Hewlett Packard Enterprise

intel

The Basics and Business of Trusted Security

Ed Tittel

- HPE delivers trusted security by design
- Security is fundamental, from the edge to the cloud
- HPE GreenLake for compute operations management

PRODUCED BY

ActualTech MEDIA

IN THIS PAPER

HPE offers a trusted supply chain, silicon-level protection and validation, and unmatched security protection and coverage in its HPE ProLiant Gen11 Server family.

CONTENTS

Cybercrime is exploding and brings towering risks and exposures to enterprises and organizations of all kinds. One need only turn to recent security and cybercrime reports to uncover some truly horrifying numbers, with potentially existential threats not far behind:

- Estimates for the total cost of cybercrime in 2025 were to top $10 trillion by 2025
- As of August 2023, IBM reported the average cost of a data breach at $4.35 million and climbing
- Cybercrime CAGR growth is predicted at 15% YoY through 2025 and could ramp up from there
- According to Red Canary the average number of cybercrime attacks grew by 31% per company in 2021, averaging 270 attacks that year, and show no signs of abating
- Likewise, 83% of organizations report more than one breach, which indicates that two or more of those attacks actually succeeded (subject to the cost of breach cited above).

Given the time, cost, and effort involved in establishing and maintaining security, organizations need to realize a return on such investments, especially when it comes to managing and mitigating risk. Ever more complex and convoluted infrastructures and operations make zero trust and secure transformation essential in a world where so much activity occurs in hybrid cloud environments, and where workers are increasingly mobile (working from home, on the road, at customer sites, and so forth).

Then, too, there's a powerful personnel shortage in cybersecurity with over 3.5 million jobs in that area expected to go unfilled by 2025. No wonder cyberattacks hit the No. 1 spot as the top concern for global businesses in 2023. Likewise, it's no accident that Statista reports 12% or more of total IT outlays went to security from 2018 to 2022. All these numbers underscore a hard and massive truth: It's a tough, scary, and challenging world out there!

HPE Delivers Trusted Security by Design

Thanks to its long-standing focus on security and risk avoidance, HPE lets organizations deploy technology with confidence. From the ground up, HPE delivers substantial protections against security threats. It begins with a "silicon root of trust" that secures millions of lines of firmware and over 4 million HPE servers around the globe to provide fundamental, innovative security. Hardware-based security supports sensitive enterprise or agency deployments (see **FIGURE 1**) where privacy, confidentiality, and protection concerns trump all else.

From the very first moments of start-up, power-on, and self-test, security and IT protection is established and maintained via the HPE integrated Lights Out (iLO) management system. This verifies all devices during system boot to make sure they're intact, secure, and tamper-free. Furthermore, HPE embraces the partners within its security ecosystem to extend protection to them. This includes a security protocol and data model to verify the integrity of components and to authenticate supported option cards. Nothing runs that's not designed, vetted, and checked in real time for security.

Given the time, cost, and effort involved in establishing and maintaining security, organizations need to realize a return on such investments, especially when it comes to managing and mitigating risk.

