WHITE PAPER

Hewlett Packard Enterprise | Red Hat

HPE and Red Hat: Transforming Server Security

Securing your company's compute infrastructure is critical, given the ever-increasing threats to data and resources. Cyberattacks range from stealing an organization's intellectual property, to creating and distributing viruses, using web-based attacks, malware, denial of service attacks, malicious code, and even stolen devices.

Vulnerable 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 surfaces are being "hardened" to defend against them.

Servers are virtual treasure chests of the sensitive and confidential data that hackers want most. The server hardware and operating system (OS) provide a vast attack surface; hackers see the opportunity, targeting supply chains and firmware to infiltrate systems early and surreptitiously. All it takes is a single vulnerability at either the hardware or OS level for attackers to find the toehold they need for infiltrating your system.

The traditional approach to server security doesn't cut it anymore. A modern server infrastructure requires robust hardware and software that work together at the firmware level to prevent compromise. Together, HPE and Red Hat Enterprise Linux are transforming server security holistically.

This white paper explores the requirements for a modern server infrastructure and introduces the new partnership linking HPE Gen10 servers and Red Hat Enterprise Linux 8.1.

The New Security Requirements

Today's compute infrastructure is vastly different from 5-10 years ago. The network perimeter has dissolved. Most IT infrastructure uses a hybrid cloud model. Assets are accessed directly. Despite the fact that security threats pose a greater risk than ever before, many operating models remain the same: they are built on a chain of trust. If firmware is compromised, the entire basis of how the OS, the server itself, and remediation processes operate are compromised.

Simply put, the server OS and the underlying hardware must be secure together from the ground up. That includes built-in controls to help prevent compromise and stop processes from running if a problem is detected..

HPE and Red Hat Enterprise Linux: Transforming Server Security

Together, HPE and Red Hat Enterprise Linux offer a joint solution that ties together the data plane (where packets are moved between endpoints) and the control plane (where network signaling, learning, and planning occur) for superior protection as well as detection and recovery capabilities—all while maintaining high performance.

Under the hood: HPE Gen10 servers

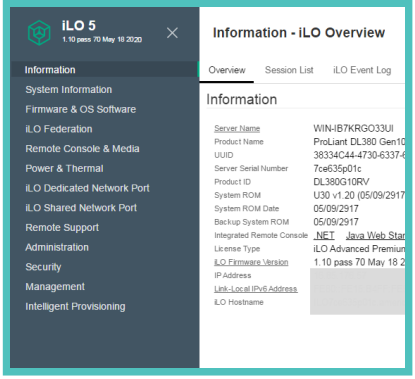
HPE Gen10 servers are built for virtualization, with security features that help protect your hardware, firmware, and network from unauthorized access and unapproved use. These features include the following:

- **HPE Silicon Root of Trust**—HPE is the only vendor to provide the Silicon Root of Trust, which anchors essential firmware to the custom HPE Integrated Lights-Out (iLO) 5 chip. The iLO 5 chipset acts as a Silicon Root of Trust and includes an encrypted hash embedded in the silicon hardware at the chip fabrication facility. This means it is virtually impossible to insert any malware, virus, or compromised code that would corrupt the boot process. The iLO 5 hardware determines whether to execute the iLO firmware based on whether it matches the encryption hash that is permanently stored in the iLO chipset silicon.

  The HPE Silicon Root of Trust has earned the Marsh Cyber CatalystSM designation, a testament to the technology's ability to reduce risk. The Cyber CatalystSM program was created by Marsh, an insurance broker and risk management firm. It is designed to help organizations make more informed choices about the cyber security products and services they use to manage their cyber risk. Companies that deploy technologies recognized by the program are eligible for enhanced terms and conditions on their cyber insurance policies from participating insurers.

