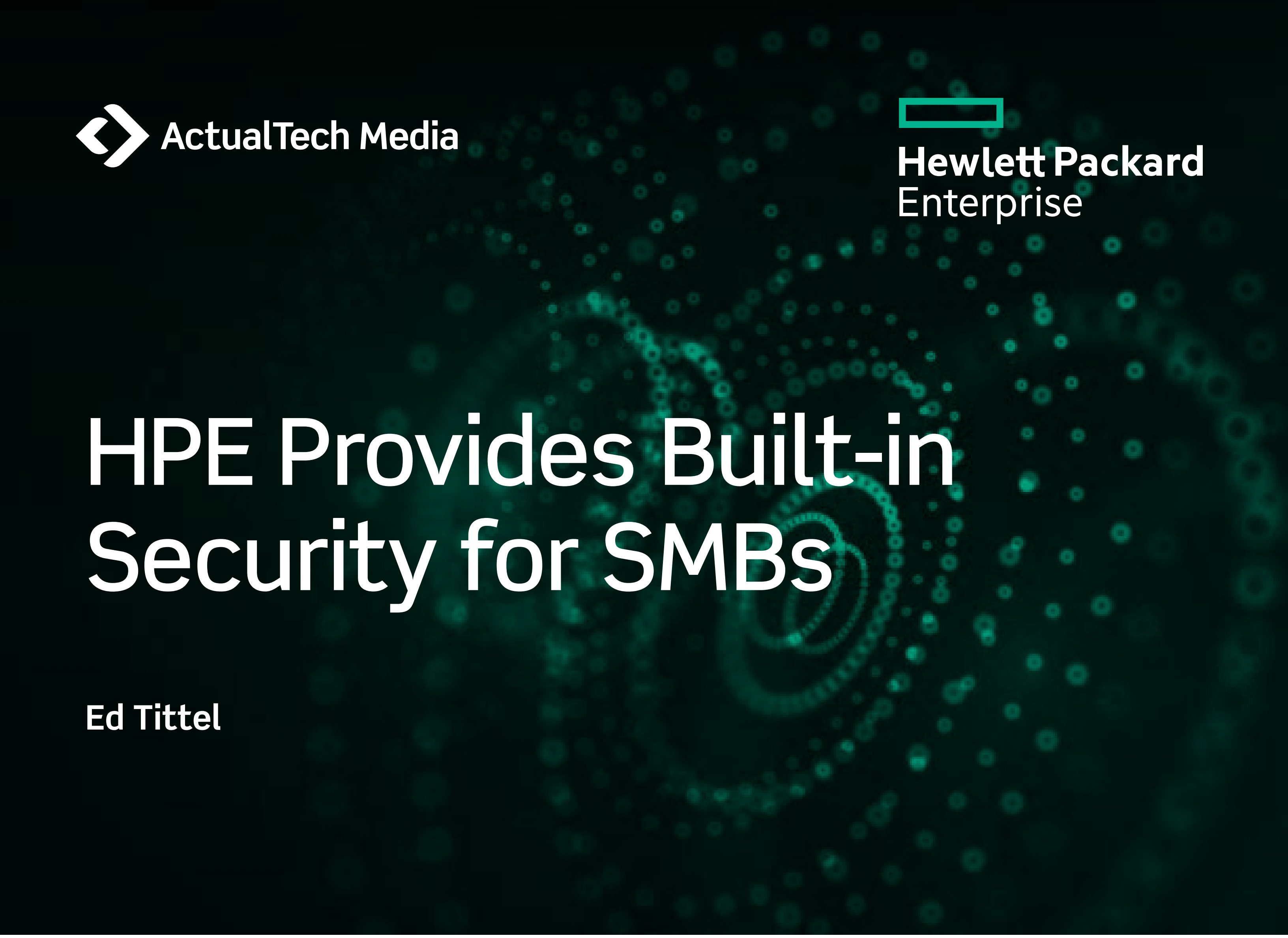

ActualTech Media

Hewlett Packard Enterprise

HPE Provides Built-in Security for SMBs

Ed Tittel

CONTENTS

IN THIS PAPER

HPE offers built-in security that extends from the silicon level into the server supply chain to provide protection throughout the entire IT lifecycle. This tech brief explores how HPE addresses security directly and explicitly through different mechanisms.

Security plays into all aspects of IT operation across the entire organization. Thus, security is important not just for system hardware and software, it's also important for the people who use such things. Establishing and maintaining security works best for businesses who choose a vendor who understands that security must be designed into systems and software, built into them from their inception, and maintained as part of a complete lifecycle process. In fact, HPE provides complete security coverage for the whole business, from end to end, for all systems and users alike.

