Hewlett Packard Enterprise

Solution brief

Check if the document is available in the language of your choice.

PROTECT. DETECT. RECOVER

14 seconds

is the time another business has become victim to ransomware[1]

$9.5M

is the average annualized incident cost[2]

$6 trillion

expected cost of cybercrime by 2021[3]

HPE NEXT-GENERATION INFRASTRUCTURE SECURITY

The global security risks are increasing exponentially due to the increased attack surfaces (IoT, mobile, and internet), compounded by the increased sophistication of the attackers (nation states and highly skilled hackers).

Surviving and thriving in the era of digitization as IT transforms from sole provider to a broker of digital services is a difficult task. Customers are faced with these three key challenges.

1. Nature and motivation of attacks Sponsored and organized for profit and disruption
2. Regulatory pressures Increasingly burdensome and complex compliance regulations including HIPAA, HITECH, FISMA, GDPR, and PCI DSS v3
3. Transformation to hybrid cloud Delivery and consumption changes

HOW DOES HPE HELP?

The HPE ProLiant 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. The HPE-exclusive silicon root of trust and the Aruba Policy Enforcement Firewall (PEF), have been recognized for their ability to reduce risk by insurers in the Cyber Catalyst℠ program created by Marsh, a global leader in insurance broking and risk management. Cyber Catalyst is Marsh's new cybersecurity evaluation program that enables customers that adopt designated technologies to be considered for enhanced terms and conditions on cyber insurance policies from participating insurers. Also HPE InfoSight for servers transforms how your infrastructure is managed and supported by enabling simplified, cloud-based AI driven operations. HPE has one of the most comprehensive security strategies, focusing on protecting, detecting, and recovering within its products.

[1] "Comprehensive server restoration with Hewlett Packard Enterprise," Moor Insights & Strategy, 2018

[2] "Moor Insights: HPE locks down server security," 2017

[3] Forbes, "Hewlett Packard Enterprise Releases iLO Amplifier Pack With Server System Restore," February 2018.

FIPS 140–2 Level 1 validated
HPE ProLiant DL325 Gen10 and HPE ProLiant DL385 Gen10 servers with HPE iLO 5 use an intelligent microprocessor, secure memory, and dedicated network interface to operate in a mode that complies with FIPS 140–2 Level 1 requirements.

For more information about HPE security features

- HPE Secure Compute Lifecycle white paper
- HPE Gen10 Security Reference Guide

PROTECT

HPE Silicon Root of Trust

HPE is the only vendor to provide Silicon Root of Trust, which anchors essential boot block firmware to the Made in House HPE iLO 5 chip. This creates an immutable fingerprint that verifies the firmware code is valid and uncompromised, so the server won't boot with compromised firmware.

Secure boot

Secure boot is an industry standard security feature that is implemented in the BIOS. Secure boot ensures that any drivers launched during the boot process and the OS bootloader are digitally signed and validated against a set of trusted certificates securely stored by the BIOS. With secure boot enabled, only validated drivers and OS boot loaders are executed.

Secure supply chain

HPE reduces the risk of supply chain threats—such as counterfeit materials, malicious software, and other untrustworthy components—by vetting component vendors and sourcing from Trade Agreements Act (TAA)—designated countries. HPE further reduces security concerns and threats by developing the BIOS, management firmware, and iLO 5 chip in-house. Secure server options such as a chassis intrusion detection kit can further reduce the risk of tampering—even when the server is powered off. Server configuration lock ensures firmware is securely encrypted while in transit.

DETECT

Runtime firmware verification

Protection during server runtime is provided by an exclusive HPE technology that can conduct daily checks of the server's essential firmware. If compromised code or malware is inserted in critical firmware, an HPE iLO audit log alert is created to notify you that a compromise has occurred. This functionality is made possible by the exclusive HPE Silicon Root of Trust. The iLO Advanced security dashboard monitors security status of servers.

RECOVER

Automatic recovery of essential firmware

In the unlikely event of a firmware breach, given the enhanced security capabilities built into ProLiant Gen10 servers, you will be able to securely and automatically recover the firmware to a previous known-good state.

Server restoration at scale

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

FIND OUT MORE TODAY

Don't wait to protect your servers from cybercriminals. Contact your HPE or authorized channel partner representative to learn more, today.

LEARN MORE AT

hpe.com/security

Make the right purchase decision. Contact our presales specialists.

Chat **Email** **Call**

Share now

Get updates

Hewlett Packard Enterprise

a50000786ENW, February 2020