  HPE's exclusive Silicon Root of Trust is the foundation for the entire "secure start and recovery "process, enabling Gen10 servers to be the world's most secure industry standard server portfolio. The Silicon Root of Trust forms a unique link between the custom HPE silicon and the HPE iLO firmware to ensure servers do not execute compromised code. Building this security directly into the HPE silicon provides the ultimate protection against firmware and ransomware attacks, as well as the ability to automatically recover the essential server firmware.
- **Runtime firmware verification**—This exclusive HPE technology conducts scans at selected intervals on the server's essential firmware. If compromised code or malware is inserted in critical firmware, an HPE iLO audit log alert is created to flag the compromise. Customers also have the option to automatically recover the authentic firmware.
- **Secure boot**—Secure boot is an industry-standard security feature that is implemented in the UEFI BIOS. Secure boot ensures that the OS bootloader, along with any drivers launched during the boot process, 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 and is available in AMD EPYC™ processor-based HPE Gen10 server models. It manages the secure boot, tying into the HPE Silicon Root of Trust at the firmware level, and validating the HPE BIOS during the boot process.
- **Secure supply chain**—HPE reduces the risk of supply chain threats, such as counterfeit materials and malicious software, by vetting component vendors and sourcing from Trade Agreements Act-designated countries. HPE further reduces security risks by developing the BIOS, management firmware, and iLO5 chip in-house.

THE iLO 5 CHIPSET MAKES IT VIRTUALLY IMPOSSIBLE TO INSERT ANY MALWARE, VIRUS, OR COMPROMISED CODE THAT WOULD CORRUPT THE BOOT PROCESS.



Under the hood: Red Hat Enterprise Linux 8.1

Red Hat Enterprise Linux 8.1, an open source OS, provides a consistent, security-focused foundation for modern business operations across a distributed IT infrastructure. IT organizations are empowered to better protect information assets with built-in security tools such as:

- **Terminal session recording integrated with auditing**—This feature can record both the input and output of users' shell sessions—including text window resizing and timing—and correlate them with the environment and state of the system. Sessions are recorded as JSON-formatted audit records via file, system journal, or syslog. Integration with System Security Services Daemon and Red Hat Identity Management allows recording on a per-user or per-group basis. Sessions can be played back via a terminal window or the web console.
- **System-wide cryptographic profiles**—System-wide cryptographic profiles make it easier to manage and automate cryptographic settings, reducing the risk of errors and increasing compliance. System-wide cryptographic policies with support for OpenSSL 1.1.1 and TLS 1.3 help maintain cryptographic compliance. Instead of manually configuring services, IT admins can change cryptographic settings across the entire environment with a single command.
- **Security-Enhanced Linux (SELinux) profiles**—Security policy refinements for SELinux mandatory access controls as well as container-centric SELinux profiles are included in Red Hat Enterprise Linux 8.1. The latter allow IT admins to create more tailored security policies to control how containerized services access host system resources. This makes it easier to harden production systems against security threats targeting cloud-native applications and provides a more streamlined way to maintain regulatory compliance by reducing the risk of running privileged containers.
- **Live kernel patching**—Full support for live kernel patching helps keep critical workloads running more securely. Kernel updates can be applied to remediate critical or important common vulnerabilities exposures (CVEs) while reducing the need for a system reboot.
- **Red Hat Insights**—Included with a Red Hat Enterprise Linux 8.1 subscription, Red Hat Insights enables IT organizations to benefit from the experience and technical knowledge of Red Hat Certified Engineers, making it easier to identify, prioritize, and resolve issues before business operations are affected. Red Hat Insights provides proactive analytics across complete, hybrid infrastructures, so IT organizations can proactively identify and remediate risks across the Red Hat infrastructure from the moment the OS is deployed.
- **Security certifications**—As the foundation for mission-critical, sensitive workloads, Red Hat Enterprise Linux 8.1 is architected for many of the latest security certifications, including Federal Information Processing Standards (FIPS) and Common Criteria (CC).

IT ADMINS CAN CREATE MORE TAILORED SECURITY POLICIES TO MAKE IT EASIER TO HARDEN PRODUCTION SYSTEMS AGAINST SECURITY THREATS THAT TARGET CLOUD-NATIVE APPLICATIONS.

The Bottom Line

Industry standard servers running vulnerable OSes don't have a place in a modern distributed IT infrastructure. Instead, organizations need servers and OSes that work together to prevent compromise. Together, HPE and Red Hat Enterprise Linux offer the most advanced server security solution available today. IT organizations benefit from the peace of mind of knowing that they have industry-leading technology and a tested hardware-software combination that offers the world's most secure industry standard server and operating system.

LEARN MORE

HPE and Red Hat offer the industry's most secure server platform with the Linux OS. To learn more, visit

Red Hat or **HPE**