What Security Means in 2021

A good general definition of cybersecurity is a body of technologies, processes, and practices designed and enacted to protect digital systems and assets—including networks, devices, software, and data—from attack, damage, or loss, and unauthorized access. Thus, security is inherently all-encompassing and covers systems, communications, programs, data, and connections. Sensitive data often comes with the requirement for special attention and protection, be it intellectual property, financial data, personally identifiable information (PII), health records, and other kinds of data. If disclosed to the wrong parties, it could result in negative outcomes, both for the organization holding such data, and for the party to which the data refers or belongs.

Security is often applied to specific focuses or concerns and typically includes:

- **Server security:** The collection of tools, technologies, settings, firmware, and software (both inside and outside the server's operating system) that defines and provides security for networked servers belonging to an organization. Often involves access to infrastructure security elements, as well as server firmware plus standalone and operating system software components.

- **Client security:** The collection of tools, technologies, settings, firmware, and software (both inside and outside the client's operating system) that defines and provides security for networked clients belonging or connecting to an organization's networks. Often viewed as synonymous with endpoint security, because clients comprise the bulk of endpoints within most organizations. Usually incorporates threat detection and prevention components, including anti-malware, patch and update management, and more. Also interacts with infrastructure security elements, both local and remote (where applicable).

- **Network security:** The collection of tools, technologies, devices, and software that resides on or monitors and manages network devices (both physical and virtual). Generally involves inspection and filtering of network traffic, primarily at network boundaries to control ingress and egress. May host infrastructure security elements, often in the form of software-defined networking (SDN) for local or wide-area (SD-WAN) network components and services.

- **Cloud security:** The collection of tools, technologies, and software that resides in, monitors, and manages cloud access and use, setup and provisioning, tear down and decommissioning, and traffic/activity monitoring. Intended to protect the underlying physical infrastructure, cloud security may also extend to virtual infrastructures and services running and data used in the cloud, as well.

- **Infrastructure security:** The collection of tools, technologies, and software used to monitor and manage any and all components of an organization's networks and infrastructure, including client, server, and network devices, as well as cloud components and services accessible to the organization. Infrastructure security provides a big-picture view for entire infrastructures, via dashboards, automation, and other tools used to view, manage, and control their constituent elements and components.

> HPE can help small businesses deal with all of these security focuses and concerns, and ensure that their risk management strategies are in keeping with their business goals and objectives.

Interestingly, cybersecurity includes all of these various focuses and concerns. It involves software, hardware, and firmware used on clients, servers, and networks directly under an organization's control. It also involves cloud-based components often under a third-party's control (often a cloud platform, services, or Software-as-a-Service [SaaS] provider running a public or private cloud).

> Silicon root of trust prevents compromised firmware code from executing.

Risk management services also play into cybersecurity because they concern themselves with reducing or eliminating sources of risk that could potentially damage an organization's earnings, ability to conduct business, or reputation using defensive or protective measures. It requires prioritizing and managing digital defenses to offset the potential adverse impacts of threats they pose (small or minor risks get little or no response, whereas large or major risks get big and substantial responses). HPE can help small businesses deal with all of these security focuses and concerns, and ensure that their risk management strategies are in keeping with their business goals and objectives. The sections that follow explain specific HPE technologies used to offset specific security risks, especially for HPE servers and their clients.

Silicon Root of Trust

Silicon root of trust is designed to protect against specific, targeted firmware and BIOS attacks. It works for HPE ProLiant Servers, and establishes a link between custom HPE silicon on those servers and their Integrated Lights Out (iLO) firmware. Essentially, silicon root of trust prevents compromised firmware code from executing. It does so by running integrity checks on firmware code before it's allowed to execute, using special, read-only checksums and comparison tools not directly accessible to the operating system or programs that run atop the OS.

Whenever any evidence of tampering or change is detected, the HPE iLO firmware wipes the potentially (or actually) compromised firmware code. It uses a valid, known-to-be-correct firmware image from a trusted source to replace the code it finds. Then it executes that known, good working copy automatically. HPE iLO integrates encryption with its breach detection tools so that only safe firmware code can ever be executed. If the server is unable to obtain or run such safe firmware code, it will shut down rather than run potentially compromised firmware. This ensures HPE ProLiant servers are protected from rootkit and other pre-boot attack methods and vectors.

HPE Pointnext Security Services

HPE Pointnext Services is HPE's support, advisory, professional, and education services organization. HPE experts work with HPE customers to help them address security and risk management challenges across their digital transformation, IT operations from edge to cloud. HPE is happy to work with SMBs to help them prepare their workforce and re-skill their employees with security training courses and certification. Digital Learner subscriptions package HPE technical training for consumption by SMB teams, and combine access to all the value in training HPE offers—at a better value.

