Hewlett Packard
Enterprise

HPE Secure Compute Lifecycle: Building on the world’s most secure industry standard servers to optimize your security environment

Technical white paper

Contents

Introduction

Securing your company's networking and compute infrastructure is critical, given the ever-increasing threats to data and resources. Cyber attacks 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.

Statistics abound with data and predictions for the cost of protecting assets, detecting vulnerabilities, and recovering from security incidents. For example, according to a 2016 global study of 237 companies in seven countries conducted by the Ponemon Institute, [1] the annualized average cost to detect, respond to, and mitigate a breach was around $9.5 million for each company in the study. A 2016 study by Cybersecurity Ventures[2] predicts that global annual cybercrime costs (including damage and destruction of data, lost productivity, disruption to business, forensic investigation, restoration, and so on) will grow from $3 trillion in 2015 to $6 trillion annually by 2021.

Even though there is strong financial incentive to prevent attacks, it is no easy task to secure your infrastructure. Attack 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 attack surfaces are being "hardened" to defend against cyber attacks. For example, manufacturers of software applications, hypervisors, and operating systems are each improving their systems to prevent cyber attacks. In response, attackers are increasingly focusing on lower-level attacks, including attacks on the firmware. Firmware is becoming a more frequent target for denial of service (DOS) attacks since the firmware code operates in a privileged position and if compromised, can go for months without being detected. Thus, protecting networks only at the perimeter firewall level or servers at the software and OS level is no longer sufficient to provide adequate protection against security threats.

Hewlett Packard Enterprise (HPE) is proactively improving its security stance to meet challenges such as attacks on firmware by continually improving the hardware and firmware security of its server platforms and related infrastructure hardware —ensuring that every link in the chain of security provides the most effective cyber security protections possible. The world's most secure industry standard servers incorporate enhanced security capabilities throughout the HPE Gen10 platforms, including ProLiant, BladeSystem C-Class, Apollo, and Synergy, giving customers the best possible protection for their data centers and private clouds.

For more information about security threats and a general understanding of HPE's strategy related to security, refer to the HPE security website at hpe.com/security.

Overview: Building on the world's most secure industry standard servers

With HPE Gen10 Servers, HPE offers the first industry standard servers to include a silicon root of trust built into the hardware. This new silicon root of trust allows firmware to be scanned and monitored through a series of integrity checks that initiate from an immutable link embedded in silicon. Because the chain of trust is established and maintained from the immutable silicon hardware itself, customers can be confident that it is secure. Furthermore, HPE has engineered the Gen10 servers with the ability to recover to a known good state in the unlikely event that firmware becomes compromised in some way. From this silicon root of trust, to specific networking and storage options, and rack infrastructure, HPE has built in security features that help you prevent, detect, and recover from cyber attacks.

This white paper discusses the following recommended servers, licenses, components, and capabilities that will allow you to enhance the world's most secure industry standard servers and optimize them for your infrastructure environment, including networking, storage, rack cabinets, and other options:

- HPE Gen10 server with the powerful Integrated Lights Out (iLO5) server management controller made by HPE, which provides the silicon root of trust, ability to scan and monitor the chain of trust, and provide secure recovery. HPE Gen10 servers that include the iLO5 controller are ProLiant, BladeSystem C-Class, Apollo, and Synergy servers.
  - The iLO Advanced Premium Security Edition license that offers the highest level of commercial encryption capabilities, continual runtime detection of firmware validity, secure erase of the iLO5 NAND/NOR memory,, and secure recovery to authenticated states.
  - HPE offers Gen10 servers that are compliant with the Trade Agreement Act (TAA) of 1979 (19 U.S.C. §§ 2501-2581). Customers can order these unique TAA-compliant SKUs for HPE Gen10 ProLiant, Apollo, or Synergy servers. It's important to understand that while TAA is not a direct indication of cyber security; some organizations may prefer to purchase servers using the TAA-compliant SKUs.

[1] https://ssl.www8.hp.com/ww/en/secure/pdf/4aa5-5207enw.pdf , "2015 Cost of Cyber Crime Study: Global" The study was independently conducted by the Ponemon Institute, although sponsored by Hewlett Packard Enterprise.
[2] http://cybersecurityventures.com/hackerpocalypse-cybercrime-report-2016/

- HPE server options and management solutions:
  - 10 Gb and 25 Gb networking adapters that include a root of trust, device-level firewalls, UEFI secure boot, and audit logs for traceability of changes. In addition, new features to proactively protect the networking traffic with packet inspection and capture are being added to the portfolio.
  - Smart Array Controllers with Secure Encryption licenses to protect data at rest on attached storage devices. Unlike vendors that provide only self-encrypting drives, which often limits the number of protected drives, HPE offers controller-based encryption, so that all attached SAS and SATA drives are encrypted. This is a more cost-effective and comprehensive encryption solution for data at rest.
  - Enterprise Secure Key Manager (ESKM), a key management solution that works with Secure Encryption to provide centralized control and audit records for encryption keys. ESKM is FIPS 140-2 Level 2 validated and Common Criteria certified.
  - HPE SATA Solid State Drives (SSDs) and Hard Disk Drives (HDDs) that include digitally signed firmware to ensure valid operations. HPE SSDs can use a Sanitize Block Erase algorithm and HPE HDDs use Sanitize Overwrite, which both meet the requirements of the *NIST Guidelines for Media Sanitization*, NIST 800-88r1, to erase data when a drive reaches end-of-life.
- Addition of other secure components inside the server chassis, such as:
  - Chassis Intrusion Detection Switch that detects if the chassis hood has been opened or closed and can send an alert through the iLO5 management device. The switch is factory installed and provides assurance that no one has tampered with the server chassis at any time after production. For example, through the logistics supply chain of shipping, distribution and transportation, warehousing, receiving, and inventorying at resellers or other locations, including the end-user customer location.
  - Trusted Platform Module (TPM) securely stores information needed to authenticate the server platform and to enable a measured boot process for the OS, which monitors the OS initialization process to see if the OS startup has been compromised. TPM also supports specific capabilities such as Microsoft Windows BitLocker Drive Encryption. HPE offers both TPM 1.2 and 2.0 to support various operating systems. .
- HPE G2 Advanced or Enterprise racks that let you add third-party security hardware solutions easily, so you can set up two- or even three-factor authentication in your data center with solutions such as RFID readers and biometric solutions, thus enabling you to implement the most secure options in the industry. The G2 Advanced or Enterprise racks also have modified side panels that help reduce the risk of unauthorized access from an adjacent rack.
- HPE Power Distribution Unit (PDU) sensors that provide intrusion detection monitoring of the rack. If any unauthorized user opens the rack cabinet without the proper credentials, the HPE PDU products can send alerts notifying administrators of the intrusion. No other server OEM provides this level of detection alerts on their rack cabinets.
- Top of rack switches such as the Arista 7000 series that include the Extensible Operating System (EOS), which automates the insertion of security services and includes Data Analysis (DANZ) security monitoring tools for end-to-end monitoring.

