What High-Performing Security Organizations Do Differently

*Organizations that implement a range of best practices are better at closing IT security gaps and making the most of their cybersecurity investments. HPE executives **Joe Vidal**, master technologist in the company's Office of North America CTO, and **Allen Whipple**, server security and management solutions business manager, discuss key strategies for improving and simplifying IT security.*

What trends are impacting IT security in state and local governments?

Vidal: State and local governments are still trying to get a handle on remote access. At the beginning of COVID, most agencies didn't have a 1:1 ratio of devices to send home with people, so they were forced overnight into a bring-your-own-device support model and virtual desktop infrastructure (VDI) implementation. In many cases, the VDI implementation wasn't very secure, nor was it optimal. Now agencies are asking how secure their setup is, and they have to go backward to address that, which can cause some real challenges.

How do high-performing organizations close IT security gaps?

Whipple: When we say "high-performing" in this context, we mean organizations that leverage a range of key best practices related to IT security. They've adopted MFA and implemented Zero-Trust policies throughout; backup and recovery are key components of their strategy; they've trained their people to recognize threats; and so on. We've found high-performing organizations can reduce the average dwell time — that is, the average time to detect a bad actor — from 240 days to 24 hours.

What do agencies need to know about Zero Trust and its implementation?

Vidal: Zero Trust means the system continually verifies the identity of internal and external users. It's not a one-time verification process, and nobody is exempt. It starts internally because more than 60% of cybersecurity attacks happen from within an organization, where bad actors find a weakness and take advantage of someone or something. So organizations must physically secure their internal borders, boundaries and access points first. Then, they have to use artificial intelligence (AI) to look at user behavior and the way people are accessing data. Only then can they determine whether users are legitimate and authorized.

How AI and automation can improve protection?

Vidal: Many cybersecurity organizations, including the FBI, suggest that investments in AI bring the best "bang for the buck" in terms of catching and stopping breaches as they happen. Zero Trust gives you this multifactor, continuous authentication process. But more importantly, AI analyzes the user's behavior. If their activity differs significantly from previous behavior, the system alerts the security team and immediately cuts off the user — whether that's a person or an application. Unless you're using AI, you're not going to catch these things.

AI and automation are also important for regulatory compliance. There are more than 150 regulatory compliance agencies today. If you're still using manual processes to do regulatory compliance checks and reporting across those agencies, there's no way to keep up with it. It's no longer acceptable to say, "I don't know whether we're compliant; we're not scheduled to do another compliance check until June." Organizations should be using AI and automation to do that for them.

How can government organizations improve backup and recovery to combat ransomware?

Vidal: They can use immutable backups. That means standing up a network connection, creating the backup to a remote facility or remote device, and then tearing down the network connection so the backup is air gapped and immutable. It's not connected to the network, so bad actors can't access, alter or delete the backup even if they manage to get into the organization's production environment. In addition, organizations can run heuristics against that copy to detect malicious activity.

How can organizations get the most value from their cybersecurity investments?

Whipple: In one word, the answer is education. There are many wonderful tools out there, but just because an organization buys equipment does not mean security features are enabled and they're taking advantage of the security capabilities of that equipment. Suppliers can't turn on all features by default because the features require user-specific information. The organization's staff needs to understand what these tools can do, how to enable them, and how to fully utilize their features — like AI and automation — to simplify security and compliance and make life easier for everyone.