Trusted Platform Module (TPM)

The TPM comes in the form of a computer chip (microcontroller) that securely stores artifacts used to authenticate a runtime platform, including servers and client PCs (laptops, tablets, all-in-ones, and so forth). Since January 2021, Microsoft requires all new Windows Server platforms to incorporate TPM version 2.0, with Secure Boot turned on by default, and recommends that all servers also use BitLocker encryption for additional protection against potential "rootkit" malware attacks. HPE has backed and supported TPM since it became an ISO/IEC standard (11990) in 2009. Today, all available modern HPE ProLiant Servers and HP, Inc. PCs meet or exceed these requirements.

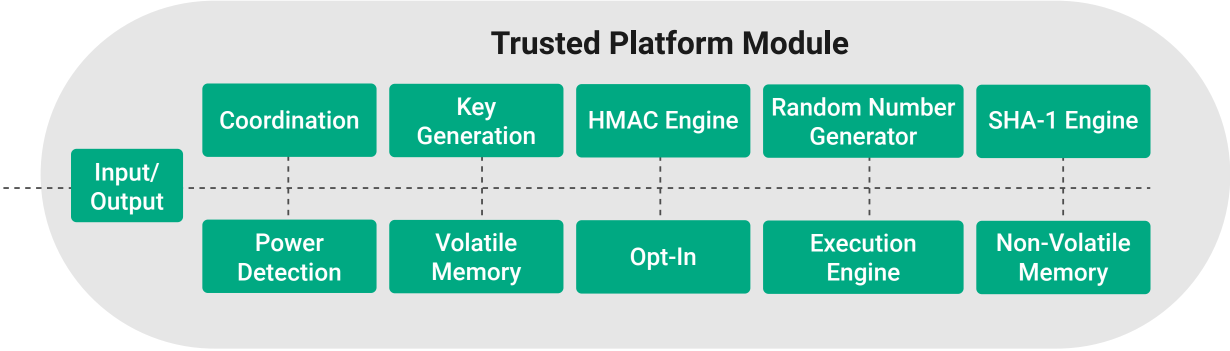

Figure 1: The Trusted Platform Module provides protected, chip-based storage, processing, and encryption tools for use at boot time

As shown in **Figure 1**, a TPM provides a protected environment where secure credentials such as keys, certificates, passwords, and so forth can be generated, stored, and used securely outside the normal device processing environment. TPM is designed to be highly tamper-resistant, secure, and to provide a silicon-based root of trust to protect against rootkit, firmware, and other pre-boot attack vectors.

On a PC (server or client) a TPM provides secure storage for administrative access and BIOS updates. It also supports drive-level encryption (e.g. Microsoft BitLocker), biometrics data (e.g. Microsoft Windows Hello facial recognition or fingerprint info), and Microsoft's secure boot facility. Thus, a TPM enables and supports low-level, hardware-based security protection against low-level attacks. Microsoft works with all the major chip vendors (AMD, intel, and Qualcomm) to ensure proper integration of TPM functionality at the CPU level. HPE's modern server and HP, Inc.'s client PCs all support TPM 2.0 at a minimum, and offer a solid, protected silicon root of trust to users and organizations.

> HPE's modern server and HP, Inc.'s client PCs all support TPM 2.0 at a minimum, and offer a solid, protected silicon root of trust to users and organizations.

HPE's Trusted Supply Chain

To serve customers with higher-than-normal security requirements and highly secure usage scenarios, HPE operates a Trusted Supply Chain. Users of this supply chain include U.S. federal and public sector consumers who must purchase only U.S.-sourced products with verifiable cyber assurance. Buyers from outside the United States can purchase through this Trusted Supply Chain around the globe (except for China, Taiwan, and India). Security is built directly into this Trusted Supply Chain in two specific ways. First, it's accommodated through additional hardened security features in products themselves. Second, it's supervised by HPE employees who oversee those products during the manufacturing process. HPE employees vet all parts, observe assembly, and make sure packaged devices remain tamper-free until customers accept delivery.

Furthermore, HPE incorporates its own exclusive silicon root of trust that embeds silicon-based security into industry-standard servers, and maintains security controls across the entire supply chain to establish and maintain stringent security at the hardware level. HPE's hardening techniques include UEFI secure boot, a reduced attack surface, tamper-proofing at the silicon level, embedded alarms in systems, and physical locks.

Visit the HPE Security Solutions page to learn more about HPE's baked-in, end-to-end security through its silicon root of trust, TPM, Trusted Supply Chain capabilities, and more.