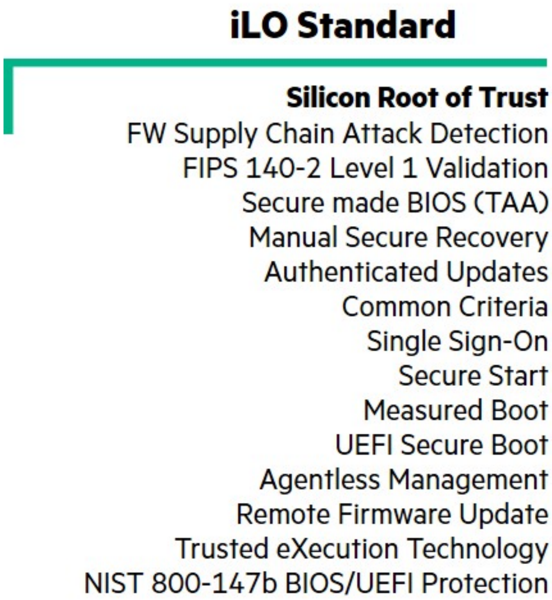
HPE Gen10 servers and iLO5 made by HPE

HPE builds the Gen10 servers with some of the industry's most advanced security capabilities, out of the box, with the foundation being the fifth-generation iLO management chipset (iLO5). The iLO chipset, included in HPE servers for years, provides secure out-of-band management functionality regardless of the server hardware or OS status, and it is available whenever the server is connected to a power source, even if the server main power switch is in the Off position. Because iLO is so powerful, HPE has designed iLO to ensure that its functionality is protected against unauthorized users. It offers strong authentication, highly configurable user privileges with strong authorization processes, and encryption of data, keystrokes, and security keys.

With HPE Gen10 servers, the iLO5 chipset provides an unprecedented level of hardware security with its silicon root of trust. The silicon root of trust:

- Is based in the silicon hardware itself.
- Is impossible to alter.
- Enables the system to authenticate the firmware as far back in the supply chain as possible.
- Provides a secure startup process and, most importantly, provides firmware runtime validation and secure recovery in the unlikely event of a security breach.

Figure 1 shows the security capabilities that iLO5 provides in all HPE Gen10 servers, without any additional licenses or options. This is not a comprehensive list of security capabilities or other iLO5 capabilities. See the documents listed in the Resources, contacts, or additional links section for more detailed information about iLO5.



iLO Standard

Silicon Root of Trust
FW Supply Chain Attack Detection
FIPS 140-2 Level 1 Validation
Secure made BIOS (TAA)
Manual Secure Recovery
Authenticated Updates
Common Criteria
Single Sign-On
Secure Start
Measured Boot
UEFI Secure Boot
Agentless Management
Remote Firmware Update
Trusted eXecution Technology
NIST 800-147b BIOS/UEFI Protection

Figure 1. Standard iLO5 functionality without any optional licenses. (Not a comprehensive list.)

Silicon root of trust and firmware protection

Roots of trust, as defined by the National Institute of Standards and Technology (NIST), are "highly reliable hardware, firmware, and software components that perform specific, critical security functions. [3]" A root of trust is a component that measures or verifies certain security-related functions, and because it can be trusted, it provides the ability to test and verify other security-related functions that depend on it.

Prior to the release of HPE Gen10 servers, the iLO4 management chipset would act as a root of trust (based in firmware), which helped protect the UEFI (BIOS) and OS from attacks by performing two types of signature checking of the iLO firmware image:

- First, it would authenticate any new firmware image before it could be programmed into the iLO ROM. This would require iLO authentication and authorization, including optional two-factor authentication.
- Second, iLO would verify the integrity of the firmware image before executing it. Because the iLO chipset is the first device initialized on the server, the server could not boot without it. As the server booted, each piece of the iLO firmware image would have its signature validated before it could execute. Subsequent pieces were checked by previous ones, until iLO was fully booted.

Why change this process, which was already quite secure? Quite simply, because as cyber security threats continue to evolve, HPE is increasingly hardening our server infrastructure to stay ahead of those threats. As operating systems, applications, and hypervisors become more secure by reducing the attack surface, the firmware becomes an increasingly attractive target. Because the firmware always loads over a million lines of code before the OS even boots, the firmware and BIOS must be protected. Only a few lines of corrupt code hidden among those millions of code lines could permanently brick a server. An unauthorized driver or malware with kernel privileges could create a permanent denial of service (PDOS) attack by corrupting the data or devices required for proper booting and operation of the server. Regardless of how good your other tools are, such as network perimeter firewalls, anti-virus scanning, or security information and event management (SIEM) tools, those capabilities operate at the data plane level, and never scan at the firmware level. If someone can access the server through unsecured firmware, they can create a PDOS and render the server useless.

[3] http://csrc.nist.gov/projects/root-trust/ Hardware Roots of Trust, Overview

To protect against this, the iLO5 chipset within HPE Gen10 servers has a silicon root of trust. The iLO5 chipset provides an inextricably tied link between the silicon and firmware—making it impossible to insert any malware, virus, or compromised code that would corrupt the boot process. Now, rather than the iLO firmware checking the integrity of the firmware every time it boots, the iLO5 hardware determines whether to execute the iLO firmware (see Figure 2).