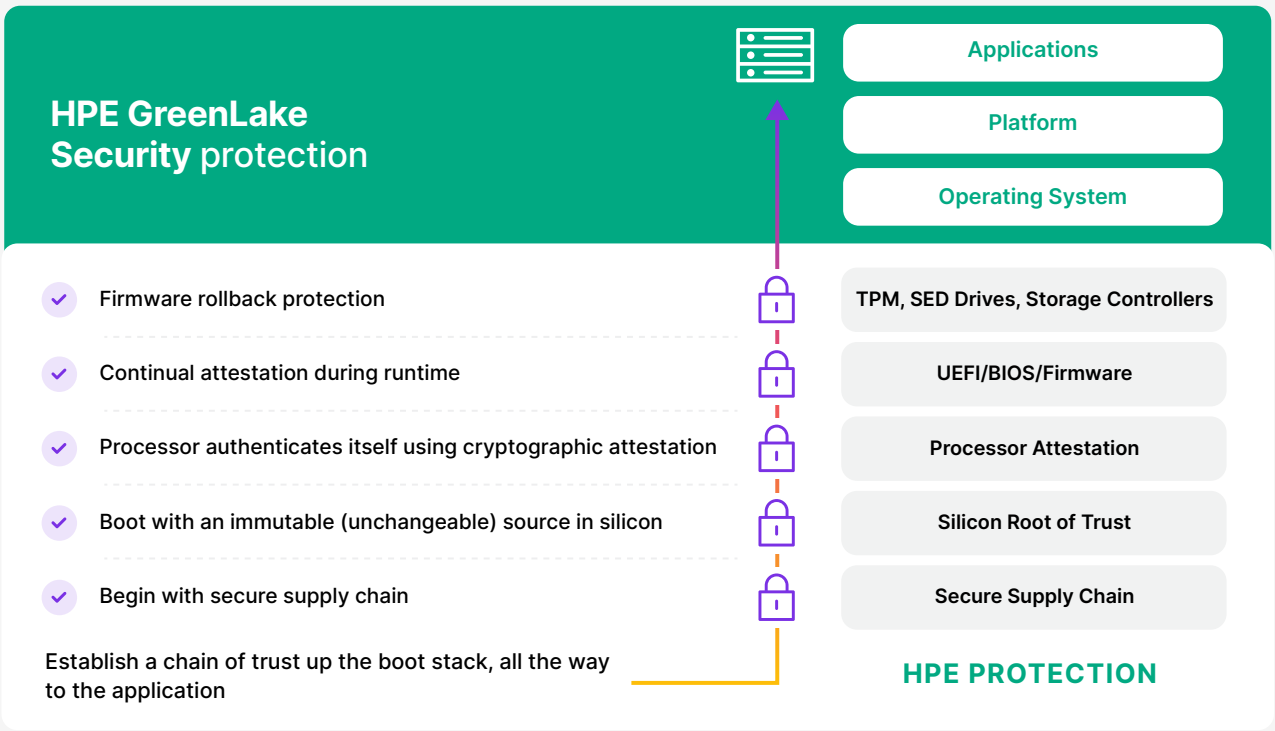

FIGURE 1: HPE Protection spans the whole path from the supply chain, to the hardware, up through the stack into the OS, platform, and application layers

HPE also extends security coverage to all parties involved in its trusted supply chain now available around the globe. This includes protection and confidence for HPE ProLiant servers obtained from trusted suppliers and manufacturing facilities, and extends protection against tamper-proofing while servers are in transit for delivery. See the September 2022 blog post, "HPE trusted supply chain expands to worldwide customers," for more information.

Security Is Fundamental, from Edge to Cloud

Silicon-level security provides continuous zero trust architecture to protect against advanced and persistent threats. This means that UEFI and firmware gets checked before it's used (with a read-only backup should anything change). This is how HPE ensures its customers don't fall prey to rootkit or other UEFI attack vectors. Worst case, if a known, good, working, and secure item can't be loaded, the server will take itself out of action until it can be securely repaired. Such robust protection may not be available from other server vendors.

From the ground up, HPE delivers substantial protections against security threats.

That's how buyers can be sure they're getting what they're paying for and that servers are secure (and secured) before they ever reach the premises. Once deployed, servers are kept secure from the silicon up, and stay that way thanks to rigorous ongoing checks, updates, and management.

Security Is Uncompromising, Across the Entire Server

HPE end-to-end security (see **FIGURE 1** for a reminder) means that platform components get checked and authenticated before they're installed, and before they get used. This secures against entry points where an attack might otherwise compromise entire server infrastructures. Processors authenticate themselves using crypto-based attestation at start-up, with ongoing runtime checks to make sure nothing has been compromised.

Silicon-level security provides continuous zero trust architecture to protect against advanced and persistent threats.

