Fact sheet

Hewlett Packard
Enterprise

HPE Gen10 Server security

There are 720 million hack attempts every 24 hours worldwide.[1] Are your servers protected?

HPE Gen10 Servers are "The World's Most Secure Industry Standard Servers."[2] This bold claim is founded on our unique silicon root of trust technology along with several differentiating security technologies that only Hewlett Packard Enterprise offers.

HPE servers are built on the belief that infrastructure should be the strongest defense, armed with the latest innovations to **protect, detect, and recover** from security attacks. Just as customers expect and deserve high-quality and reliable products, they should also expect the most secure infrastructure in the industry.

Protect

> "As cyber-attacks become more sophisticated, the potential for BIOS or other firmware attacks is growing"
>
> – National Institute of Standards and Technology

Silicon root of trust

HPE Gen10 Servers have an exclusive advancement in security protection called silicon root of trust. In our unique root of trust implementation, the server essential firmware is anchored to the iLO 5 silicon—an immutable fingerprint that verifies all the firmware code is valid and uncompromised. This bond guarantees that only valid and uncompromised firmware code can boot. Learn more in the **Demystifying Server Root of Trust** white paper.

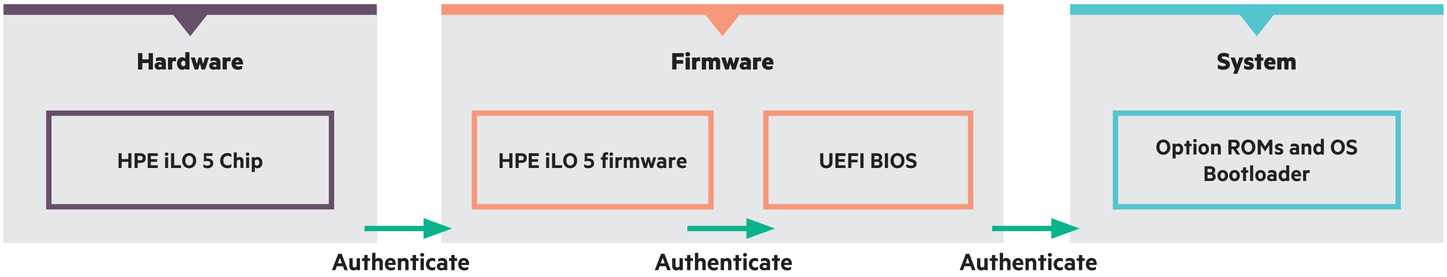


Figure 1. Silicon root of trust

Secure supply chain

A vendor's supply chain is an essential element of cybersecurity because of the possibility that products could be compromised at their source. HPE reduces the risk of exposing the supply chain to threats such as counterfeit materials, malicious software embedded in products, and other untrustworthy components by vetting component vendors and sourcing from the Trade Agreements Act (TAA) designated countries. Unlike other organizations, HPE reduces **security** concerns and threats further by developing BIOS, management firmware, and ASIC in-house while competitors choose to outsource their baseboard management controller (BMC) solutions. Secure server options such as the chassis intrusion detection kit also ensure your server is delivered free from tampering. Even when the server is powered off, the chassis intrusion detection kit will trigger an **HPE iLO** audit alert if the hood is ever removed from the server.

[1] CNBC 2016

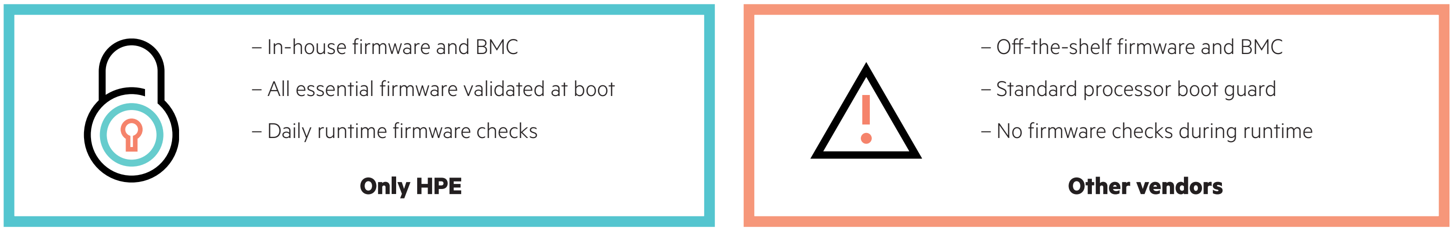
[2] Based on external firm conducting cybersecurity penetration testing of a range of server products from a range of manufactures, May 2017

Detect

It takes the average business **101 days** to detect malicious code[3]

Runtime firmware verification

Ensuring security at boot is essential but what about protection during the server runtime? During server operation, HPE has an exclusive technology that conducts daily runtime firmware validation. If compromised code or malware is inserted in any of the critical firmware, an HPE iLO audit log alert is created to notify the customer that a compromise has occurred. This functionality is made possible by the exclusive silicon root of trust.



– In-house firmware and BMC

– All essential firmware validated at boot

– Daily runtime firmware checks

Only HPE

– Off-the-shelf firmware and BMC

– Standard processor boot guard

– No firmware checks during runtime

Other vendors

Figure 2. Runtime firmware verification

Recover

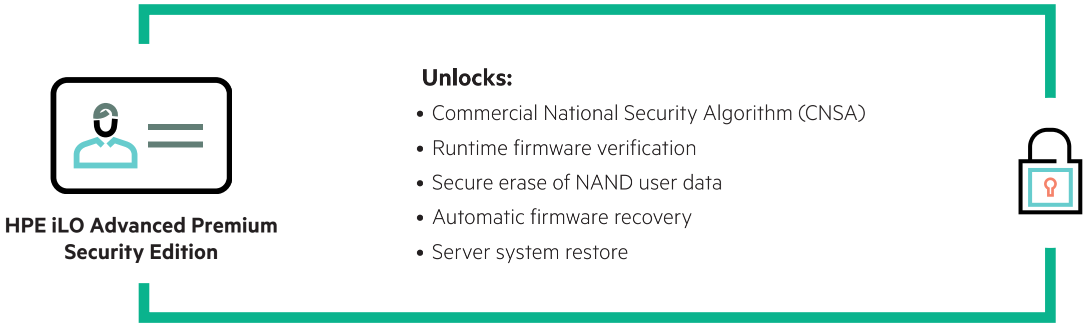
Companies lose **$9 million**, on average, each year due to cybercrime[4]

Automatic recovery of essential firmware

In the unlikely event of a breach into the HPE server firmware due to silicon root of trust protection, after breach detection has been completed, the customer may then securely recover the firmware automatically to a previous known good state. HPE provides this function through the HPE iLO Advanced Premium Security Edition License.

Server restoration at scale

In addition to essential firmware recovery, the HPE exclusive server system restore feature leverages HPE iLO Amplifier Pack software to securely restore up to 10,000 servers[5] with a single click. In the event of a ransomware attack or other breach, users can leverage the feature to automatically or manually recover the server's essential firmware, firmware configuration settings, operating system, and host environments back to an operational state.



HPE iLO Advanced Premium Security Edition

Unlocks:

- Commercial National Security Algorithm (CNSA)
- Runtime firmware verification
- Secure erase of NAND user data
- Automatic firmware recovery
- Server system restore

[3] **M-Trends 2018, Mandiant**

[4] **2016 Cost of Cyber Crime Study & the Risk of Business Innovation**, Ponemon, 2016

[5] HPE Internal Testing, February 2017

Learn more at
hpe.com/security

a00044916ENW, April 2018