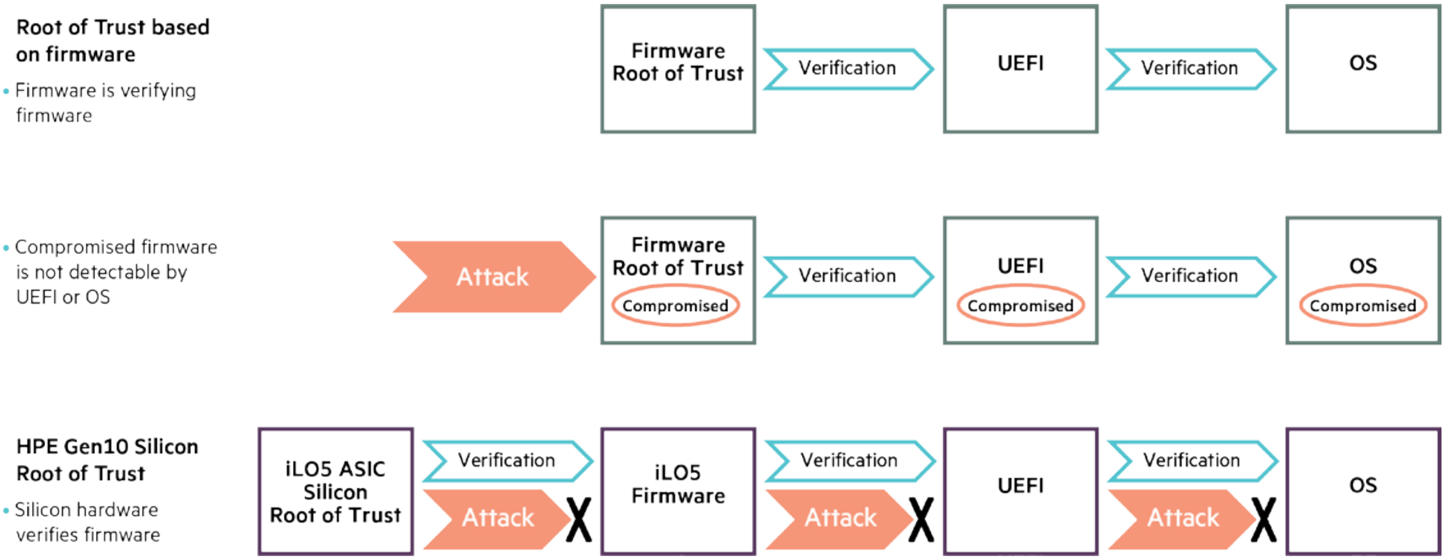


Figure 2. The HPE silicon root of trust moves the integrity and verification as far back in production as possible, protecting against security breaches even before HPE manufactures the server.

Silicon root of trust and the supply chain

Because the silicon root of trust is embedded in the hardware itself, iLO5 is able to detect any compromised firmware—as far back as the supply chain process. HPE can address platform security all the way back to the supply chain because HPE designs the iLO5 entirely—hardware and firmware—and controls the iLO5 production process. Unlike other companies, HPE does not outsource the server management controller. HPE also has strict internal processes that dictate the firmware approval process. This gives customers an unprecedented level of assurance that no hackers have compromised the firmware before the customers receive their server.

Silicon root of trust and firmware runtime validation enablements

The silicon root of trust enables other critical capabilities as well:

- Secure Start and Manual Recovery
- Authenticated updates

Secure Start and Manual Recovery

The silicon root of trust enables the boot process to provide a Secure Start. When the system boots, iLO5 validates and boots its own firmware first, then validates the system BIOS. Because the silicon root of trust is inextricably tied into the iLO5 hardware, every validated signature throughout the boot process can be trusted. However, in the unlikely event that iLO5 finds tampering or corruption at any point in the process, trusted firmware is immediately available for Secure Recovery.

First, if iLO5 finds that its own firmware has been compromised, it will load its own authenticated firmware from an integrated backup. The iLO5 firmware recovery is always available and always automatic—regardless of license. Remember that the silicon root of trust in hardware is how the iLO5 firmware is verified, so it can always be trusted.

Second, if iLO5 finds that the system BIOS has been compromised, iLO5 will try to recover it from a backup copy. If the backup copy is also compromised, iLO5 will alert the customer that the system BIOS is compromised. By default with iLO standard, customers can connect to iLO5 and manually recover to authenticated firmware. Customers have the option for iLO5 to automatically recover authentic firmware if they upgrade to the iLO Advanced Premium Security Edition license.

The silicon root of trust is the foundation for the entire Secure Start and Manual Recovery process, enabling Gen10 servers to be the world's most secure industry standard servers and providing the extraordinary ability to verify the digital signatures up through the entire boot process.

Authenticated firmware updates

The iLO5 chipset expands the number of firmware items that customers can update directly and securely in the Gen10 servers, including CPLDs (complex programmable logic devices), PowerPIC (ProLiant power interface control utility) firmware, the Intel innovation Engine and Management Engine, and other low-level system components.

It also contains a firmware repository on the iLO5 non-volatile flash memory (NAND), which allows components such as the Service Pack for ProLiant (SPP) to be applied and installed offline through iLO5. The NAND flash contains the known good recovery image, so that if for any reason firmware becomes compromised, iLO5 can recover by reverting to its verified image stored in the NAND flash.

UEFI Secure Boot

HPE Gen10 servers have the ability to boot from legacy BIOS or from UEFI. To have the most robust server security, HPE recommends using UEFI rather than legacy BIOS.

UEFI Secure Boot ensures that only firmware components, UEFI applications, and operating system bootloaders that have appropriate digital signatures, and verify as authentic, can execute during the boot process. Secure Boot differs from Secure Start in that it checks additional firmware beyond the iLO5 and UEFI firmware, including third-party modules that may be present.

Secure Boot ensures that each component launched during the boot process is digitally signed and that the signature is validated against a set of trusted certificates embedded in the UEFI BIOS. Secure Boot validates the software identity of the following components in the boot process:

- UEFI drivers loaded from PCIe cards
- UEFI drivers loaded from mass storage devices
- Pre-boot UEFI shell applications
- OS UEFI boot loaders

HPE servers, starting with the Gen9 family, significantly enhanced the standard UEFI Secure Boot process with additional functions including the secure firmware update via iLO, secure NVRAM storage, and management of the Secure Boot process through iLO. For more information about the differences between UEFI and legacy BIOS, see *UEFI, successor to legacy BIOS*, document number 4AA5-1111ENW.

