.
- **EU Cybersecurity Act:** This is a security framework and certification program for electronic communications networks operating in the European Union (EU), created by the EU Agency for Cybersecurity (formerly the European Network and Information Security Agency [ENISA]). The act includes sanctions for organizations that fail to impose appropriate controls for detecting and responding to cyberattacks.

Choosing a common framework allows organizations to evaluate their cybersecurity defenses in a uniform and predictable way. "We try to go standards based whenever possible," says Ferrell. "We never want to be caught with our pants down when customers say, 'Well, how did you come up with that?' It helps to point to an authoritative source."

6 Conduct a thorough risk assessment

All IT projects involve some level of risk. And the level of risk that is deemed acceptable will vary from organization to organization, project to project, and even between different departments within a single enterprise. Every project needs to start by identifying risks, assessing how serious a threat they pose to the organization, and presenting that information to top leadership so they can determine their appetite for those risks.

Conducting a risk assessment involves a few key best practices.

- **Involve as many stakeholders as possible**

  Organizations need to include all relevant stakeholders to surface any potential threats and vulnerabilities that could expose corporate assets and data. Ideally, risk assessments should include the project developers; the owners of the data, network, and infrastructure involved; security practitioners; and project owners.

  "When you're building a new application, you need to involve the lead architect, because they will often have unique views on how a solution works and certain risks that can occur," says De Clercq. "That's something a C-suite person would never know."

- **Put it in terms executives can understand**

  Business leaders aren't being paid to understand security protocols or go deep on threat assessment and mitigation. Their job is to enable the business to grow and thrive. Security practitioners need to measure the practical impact on future revenue, reputational damage, and digital trust, says Ferrell.

  He adds, "One of the things your decision-makers will ask is, 'What would be the cost of preventing this versus the cost of remediating it if it happened?' One of the factors will be how much cyber-insurance the organization has. The problem is that insurance can't prevent downtime or restore your company's reputation."

- **Address the most critical threats first**

  It's tempting after a risk assessment to go after the low-hanging fruit and collect some quick wins, notes Ferrell. But a smarter approach is to identify the threats that are most critical to the continued operations of the company and address those first, even if they require additional resources. "If I were a chief information security officer (CISO) and my risk assessment turned up a couple of things that would be crippling for the company, that's what I would go after," he says. "That's the stuff you fight for."

- **Accept that the risk decision may be out of your hands**

  At the end of the day, the final determination of what risks are acceptable lies with top management. Once security practitioners make their case, it's up to business leaders to determine their appetite for risk. "Someone in leadership who owns the project needs to say, 'I accept this risk' or 'I accept this risk but only under the following conditions,'" says Ferrell. "This is where risk assessment gets tricky: you can enumerate the risks and rate them, but figuring out the treatment of those risks is a whole different game that has to involve executive input and support."

The need for cyber-agility

The threat landscape is evolving rapidly, and that rate of change is likely to accelerate over time. A security posture that is more than sufficient to protect against today's major risks may be woefully inadequate to protect against new threats that emerge over the next few years, especially as attackers adopt many of the same artificial intelligence (AI) tactics and tools used to defend corporate assets.

"Organizations need to focus more on cybersecurity agility," says De Clercq. "They need to make their security controls more flexible and agile to cope with the changes that are happening all the time. One way they can do that is by increasing their use of automation and infrastructure as code and calling more on the AI that is incorporated in security controls."