World Wide Technology
Hewlett Packard Enterprise

HPE Secure Compute Lifecycle:

Optimizing Public Sector Agency Security Environments with the World's Most Secure Industry Standard Servers

Securing networking and compute infrastructure within public sector agencies is critical, given the ever-increasing threats to government data and resources. With cyber-attacks occurring every 39 seconds, how can you protect your organization from attacks that can steal data or create or distribute viruses using web-based attacks, malware, denial of service attacks, or malicious code?

Secure data begins with secure infrastructure. Attack surfaces include the network perimeter, server applications and operating systems, data at rest and in transit, the platform hardware, and even the firmware in the server. As the number of attacks and cost of threats rise, more and more attack surfaces are being "hardened" to defend against cyber-attacks. In response, attackers are increasingly focusing on lower-level attacks, including attacks on the firmware.

Firmware is the New Target

Firmware is becoming a more frequent target for denial of service (DOS) attacks since the firmware code operates in a privileged position and if compromised, can go for months without being detected. Thus, protecting networks only at the perimeter firewall level or servers at the software and OS level is no longer sufficient to provide adequate protection against security threats. That's where Hewlett Packard Enterprise's exclusive Secure Compute Lifecycle comes in.

Hewlett Packard Enterprise is proactively improving its security stance to meet challenges, such as attacks on firmware, by continually improving the hardware and firmware security of its server platforms and related infrastructure hardware. This ensures that every link in the chain of security provides the most effective cyber security protections possible.

HPE Secure Compute Lifecycle

Security is top-of-mind for public sector organizations of all sizes. Hewlett Packard Enterprise delivers an end-to-end security solution that addresses protection at every stage in the server's lifecycle:

Stage 1: Ultimate Firmware Protection
Hewlett Packard Enterprise provides the only industry-standard servers with a Silicon Root of Trust capability built into the hardware, which prevents compromised firmware code from executing. We can address platform security all the way back to the supply chain because we design the iLO 5 entirely— hardware and firmware—and control the iLO 5 production process. This gives customers an unprecedented level of assurance that no hackers have compromised the firmware before they receive their server.

Secure Compute Lifecycle

1
Ultimate Firmware Protection

2
Run Time Attack Protection

3
Identification of Potential Behavioral Risks

4
Data Security within the Server

5
Accelerated Regulatory Compliance

6
Safe Disposal of Data and Infrastructure

Stage 2: Run Time Attack Protection
As soon as the server is booted and the iLO firmware becomes active, Hewlett Packard Enterprise's Silicon Root of Trust looks for the immutable fingerprint that verifies all firmware code is valid and uncompromised. Before the operating system (OS) even starts, over a million lines of firmware code run, confirming that all server essential firmware is free from malware or compromised code.

Hewlett Packard Enterprise's Runtime Firmware Verification checks the firmware stored in the server operation. At any point, if compromised code or malware is inserted in any of the critical firmware, an iLO audit log alert is created to notify you that a compromise has occurred. Feature sets like Runtime Firmware Verification can detect such an event and allow you to securely recover the firmware automatically to a previous known good state. Given the enhanced protection and detection capabilities built into our Gen10 servers, it is unlikely to have a firmware breach.

Stage 3: Identification of Potential Behavioral Risks
Aruba ClearPass creates a strong networking security clearance protocol for clearing anyone requesting access to the network. Niara, a subsidiary of Hewlett Packard Enterprise, monitors user activity inside the network. Once ClearPass vets and clears users into networks, Niara takes over and, using machine learning, works to predict any nefarious behavior before any serious damage can be done. If Niara identifies abnormal activity resembling potential malicious behavior, it communicates to ClearPass, temporarily terminating the suspected user's access to the network until more thorough vetting can be conducted.

Stage 4: Data Security within the Server
Protecting data and communication to and from the server, and inside the server is crucial. Hewlett Packard Enterprise is the first industry server manufacturer to provide support for the commercial national security algorithms (CNSA) suite. This is the very highest level of security, typically used for confidential and top-secret information. We also have FIPS validation on firmware as another level of protection during the operation phase of the server's life. Scalable encryption is another differentiated offering that protects data stored in the server. Going one step further, Atalla Enterprise Secure Key Manager (ESKM) takes key management to a higher level. Through this technology, we save you the agony of tracking—sometimes on spreadsheets—an unmanageable number of encryption key**s.**

Stage 5: Accelerated Regulatory Compliance
HPE Gen10 servers comply with multiple security standards and encryption protocols, including Federal Information Processing Standard (FIPS) Publication 140-2, the National Institute of Standards and Technology (NIST) 800-147b, the payment card industry data security standard (PCI DSS), and Common Criteria.

Stage 6: Safe Disposal of Data and Infrastructure
The final stage comes after the servers and other equipment have reach their full use and entered end of life. HPE Pointnext security and protection services provide final disposal of equipment, ensuring the data is properly disposed of according to NIST standards.

About World Wide Technology

World Wide Technology (WWT) is a technology solution provider with $13.4 billion in annual revenue that provides digital strategy, innovative technology, and supply chain solutions to large public and private organizations around the globe. Based in St. Louis, WWT employs more than 7,000 people and operates over 4 million square feet of warehousing, distribution, and integration space in more than 20 facilities throughout the world. For more information about World Wide Technology, visit **wwt.com.**

About Hewlett Packard Enterprise

Hewlett Packard Enterprise is a global, edge-to-cloud Platform-as-a-Service company built to transform your business. How? By helping you connect, protect, analyze, and act on all your data and applications wherever they live, from edge to cloud, so you can turn insights into outcomes at the speed required to thrive in today's complex world. Click **here** to learn more.