Compliance with security industry standards and encryption protocols

HPE Gen10 servers comply with multiple security standards and encryption protocols, including Federal Information Processing Standard (FIPS) Publication 140-2, the National Institute of Standards and Technology (NIST) 800-147b, the payment card industry data security standard (PCI DSS), and Common Criteria.

FIPS 140-2 Level 1

FIPS is a set of standards mandated for use by United States government agencies and contractors. The cryptographic module in HPE iLO5 firmware is in the process of achieving FIPS 140–2 Level 1 validation. (Both the iLO3 and the iLO4 devices were FIPS 140-2 Level 1 validated.)

The iLO5 chipset in HPE Gen10 servers allows you to operate in FIPS 140-2 Mode, which is one of the four possible iLO5 security modes. It is the next highest security setting compared to CNSA mode; FIPS mode mandates high-grade encryption ciphers and closes down insecure interfaces and ciphers that will not meet CNSA government standards. The section titled Understanding Gen10 security modes and potential consequences describes this more fully.

NIST 800-147b BIOS protection guidelines

HPE Gen10 servers fully comply with the NIST 800-147b guidelines, *BIOS Protection Guidelines for Servers*, which describe methods for protecting server BIOS components. Both the legacy BIOS and the UEFI firmware comply with this NIST standard. The guidelines support secure update mechanisms including:

- Authenticated BIOS update mechanisms, where digital signatures prevent the execution of BIOS update images that are not authentic.
- Firmware integrity protections, to prevent unintended or malicious modification of the BIOS outside the authenticated BIOS update process.
- Non-bypassability features, to ensure that there are no mechanisms that allow the main processor or any other system component to bypass the BIOS protections.

Payment Card Industry Standards

The Payment Card Industry Data Security Standard (PCI DSS) is a broadly accepted set of policies and procedures designed to protect the safety of credit, debit, and cash card transactions and protect cardholders against misuse of their personal information. The PCI DSS set the operational and technical requirements for organizations accepting or processing payment transactions, and for software developers and manufacturers of applications and devices used in those transactions. See pcisecuritystandards.org/pci_security/ for more information.

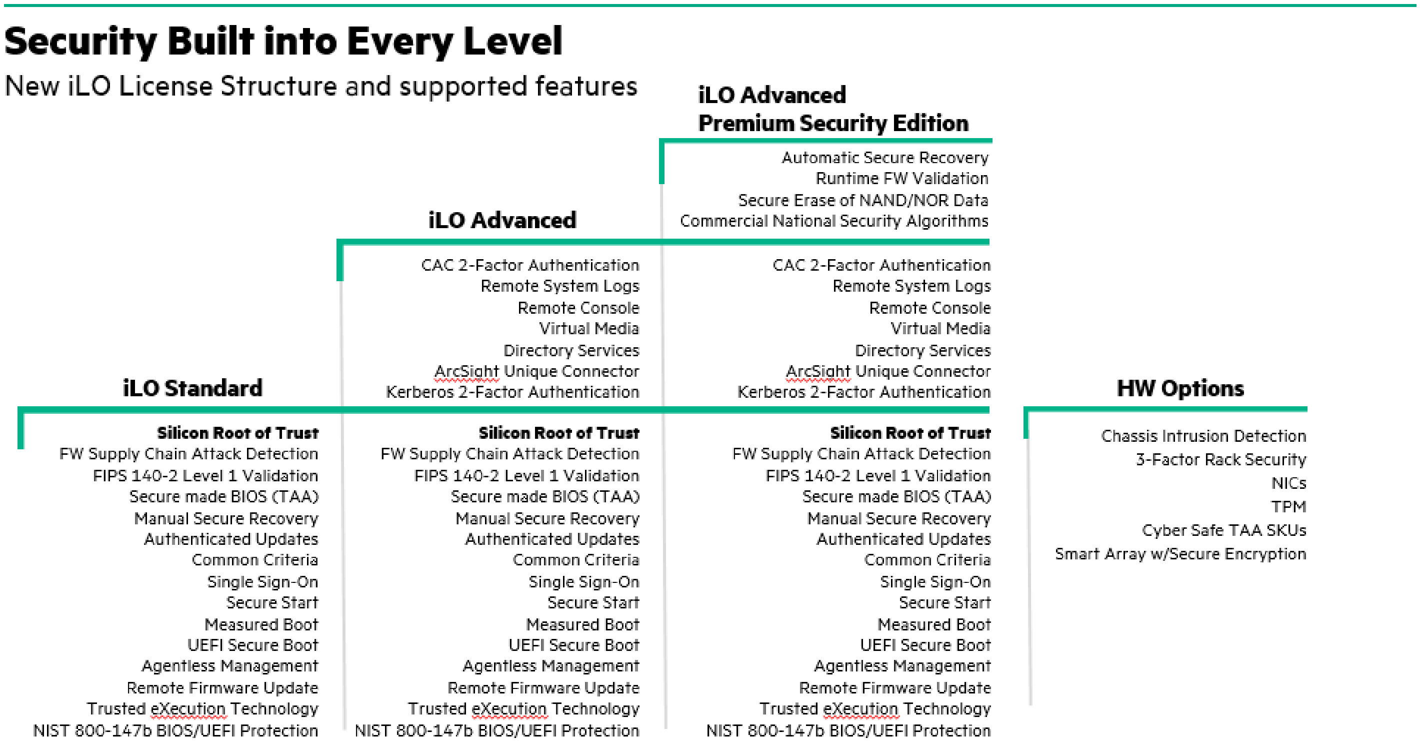
Common Criteria

HPE supports the objectives of the National Information Assurance Partnership (NIAP) Common Criteria (CC) certification standard. CC is a set of guidelines and specifications developed for evaluating information security products, specifically to meet security standards for government deployments. HPE is committed to taking many of our server, storage, and networking products through the lengthy, demanding, and costly CC certification process to ensure that the products meet the cyber security demands of our government customers. This also delivers greater security benefit to our commercial customers. For example, as of this writing, HPE is taking the iLO5 chipset from Gen10 servers and a set of ProLiant Gen10 C-Class blades through a Common Criteria certification as well as the FIPS 140-2 validation. HPE will continue to pursue these certifications for additional products to give our customers confidence in HPE's ability to deliver the most secure servers in the market.

