Hewlett Packard Enterprise

Protect, detect, recover

HPE ProLiant Gen10 and AMD EPYC technology for secure virtualization

Part of the world's most secure industry-standard server portfolio[1]

1.9 billion
records breached in 6 months[2]

15X
increase in ransomware attacks[3]

$6 trillion
expected cost of cybercrime by 2021[4]

Are you protected?

Virtualization remains the primary means for maximizing agility and efficiency in a hybrid environment. In 2016, 26% of workloads were virtualized, with enterprise leaders open to virtualizing more than 80% of their workloads,[5] and server virtualization was the #1 planned infrastructure project.[6] In fact, analysts predict that 41% of new server shipments will be virtualized in 2020 up from 33% in 2015.[7] And it's no wonder—enterprises report savings of almost 20% from server virtualization.[8]

As the data center becomes more virtualized, servers should be your strongest defense, arming you with the latest innovations to prevent, detect, and recover from security attacks. That's why we've developed unique security technologies, giving you a new security foundation to protect your data—and your business.

HPE ProLiant DL325 Gen10 and HPE ProLiant DL385 Gen10 servers are built for virtualization, with security features that help protect your hardware, firmware, and network from unauthorized access and unapproved use. HPE also offers an array of embedded and optional software and firmware so you can choose the Right Mix of remote access and control for your network and data center.

HPE ProLiant DL325 Gen10 and HPE ProLiant DL385 Gen10 servers with AMD EPYC™ processors provide advanced security features you can count on to create a best-in-class secure server solution for virtualization.

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

[2] CNBC, "**The number of devastating cyberattacks is surging—and it's likely to get much worse**," September 2017.

[3, 4] Forbes, "**Hewlett Packard Enterprise Releases iLO Amplifier Pack With Server System Restore**," February 2018.

[5, 6] IDC, "**Market Trends in Virtualization Infrastructure and Software, 2016: Market Survey Report**," December 2016.

[7] TechTarget, "IT Priorities 2017," February 2017.

[8] Function with an HPE iLO Advanced Premium Security Edition License.

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**
- **Demystifying Server Root of Trust—Moor Insights & Strategy white paper**

[9] HPE Internal Testing, February 2017

Protect

HPE Silicon Root of Trust

HPE is the only vendor to provide Silicon Root of Trust, which anchors essential firmware to the custom 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.

AMD Secure Processor

A dedicated AMD Secure Processor is embedded in the AMD EPYC system on a chip. It manages secure boot, tying into the HPE Silicon Root of Trust at the firmware level, and validating the HPE BIOS during the boot process. AMD Secure Memory Encryption (SME) enables inline encryption and decryption with secure key generation and management—and minimal performance impact. AMD Secure Encrypted Virtualization allows virtual machine (VM) memory contents to be transparently encrypted with a high-performance encryption engine that can be programmed with multiple keys for use by different VMs in the system.

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.

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.

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.[9]

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.

HPE innovations

HPE ProLiant DL325 Gen10 and HPE ProLiant DL385 Gen10 servers, along with AMD EPYC processors, bring together the latest innovations in security and performance. The advanced capabilities of iLO 5 enable secure boot, daily scanning of firmware, and automatic restoration to the last known-good configuration.

Find out more today

Don't wait to protect your servers from cybercriminals.

Our solution partner

AMD

Make the right purchase decision. Click here to chat with our presales specialists.

Share now

Get updates

a00049646ENW, February 2019, Rev. 1