Also, firmware is checked at start-up to make sure that all such items match their "safe state data" (e.g., hashes, checksums, and so on). This applies to the Trusted Platform Module (TPM), self-encrypting storage devices (SEDs), storage controllers, and other firmware elements. For PCIe devices, firmware gets authenticated via the

industry-standard Security Protocol and Data Model (SPDM) so that storage and network controllers provide no entry points for attack, either. And, finally, through its ecosystem partnership with other manufacturers and software/service vendors—e.g., Intel, Broadcom, VMware, and others—HPE fosters and shares continuous innovation for best-in-class security on its servers and other equipment.

Protection for a Trusted Supply Chain

Indeed, customers must pay more to obtain servers from the trusted HPE supply chain. But it's now available globally under the HPE Server Security Optimized Service for HPE ProLiant. This ensures that all third-party components are checked and vetted for security before they leave their maker's points of manufacture, and that a chain of security is maintained as items are shipped to HPE, and as servers make their way from HPE to their chosen delivery locations.

HPE GreenLake covers the gamut of possible deployments from platforms (individual servers) to entire fleets (multitudes of servers in multiple data centers).

HPE GreenLake for Compute Operations Management

On the hybrid cloud front, HPE GreenLake—a potent portfolio of cloud and as-a-service options designed to simplify and accelerate business innovation—includes its own suite of security and data protection capabilities. These are designed to enhance data value through attestation (proof of identity, and a showing that OS and application software remain intact, secure, and trustworthy, based on certification authority registered TPM sign-offs) and verification (automated and ongoing checks on data integrity, coherence, validity, and relevance). In fact, HPE GreenLake covers the gamut of possible deployments from platforms (individual servers) to entire fleets (multitudes of servers in multiple data centers).

By design, HPE GreenLake delivers secure, authenticated, and encrypted connections between compute devices and the HPE GreenLake platform itself, as a function of the HPE GreenLake for Compute Ops Management service. This latter element is key, because such management lets organizations remotely access any and all parts of their runtime environment (on premises, at the edge, and in the cloud) and maintain constant, consistent, and policy-driven control over everything.

HPE GreenLake platform security, integrity, and verification mechanisms help to speed innovation and new technology adoption by creating and building upon a zero trust foundation.

HPE GreenLake platform security, integrity, and verification mechanisms help to speed innovation and new technology adoption by creating and building upon a zero trust foundation. This means all parties must continuously prove their identities, and demonstrate verifiable access rights or permissions with each and every interaction with applications, services, and so forth. Zero trust makes it much easier to identify actual or potential attacks. It also helps organizations protect their investments by minimizing attack surfaces, thereby limiting their risks of exposure or compromise. This extends across the entire chain shown in **FIGURE 1**, as follows to secure the servers in use:

1. **A secure supply chain** makes sure all elements and components are designed and built for security, and that nothing gets changed from checked and vetted designs.

2. **A silicon root of trust** provides access to immutable (read-only) sources for firmware, UEFI, and so forth in silicon so that a known, good, working, secure version is always available for use.

3. **Processor attestation** means the CPU authenticates itself through cryptography-based proofs of identity and integrity.

4. **UEFI/BIOS/Firmware** are continuously checked for attestation at runtime, and prevented from running if checks should fail.

5. **HPE ProLiant Gen11 servers** include firmware rollback protection to prevent tampering with TPM, self-encrypting drives, storage controllers, and more. SPDM provides similar protection for PCIe devices and controllers, especially for storage and networks.

Thus, HPE provides solid security from end-to-end all the way from silicon into applications and services. And it does so at scale all the way into and across the hybrid cloud combinations typical in most modern enterprises, organizations, and agencies.

LEARN MORE

Explore how HPE ProLiant Gen11 servers are built entirely to establish and maintain security, so organizations can trust their valuable data and services and customers will remain safe and sound as workloads start up, run, and complete within their embrace. To learn more, please visit the HPE ProLiant Gen11 pages, especially the "HPE Compute, trusted security by design" resources.

HPE GreenLake