Extended capabilities with iLO licenses

Depending on a customer's need for security, iLO5 security capabilities can be extended with the iLO Advanced license or the iLO Advanced Premium Security Edition license. HPE recommends the iLO Advanced Premium Security Edition license to enable the most security features and highest-level encryption capabilities.

Figure 3 shows some, not all, of the most important iLO5 capabilities with the Advanced licenses. It is important to recognize that iLO Advanced Premium Security Edition includes the features of iLO Advanced, but a customer need not buy both those licenses. A customer would upgrade to either iLO Advanced or iLO Advanced Premium Security Edition.



Security Built into Every Level

New iLO License Structure and supported features

iLO Standard

Silicon Root of Trust
FW Supply Chain Attack Detection
FIPS 140-2 Level 1 Validation
Secure made BIOS (TAA)
Manual Secure Recovery
Authenticated Updates
Common Criteria
Single Sign-On
Secure Start
Measured Boot
UEFI Secure Boot
Agentless Management
Remote Firmware Update
Trusted eXecution Technology
NIST 800-147b BIOS/UEFI Protection

iLO Advanced

CAC 2-Factor Authentication
Remote System Logs
Remote Console
Virtual Media
Directory Services
ArcSight Unique Connector
Kerberos 2-Factor Authentication

Silicon Root of Trust
FW Supply Chain Attack Detection
FIPS 140-2 Level 1 Validation
Secure made BIOS (TAA)
Manual Secure Recovery
Authenticated Updates
Common Criteria
Single Sign-On
Secure Start
Measured Boot
UEFI Secure Boot
Agentless Management
Remote Firmware Update
Trusted eXecution Technology
NIST 800-147b BIOS/UEFI Protection

iLO Advanced Premium Security Edition

Automatic Secure Recovery
Runtime FW Validation
Secure Erase of NAND/NOR Data
Commercial National Security Algorithms

CAC 2-Factor Authentication
Remote System Logs
Remote Console
Virtual Media
Directory Services
ArcSight Unique Connector
Kerberos 2-Factor Authentication

Silicon Root of Trust
FW Supply Chain Attack Detection
FIPS 140-2 Level 1 Validation
Secure made BIOS (TAA)
Manual Secure Recovery
Authenticated Updates
Common Criteria
Single Sign-On
Secure Start
Measured Boot
UEFI Secure Boot
Agentless Management
Remote Firmware Update
Trusted eXecution Technology
NIST 800-147b BIOS/UEFI Protection

HW Options

Chassis Intrusion Detection
3-Factor Rack Security
NICs
TPM
Cyber Safe TAA SKUs
Smart Array w/Secure Encryption

Figure 3. Upgrade path from iLO Standard to either iLO Advanced or Advanced Premium Security Edition Licenses. (Not a comprehensive list of the security-related capabilities.)

iLO Advanced Premium Security Edition

The iLO Advanced Premium Security Edition provides the highest-level commercial-grade encryption ciphers when in the CNSA mode. This is especially important for government contractors and agencies. This license enables a Secure Start capability with automatic recovery and continual runtime verification of iLO5 and UEFI firmware. It also lets customers securely and confidently redeploy servers, through its secure erase of the non-volatile memory in the iLO5 chipset.

CNSA

In addition to the security standards already mentioned, the HPE Gen10 servers also support the highest-level cryptographic standard available for commercial use, the Commercial National Security Algorithm Suite (CNSA).

CNSA is a suite of cryptographic algorithms approved for use by the US National Security Agency for protecting secret and top secret information with the U.S. government, and is the highest-level cryptographic algorithm available for commercial systems. CNSA replaces the previous National Security Agency (NSA) Suite B algorithms.

CNSA mode is one of the four iLO5 security modes. It requires the user to enable FIPS mode first, then enable the CNSA mode (see the Understanding Gen10 security modes and potential consequences section for more information).

Automatic Secure Recovery

As described previously, the silicon root of trust enables the Secure Start process. As the system boots and iLO5 verifies the series of digital signatures, iLO5 can access trusted firmware immediately and recover to a known good state if it finds tampering or corruption in its own firmware or the system BIOS.

First, if iLO5 finds that its own firmware has been compromised, it will load its own authenticated firmware from an integrated backup. The Secure Recovery of iLO5 firmware is always available and always automatic—regardless of license. Remember that iLO5 firmware can always be trusted because it is verified using the silicon root of trust in hardware.

Second, if iLO5 finds that the system BIOS has been compromised, iLO5 will try to recover from a backup copy. If the backup copy is also compromised and the customer has upgraded to the iLO Advanced Premium Security Edition license, iLO5 can automatically recover authentic firmware.

The silicon root of trust is the foundation for the entire Secure State and Secure Recovery process, enabling Gen10 servers to be the world's most secure industry standard servers and providing the extraordinary ability to not only verify the digital signatures up through the entire boot process but also to recover securely if any firmware is compromised.

Runtime firmware validation

With the iLO Advanced Premium Security License, the iLO5 chipset enables runtime validation of firmware. The iLO5 chipset performs the same checking process that happens during the boot process on a continual basis while the server is running. As frequently as once a day, iLO5—with its silicon root of trust—runs a background verification check on the iLO5 firmware and the UEFI BIOS. The user can select the number of days between scans. This gives customers a distinct advantage in knowing quickly if an attacker has compromised their firmware and gets the customer back on the road to recovery quickly. The process can be fully trusted, because it is rooted in hardware at the silicon fabrication facility.

Secure Erase of NAND/NOR memory

Customers needing to redeploy a server can do so confidently with the Secure Erase of the 4 GB of non-volatile memory stored on the iLO5 chipset. The iLO5 chipset erases all data in this non-volatile memory—including Active Health System logs, Intelligent Provisioning data, and iLO5 configuration settings—by making multiple passes and scrambling binary bits. This process exceeds the requirements of *NIST Guidelines for Media Sanitization*, NIST 800-88r1 (http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-88r1.pdf).

iLO Advanced

Two-factor authentication

Two-factor authentication (something you have and something you know) can be enabled when using the iLO Advanced License, using either Kerberos or Common Access Card (CAC) protocols.

