HPE GreenLake

When it comes to protecting your data, how do you adapt to today's shifting threat landscape?

Security experts share their advice on how to better protect your data by building smarter and faster defenses across your hybrid cloud.

Complex IT environments have become the new normal for many organizations. While the mix of public cloud services, private clouds, and on-premises infrastructure brings a host of well-documented benefits, the hybrid cloud model can also introduce cybersecurity challenges to teams unfamiliar with the ins and outs of hybrid operations. According to a recent Ponemon Institute study, 37% of organizations cited an inability to verify the security of all apps and workloads as the biggest challenge to achieving a stronger security posture, followed by the aging of legacy security controls (33%), and siloed or point security solutions (32%).[1]

How does your organization best adapt to manage these challenges? We spoke to three security experts at Hewlett Packard Enterprise — John Spiegel, director of strategy and field CTO for HPE Aruba Networking; Paul Lloyd, HPE's internal security strategist; and Kevin Cole, director of product and technical marketing for HPE Data Protection portfolio — to get their advice on how to better protect your data across your hybrid cloud.

[1] "The 2023 Global Study on Closing the IT Security Gap," Ponemon Institute, sponsored by HPE, March 2023

How do you adapt to shifting threat landscapes?

John: I think one of the most important things is the verification aspect of zero trust, that nothing on the network should be trusted without authorization. But if your verification service has been tampered with, that kills your zero trust environment. You want to continuously monitor your security services so you can understand if they have been tampered with or if additional access has been provided without your knowledge. And automating protection of these critical assets is a key component of being successful in terms of zero trust.

You also must have a way to include information about emerging threats in your solution. If your solution is static, if it's only evaluating your applications but not the evolving threat landscape, that's another area that opens you up to risk.

Paul: I'd add that having a formal, documented baseline understanding of your security situation is crucial. Baselines are an ideal way to realize the value of standardization, which is having a known, default posture everywhere it's expected. But one size probably won't fit everything. For some assets or devices, the baseline may need to be raised over time. You want a dial to adjust your baseline posture for each asset based on its value, so you can make your controls stronger or add another layer to your multifaceted defense-in-depth model.

How do you use AI and machine learning to disrupt attacks and foster data- and asset-centric protection approaches?

Kevin: Where we see AI and machine learning helping us the most in the data protection space is in threat detection and assessment, where you're being attacked, what's being impacted, and how fast it's spreading. Organizations have a skills shortage in cybersecurity and limited bandwidth. How do you quickly and accurately weed through and make sense of the massive quantities of data points that are streaming in? AI and machine learning are going to play a crucial role in detecting and mitigating threats, and that will transform how we address cyber risks.

John: I agree with what Kevin said about the lack of security resources, and how AI and machine learning could assist with that. I also think it's worth investigating training AI systems to be used as a virtual cybersecurity mentor or to provide an additional perspective in monitoring or incident handling. A security analyst could ask the virtual mentor questions like, "What's the current state of my business? Are there indicators of compromise? Are there areas I need to prioritize versus others?" It's extremely hard for a human to know when you might have a change that creates a compromise and how to solve that. If AI can allow you to understand where an attack is coming from, you'll have a better idea of which team and resources to engage. It would help simplify what we deal with daily and allow us to better target where we need to spend our time.

What's the best way to safeguard AI workloads?

Paul: For all the wow factors of AI, you must recognize that these systems are just code running on infrastructure. Start with architecture and look for the kind of patterns that facilitate good cybersecurity with respect to your attack surface. For example, traditional layers and tiers like user interface, database, orchestration, and so on have natural counterparts in new, sophisticated AI applications.

Kevin: Paul is correct that these things run on a variety of different infrastructure, and you need to understand that one size does not fit all. Distinct types of AI have diverse needs, so tailoring your approach is critical. You also need to understand each workload more specifically because an AI workload could refer to many things. It could be generative AI, natural language processing, or a more traditional type of AI. You need to understand exactly what you have and what you want to achieve, and then take an outcome-based approach to determine what you need to protect.

What's the best way to leverage cybersecurity frameworks, such as National Institute of Standards and Technology (NIST)?

John: First, we need to recognize frameworks such as NIST are only a starting point for large organizations. They provide value by distilling the cybersecurity profession's collective experience, wisdom, and lessons learned the hard way. But you can't just rely on the standard — you still must leverage your own experience and wisdom. A framework such as NIST can be a great tool for identifying and prioritizing the tasks you need to perform to achieve a desired posture, but you must avoid turning frameworks into project management tools. That's not their purpose.

Kevin: I think there's value in the NIST framework. What we see over and over is folks paying a lot of attention to identifying and detecting threats. Response and recovery tend to be ignored, unfortunately. All the preventive solutions in place are critical, but you absolutely need to think about what happens if all that fails. It's also important to know that not every compromise or infection is going to be the same. So, you need to determine if you have the right solutions, tools, people, and processes in place to handle everything from a small-scale attack all the way to something that's potentially an existential threat to your business.

How can customers make sure they can quickly back up and recover their data and maximize its value?

Kevin: It's important to understand the difference between backup, disaster recovery, and cyber attack recovery. It's critical to run all of these in parallel, yet they're unlikely to be the same solution. Backup and disaster recovery have slightly different use cases, so you need both.

Cyber recovery is a different animal. A disaster, like a hurricane, is impersonal. There's no attacker who's looking to evade you at every turn. So, it's important to make sure you adapt your processes to align with those differences.

Paul: I'll add one other thing to what Kevin was saying: Make sure you run an exercise on a regular basis and determine if you can recover. And do it from the perspective of not only disaster recovery but also from a cyber perspective because that's where you're going to learn whether your systems work and, more importantly, whether your humans work. Because it honestly will come down to your humans. They are the unpredictable part of any recovery scenario.

Modernize your data protection to reduce your risk without adding complexity

Protecting your data across your hybrid cloud presents plenty of challenges. You must manage backup infrastructure in distributed locations, plan and forecast unpredictable data growth, address increased risk due to cyber threats, and deal with multiple administrative touchpoints to manage backup and recovery operations on-premises and in the cloud. Modern data protection strategies allow you to keep pace with dynamic hybrid cloud environments and enable your data and applications to achieve always-on availability while building smarter and faster defenses — all while minimizing complexity in your environment.

Learn more at
HPE.com/data

Visit **HPE GreenLake**

Chat now

Hewlett Packard Enterprise

a50010131ENW