EXECUTIVE VIEWPOINT

Cole Humphreys
Global Server Security Product Management

Cole Humphreys, Global Server Security Product Management at Hewlett Packard Enterprise (HPE), is an IT industry veteran and leader with global experience. Over his decades-long career, Cole has engaged and ignited product management programs across complex business models to deliver value to customers and partners in the Americas, Europe, and Asia Pacific regions.

HPE and Intel: Building a Chain of Trust in Your Compute Environment

When it comes to your IT environment, preparing for evolving security threats and vulnerabilities requires following best practices while layering in new technologies and proactive strategies to strengthen defenses. In a recent conversation, Cole Humphreys, global server security product manager at Hewlett Packard Enterprise (HPE), shared his insights on what security teams can do to strengthen readiness and response.

How can full-stack security make for better defense and protection?

It's really about the entire chain of trust. Step one is the supply chain, trusting where the server comes from. But it's also about building on every layer after that. So, for our customers, security is built into the core of our technology with HPE iLO ASIC as well as in integrated security technologies like Intel's Xeon processors, which architecturally acts as a silicon root of trust. With each new layer, whether that's partner technology or third-party products, we've built an authentication chain that extends the silicon root of trust to protect the core components of the server and processor. Plus, we work with partners outside of the server to do remote key management and data security with secure encrypted devices. It's truly end-to-end, from supply chain to secure data operations for a single Intel powered server, and that's a big deal.

Confidential computing helps protect data while in use. Intel Xeon processors allow you to pick the confidential computing technologies that best meet your business and regulatory requirements. Intel Trust Domain Extensions (Intel TDX) offers isolation and confidentiality at the virtual machine (VM) level while Intel Software Guard Extensions (Intel SGX) provide application-level isolation. With Intel, you can choose from the most deployed data center confidential computing options on the market today.

Here's a real world example: Working with Penn Medicine as part of the largest federated learning healthcare collaboration to date, researchers improved cancerous brain tumor detection by 33% using Intel® SGX for privacy-preserving AI.

Here's a real world example: Working with Penn Medicine as part of the largest federated learning healthcare collaboration to date, researchers improved cancerous brain tumor detection by 33% using Intel® SGX for privacy-preserving AI.

Security vulnerability starts in the supply chain. What is your advice to security teams for how to manage that risk?

It starts in the supply chain, but it isn't only part of the supply chain. I advise having that philosophy, while also backing up security verifications with technical proof points. It starts with platform certificates, so you can assess the level of security when you bring the server into production. Second, make sure it comes with a cryptographic identity from that secure supply chain source. For HPE and Intel customers, we give resources that trusted identity. That way, they have access to it throughout its life cycle with automation and zero-touch provisioning.

As attacks increasingly target across compute environments, how can security leaders take a proactive approach to embedding zero trust?

We've gone from trusting someone based on their location to trusting nothing and no one. So, there's a lot of complexity to operationally achieve a zero-trust computing approach. There isn't one quick fix. You must position pieces of your strategy with new partnerships and new technologies that help you put it into practice. So, a customer may need to prove they have a zero-trust architecture running a classified, disconnected cloud, for example. In this case having HPE iLO ASIC, Gen 11 server, trusted supply chain hardening service, and HPE GreenLake for compute ops management will help prove their zero-trust computing approach. On top of that, using Intel Xeon processors adds additional layers of protection by using secure enclaves to keep data protected from unauthorized access. It's strategy, backed by a product approach.

How can infrastructure teams best manage securely retiring and decommissioning resources?

We address and manage this by easing the process for HPE and Intel customers. Whether it's supply chain or server decommissioning, we're guided by the principle of "trusted security by design." Teams don't want to be stuck properly sanitizing data on their own, yet it's critical when you're retiring, decommissioning, or repurposing a resource, so you can bring it back to the beginning of the life cycle. Instead, we've created specific HPE iLO features called One-button Secure Erase and System Erase and Reset that'll wipe the data for you. The idea is "no confidential information left behind."

How should CIOs and IT leaders manage security across multiple servers?

When you have 1,000 or 10,000 servers, managing all the security settings can be problematic, even more so when a security event happens. And with the speed of technology, there's a blast radius. The sooner you can act, the better.

For our customers, it goes back to that end-to-end coverage up the stack. Security is embedded in the core of our product in the silicon root of trust, extending out into the layers of key components, data security, and then complementary support. All of those surround a single server, except now we're looking at an entire fleet. We do that through our HPE GreenLake for Compute Ops Management solution that allows customers to remotely manage security issues across all servers and update firmware on the spot. That's supported, of course, by Intel's Crypto Acceleration and Quick Assist Technology, which facilitates faster and more secure data processing across these environments. Now, a customer can act with visibility and speed when they have a security issue on a server while maintaining policy scanning and enforcement across their entire fleet.

For more information on HPE, visit:
https://www.hpe.com/us/en/compute/hpe-proliant-with-intel.html

Click here for more information on Intel's approach to security.