HPE implemented two-factor Kerberos authentication in the HPE Gen9 servers and continues it in the Gen10 servers. Kerberos is an authentication protocol that uses a trusted third party to authenticate between a client and a host server. This avoids the need to store passwords locally or to send them over the Internet. It allows users to log in once and navigate between servers without the need to log in again.

To meet more stringent requirements such as those for U.S. Defense Information Systems Agency (DISA) and the U.S. National Security Agency (NSA), the HPE Gen10 servers support Common Access Card (CAC) two-factor authentication. A CAC is a smart card used for identifying military personnel, U.S. Department of Defense (DoD) employees and contractor personnel. It leverages a Public Key Infrastructure (PKI) Security Certificate to verify a cardholder's identity prior to allowing access to protected resources. If the user's identity is not verified, the Gen10 server will deny that user's access to the iLO5 interface. Customers that wish to use two-factor CAC authentication to access iLO5 must have a CAC reader built-in or attached to their administrator laptop or desktop.

Security information and event management integration

The best security organizations today take advantage of integrated and powerful analytics using security information and event management (SIEM) tools to provide log management, alerting, rapid detection, and real-time analysis of threats. HPE Gen10 servers with iLO Advanced or Advanced Premium Security licenses support SIEM integration with tools such as ArcSight or Splunk Enterprise.

ArcSight is building a connector for our iLO firmware that will allow ArcSight to gather data and logs directly from iLO5, allowing them to better conduct scans and look for anomalies that might be security breaches. Splunk can integrate SysLog input from iLO5 into their log management systems. For an example of how you can use Splunk with HPE servers to provide this important operational intelligence, see the architecture guide *Splunk Enterprise powered by HPE Moonshot and HPE ProLiant DL360 Gen9 Servers* at https://www.hpe.com/h20195/v2/GetPDF.aspx/4AA6-5306ENW.pdf

Physical platform security additions

To further enhance the world's most secure industry standard servers, in addition to enabling the iLO Advanced or iLO Advanced Premium Security License, customers should consider adding one or more of the following options, depending on their needs.

HPE Gen10 servers support the following additional physical security options:

- Trusted Platform Module (TPM) 1.2 and 2.0□

Trusted Platform Modules are computer chips that securely store passwords, certificates, or encryption keys, which are used to authenticate the platform and validate software. TPM modules are also used with a measured boot process for the OS, which monitors the OS initialization process to see if the OS startup has been compromised. Having a TPM is required for some Microsoft Windows features to be enabled, such as BitLocker Drive Encryption.

HPE supports TPM 1.2 and 2.0. TPM 1.2 works with any Linux OS and Microsoft Windows Server 2012 and 2012r2. TPM 2.0 works with any Linux OS and Microsoft Windows Server 2016. TPM 2.0 has several advantages over TPM 1.2, including a flexible algorithm, enhanced authorization, simplified provisioning, and internally protected assets using symmetric algorithms.

- Chassis intrusion detection

  Select HPE Gen10 servers include an option for a chassis intrusion detection switch, which detects if the chassis hood is opened or closed at any time after installation at the factory. The iLO5 management processor monitors the battery-operated switch and if there is a change (if the hood is either opened or closed), it creates a log entry noting the intrusion. Because the switch is factory installed and battery-operated, it can provide notifications for any change in status throughout the logistics supply chain of shipping, distribution, warehousing, and receiving; and it can be configured for various alerting mechanisms (Remote SysLog, SNMP, alertmail, etc.).

Customers should also consider the option to purchase specific HPE Gen10 servers that are TAA compliant. While TAA is not a direct indication of cyber security, some organizations may prefer to purchase servers using the TAA-compliant SKUs. Customers can order these unique SKUs for HPE Gen10 ProLiant, Apollo, or Synergy servers. HPE Gen10 server SKUs that are TAA compliant provide customers with the assurance that the major transformation of the server firmware and hardware has occurred within the United States or in a signatory country designated as TAA compliant.

Gen10 networking and storage options optimized for security

In addition to the security embedded within the HPE Gen10 server platforms that makes them the most secure industry standard servers in the world, HPE maximizes your opportunity to build out a completely hardened infrastructure by offering hardened and robust security solutions in networking and storage options, racks, and rack options such as PDUs.

Network adapters

Because network connections are frequent points of attack, both inside and outside the firewall, it is critical that customers optimize their security stance on all network devices, including the network adapters inside the server box.

A broad variety of Ethernet adapters (NICs) are available for Gen10 servers. Depending on vendor and family series, the NIC security features include capabilities such as a root of trust (in hardware or firmware) to enable secure bootup, sanitization capabilities for secure erase of data, device-level firewalls, packet inspection, and hardware authentication capabilities. Customers will want to select NIC adapters that meet their specific requirements and supply as many of these features as possible (see Table 1).

Table 1. Networking Security Features and Benefits for HPE Gen10 Servers

	Protect	Detect	Recover
FEATURES	**NIC root of trust/Chain of trust** **Authenticated updates**	**UEFI Secure boot** **Device-level firewall** **Packet inspection**	**Audit logs** **Sanitization**
BENEFITS	Root of trust • Enables a chain of trust for authenticating updates to firmware via signature validation. • Helps block installation of rogue, compromised, or corrupted firmware. • Ensures that the executing firmware is trusted.	UEFI Secure boot • Safeguards the system and ensures that no rogue drivers are executing on startup.	Audit logs • Captures notifications about firmware changes into system logs • Provides traceability for authenticated firmware updates
	Authenticated Updates • Stores the cryptographic keys on the NIC itself to protect user and configuration	Device-level firewall • Blocks unmanaged access to memory or storage.	Sanitization (Secure User Data Erase) • Renders user and configuration data on the NIC irretrievable so that NICs can be safely redeployed or disposed.

Table 1. Networking Security Features and Benefits for HPE Gen10 Servers

	Protect	Detect	Recover
FEATURES	**NIC root of trust/Chain of trust** **Authenticated updates**	**UEFI Secure boot** **Device-level firewall** **Packet inspection**	**Audit logs** **Sanitization**
	data from unauthorized access and allows signed firmware updates.	• Ensures that only authorized agents can access on-device firmware and configuration data.	
		Packet Inspection • Blocks or rate-limits packets based on packet headers and contents. • Filtering behavior is configurable by user. • Allows DDoS attacks by "bad" traffic to be absorbed without degrading benign traffic.	

