Edge-to-cloud security: closing the gap

Although there's no such thing as 100% security, top performing teams have improved cybersecurity by addressing three critical factors.

CIO

SPONSORED BY

Hewlett Packard Enterprise

Organizations are more security conscious than ever. And yet security remains a huge challenge. Despite ongoing training efforts and technology upgrades, organizations often struggle to keep up with the constantly changing threat landscape. This creates a gap between security threats and the ability to identify, detect, and resolve security incidents.

If this sounds familiar, you're not alone. In fact, in the 2023 Global Study on Closing the IT Security Gap by the Ponemon Institute, sponsored by HPE, only 44% of survey respondents rated their organizations' efforts to close the gap as very or highly effective. That said, there are tactics that can help.

4 issues that are widening the security gap

Closing the security gap doesn't happen overnight. It's a journey that involves overcoming challenges that many organizations face: the threat landscape, talent shortages, compliance issues, and hybrid cloud complexity.

1. **The expanded threat landscape:** The IT environment now extends from on premises to public cloud and from hybrid cloud to edge. "Cybercriminals are getting more clever in terms of the methodologies they're using," said Simon Leech, deputy director, Center of Excellence, Cybersecurity and Digital Risk Management at HPE. "Also, they are using sophisticated tools to launch very efficient and effective attack campaigns against organizations."
2. **Security skills gap:** It's difficult to keep pace with cybercriminals, especially considering the security skills gap. "This talent shortage is not expected to go away quickly, so organizations need to look at new ways to hire, train, retain, and augment staff," Leech said.
3. **Increased regulatory and compliance pressures:** The regulatory environment is becoming more complex as global businesses grow and countries institute new compliance legislation. "We think organizations are doing a better job at aligning their activities and technologies with regulatory issues," said Larry Ponemon, chairman and founder of the Ponemon Institute. "However, we still see problems such as compliance issues that are not fixed in an effective way."
4. **Hybrid cloud complexity:** IT infrastructure is now increasingly distributed across hybrid cloud and edge environments. "Not every workload is built equally," according to Leech. "So, due to reasons like data gravity and data sovereignty, there will be certain workloads that cannot go into a public cloud. This causes challenges as organizations try to implement security controls that cover the entire hybrid cloud."

3 factors that help close the security gap

Although there's no such thing as 100% security, it's possible to improve effectiveness around cybersecurity. Early in 2023, Ponemon Institute surveyed 2,084 IT and IT security practitioners to learn about the security gap in their organizations and to discover what measures they are taking to close that gap. Here are three tactics that top-performing security teams deploy:

1. **Centralized security decisions:** There should be agreement across the organization about investments in security solutions and architectures. According to the Ponemon report, IT and IT security teams that work together to assess and prioritize activities can more effectively close the IT security gap.

2. **Zero trust:** For organizations with hybrid cloud environments, it's especially important to consider using a zero trust architecture and working with a partner that follows zero trust principles. "You need to be thinking further than network access," Leech said. "Zero trust has to exist throughout your infrastructure and network, but also at the application, data, and user levels."

3. **Risk assessment:** A risk analysis can teach you a great deal about your organization. A thorough analysis should include understanding your most critical business processes, as well as workloads that should/can be moved to hybrid cloud and how those moves affect the organization's overall risk profile. "Once you've done the risk analysis," Leech pointed out, "you'll have a better picture as where to focus your resources."

Noting that a single weak link can affect the entire digital supply chain, Leech advocates a shared responsibility model for security, in which you work with partners that are committed to transparency and a secure edge-to-cloud experience. "It's important to understand which functionalities the security partner provides and which capabilities your organization will be expected to provide."

A proven security framework is also key to building a more secure infrastructure, he added. "Whether you follow the NIST Cybersecurity Framework or ISO 27001, identify one as your North Star, and allow it to guide you."

A good partner can harden and protect your infrastructure

There's no need to try closing your organization's security gap on your own. A partner like HPE can share expertise, resources, and solutions that align with your objectives and provide effective protection.

HPE GreenLake can help your organization address compliance issues, the expanded threat landscape, hybrid cloud complexity, security skills gaps, and more. The as-a-service platform enables organizations to use and pay for only the infrastructure and cloud services needed today, with the flexibility to easily scale tomorrow.

A shared responsibility model lets you retain ownership of all your data for full governance, while HPE hardens and protects the managed infrastructure — from silicon to software — based on zero trust practices and technologies.

In addition, organizations can reduce complexity with the simplified management capabilities integrated into HPE GreenLake. The platform unifies IT environments for a centralized, integrated experience with an intuitive user interface. Everything you need is there, for example, to add users, unify data across hybrid cloud, and enhance security for remote workers.

And if your organization is struggling to address skillset gaps, HPE Managed Services can serve as an extension of your existing IT department, taking care of routine patches, upgrades, customer support, and more.

Get more effective protection

It may seem daunting to address what feels like an ever-widening security gap. However, top performing security teams have shown that it's possible to gain holistic, end-to-end security from edge to cloud with the right tactics and the right partner.

Learn more about closing the security gap by visiting: hpe.com/security.