Root of trust and digitally signed firmware

HPE works diligently with its vendors to provide customers with a highly secure chain of trust and authenticated digital signatures to ensure that only validated firmware is loaded.

The HPE Server Networking portfolio offers a broad line of Ethernet adapters for Gen10 servers:

- 1 Gb/10 Gb Standard series
- 10 Gb Advanced series
- 25 Gb Performance series

As shown in Table 2, by choosing the highest performance 25 Gb Performance adapters, you will be assured of having a solid chain of trust that can confirm the validity of firmware. Depending on vendor and family product series, some NIC adapters have a root of trust based on firmware, while others have the most secure, root of trust based on hardware.

Table 2. Gen10 Security Capability by NIC Adapter Product Series.

Security Capability	1Gb/10Gb Standard Series	10 Gb Advanced Series	25 Gb Performance Series
Root of Trust - Hardware	Select Adapters	Select Adapters	✓
Root of Trust - Firmware	Select Adapters	✓	✓
Hardware Authentication	X	Select Adapters	Select Adapters
Signed Firmware	✓	✓	✓
UEFI Secure Boot	✓	✓	✓
Audit Logs	Select Adapters	✓	✓
Sanitization/Secure User Data Erase	X	Select Adapters	✓
Device-Level Firewall	Mix of support	✓	✓

Cells indicating a mix of support vary from one vendor to another. Please check individual adapter Quick Specs for specific features: https://www.hpe.com/us/en/product-catalog/servers/server-adapters.hits-12.html

Packet inspection—the next level of networking security

The NIC can protect the server in a variety of methods, as described in Table 1. HPE network adapter will also support packet inspection, which can be very useful for blocking malicious traffic and potentially stopping DDoS attacks. Each NIC has its own specific implementation to create "firewalls" against bad networking traffic and has adapters available for HPE ProLiant servers as a next level of security.

NICs that include packet inspection use a software programmable system-on-chip (SoC) implementation that does more than a standard L2 NIC. A filter engine uses a pseudo-microcode instruction set to configure the filter engine to selectively accept, reject, or rate-limit packets based on packet headers and packet contents. The microcode used for filtering is under user control. Thus, the filtering behavior is highly configurable and customers can customize the filtering for their particular use cases. The packet filtering enables "bad" traffic to be detected very early in the network stack, so DDoS attacks can be absorbed without degradation of "good" traffic. The filter engine is designed to work on large address sets and can scale to configurations with lookups against millions of IP addresses.

HPE will also offer a high performance distributed firewall that is based on a multi-core software-programmable SoC, so that the server can relay the traffic monitoring protection through a fully programmable adapter platform. This includes higher levels of encryption security and is completely programmable with the on-board processor that can be programmed to do whatever the customer wants. This includes OVS (Open v-switch) support that cloud customers require. Firewalls such as this are supported by a feature rich software development kit (SDK) that allows customers and partners to develop high performance applications using market leading IP tables, encapsulation, traffic management/QoS, deep packet inspection, and TCP and SSL processing capability of adapters. NIC adapters that use packet inspection and these high-performance distributed firewalls are ideal for cloud service providers, enterprises, and private data centers worldwide.

Top of rack switches

Since the network is the primary medium that bridges the physical, virtual and cloud environments, network traffic is becoming increasingly recognized for its role in providing an attack surface for malware and threats to enter the enterprise. Many security vendors are increasing their capabilities in analyzing network traffic for threats, anomalies, and lateral movement of malware. However, no matter how sophisticated these security solutions become, they all rely on accurate monitoring of the network traffic.

In the fall of 2016, HPE announced an enhanced strategic partnership with Arista Networks that will advance HPE's strategy to provide secure Hybrid IT solutions built on the industry's leading software-defined data center infrastructure portfolio from Arista. Arista Fixed (top of rack, or ToR) Switches are built specifically for the data center with high performance, high density, fixed configuration, and with wire speed Layer 2 and Layer 3 features. The switches are Common Access Card (CAC, a two factor PKI based authentication mechanism) enabled, FIPS 140-2 validated, and Common Criteria certified.

In addition, the following switches have been tested and approved for use on the DoD Unified Capabilities Approved Products List and Assured Services Local Area Network (ASLAN):

- 7500E Series (7504/7508)
- 7300X Series (7304/7308/7316)
- 7250QX-64
- 7050X Series
- 7150S Series

Arista switches, with their Software Driven Cloud Networking, provide IT and security operations teams with software-driven visibility and control that encompasses automation, services, and comprehensive visibility needed to:

- Maintain an agile and cost-efficient cloud infrastructure for any workload on-demand
- Inspect all east-west traffic for profiled attack patterns with redirect analysis
- Maintain next-generation firewall security rules for all at-risk traffic at any scale, in-line, all the time

Arista CloudVision provides a seamless and consolidated view of the entire cloud infrastructure and provides the foundation for automating integration of next-generation firewalls, security monitoring tools, and application delivery controllers.

This new approach to security device deployment has enabled integration of advanced security into the dynamic network segmentation of the cloud datacenter, by workload and by tenant, without any dependency on proprietary packet headers or protocols. Arista Extensible Operating

System (EOS) software automates the insertion of security services with CloudVision Macro-Segmentation Service (MSSTM) for both physical and virtualized (i.e., P-to-P and P-to-V) workloads anywhere on the network with leading ecosystem of service and security partners including Check Point Software, F5 Networks, Fortinet and Palo Alto Networks.

For security monitoring and traffic analysis, Arista has pioneered the integration of Arista Data ANalyZer (DANZ), for out of band monitoring of any cloud workflow. DANZ allows the datacenter security team to cost effectively scan for vulnerabilities while watching for signs of attack at up to 100 Gbps per link and is widely used in sensitive cloud computing environments today.

Storage encryption and key management

HPE Smart Array SR Secure Encryption is a FIPS 140-2 Level 1 validated, enterprise class controller-based encryption for data-at-rest. It provides customers with a data security solution to comply with regulations such as HIPAA (Health Insurance Portability and Accountability Act) for sensitive data.

A Secure Encryption license enables encryption for data-at-rest for RAID volumes on any bulk storage (e.g., SAS/SATA drives) attached to any P-class or E-class Gen10 Smart Array controllers in HPE Gen10 servers. Only one license is required per server, regardless of number of drives or controllers. The encryption solution can use either local or remote key management methodologies (the encryption keys do not work with TPM, but are stored on the controller card or the ESKM). The remote key management mode requires an iLO Advanced or Advanced Premium Security license and the HPE Enterprise Secure Key Manager (ESKM) hardware appliance with software v3.1 or later. ESKM v5.0 is the current version as of this writing, and all customers are encouraged to upgrade to 5.0 or later for enhanced security and current FIPS validation.

ESKM is a complete key management solution that gives you centralized control and audit records for all encryption keys, protecting your organization against loss, mishandling, and administrative and operational attacks. It is applicable to all HPE servers including NonStop, and broader HPE storage solutions including 3PAR, StoreOnce, XP7, and StoreEver. ESKM is FIPS 140-2 Level 2 validated and Common Criteria certified. It supports both HPE Key Management System (KMS) protocols and the standard KMIP (Key Management Interoperability Protocol). It enables you to protect and ensure continuous access to business-critical, sensitive, data-at-rest encryption keys, both locally and remotely.

More information about ESKM is available from the links in the Resources, contacts, or additional links section of this paper. Table 3 gives an example of appropriate SKUs that customers could use to order the ESKM solution.

Table 3. SKU and description for ESKM solution

Part Number	Description	Security Capability
M6H81AA	Enterprise Secure Key Manager v5 single node server (FIPS 140-2 Level 2 validated)	Hardware-based centralized key management solution for unifying and automating your organization's encryption keys.
Q2F26AAE	HPE Smart Array SR Secure Encryption E-LTU	License for encryption capability integrated into Smart Array controller firmware

Storage drives

HPE SSDs and HDDs include digitally signed firmware that prevents unauthorized and malicious attacks to data, ensuring that drive firmware is authentic and comes from a trusted source.

HPE SSDs are available in three broad categories based on their typical target workloads: Read Intensive, Mixed Use, and Write Intensive. These drives deliver higher performance, reduced latency, and more power-efficient solutions when compared with traditional rotating media. You can also prevent data loss and monitor the SSD life with HPE SmartSSD Wear Gauge compatibility in management tools.

HPE SSDs and HDDs are fully tested and qualified to enable compatibility with HPE ProLiant, HPE Synergy, and HPE BladeSystem solutions. HPE SSDs also offer Sanitize Block Erase while HPE HDDs use Sanitize Overwrite—which both meet the requirements of the *NIST Guidelines for Media Sanitization*, NIST 800-88r1 (http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-88r1.pdf). These algorithms allow customers to erase data when a drive has reached end-of-life.

Network and storage options summary

Table 4 gives some specific examples of network and storage options that you can use to provide the highest levels of security in your server. These particular options are applicable for HPE ProLiant Gen10 servers, but other Gen10 options are available for different form factors such as NIC mezzanine cards for the Synergy servers.

Table 4. Examples of Server Options with Advanced Security features for HPE ProLiant Gen10 Servers.

Options Category	Part Number	Description	Security Capability
Network Adapter	817709-B21	HPE Ethernet 10/25G 2-port 631FLR-SFP28 Adapter	Includes hardware root of trust (certain vendors) or firmware root of trust, secure boot, sanitization, authentication, and device-level firewall
Network Adapter	Q5W13A	Solarflare SFN8522-PLUS DP Adapter	Includes above features as L2 NIC plus programmability with SecureLock packet inspection software licenses
Network Adapter	CN2350-210SVPN-3.0-G	2x 10G (SFP+) PCIe Gen3 x8 Adapter w/ 12-core	Includes all the above features with additional encryption security, IPSEC and is programmable with an on-board processor and includes OVS (Open v-switch)
Storage SSDs	832414-B21	HPE 480GB 6G SATA MU-2 SFF SC SSD (x2)	Includes digitally signed firmware
RAID Controller	804331-B21	HPE Smart Array P408i-a SR Gen10 Controller	Ability to use HPE Smart Array Secure Encryption License
Data-at-rest Encryption	Q2F26AAE	HPE Smart Array SR Secure Encryption E-LTU	License for encryption capability integrated into Smart Array controller firmware

Rack-level hardware infrastructure

It is also important to consider the hardware infrastructure where your secure server resides—from the rack itself to the other components inside the rack, such as power distribution units (PDUs), and KVM switches.

HPE G2 series racks

HPE has redesigned the HPE G2 Advanced and Enterprise series racks to support an industry standard format for the door locks. This means customers can easily remove the locks and replace them with electronic and biometric security solutions from third-party lock vendors. Customers can choose to install two- or even three-factor authentication solutions in their data centers that include keypad locks, RFID readers, and biometric solutions such as fingerprint readers and retinal scanners. While HPE will not be stocking these types of alternative lock solutions, customers can purchased them directly from leading lock vendors. Customers can also order them through HPE Factory Express for integration by HPE's team of integration specialists.

In addition, HPE changed the G2 rack design to include flush-mounted side panels, which allow racks to be bayed together with the side panels intact—reducing the risk of easy access from the side panel of one rack to an adjacent rack by unauthorized personnel.

HPE power distribution units

HPE can also provide increasing levels of physical security through external sensors available with the PDUs.

Advanced PDUs from HPE include a 1 Gb Ethernet connection that allows you to connect the management card inside the PDU to your network to transmit alerts. Customers can configure the alerts to transmit using SNMPv1 or the more secure SNMPv3. Customers can purchase rack intrusion sensors that plug into the PDU (see Figure 4) and send alerts to IT administrators if anyone opens the front or back door of the rack.

HPE KVM switches

HPE provides additional local and remote access security through the HPE IP Console Switch G2. The HPE IP Console Switch G2 with VM and Server Console Switch G2 with VM integrated keyboard, video, and mouse (KVM) capabilities come with Common Access Card (CAC) support, which is a key component in managing data centers that require two-factor authentication. CAC, backed by AES encryption, helps protect your business-critical data.

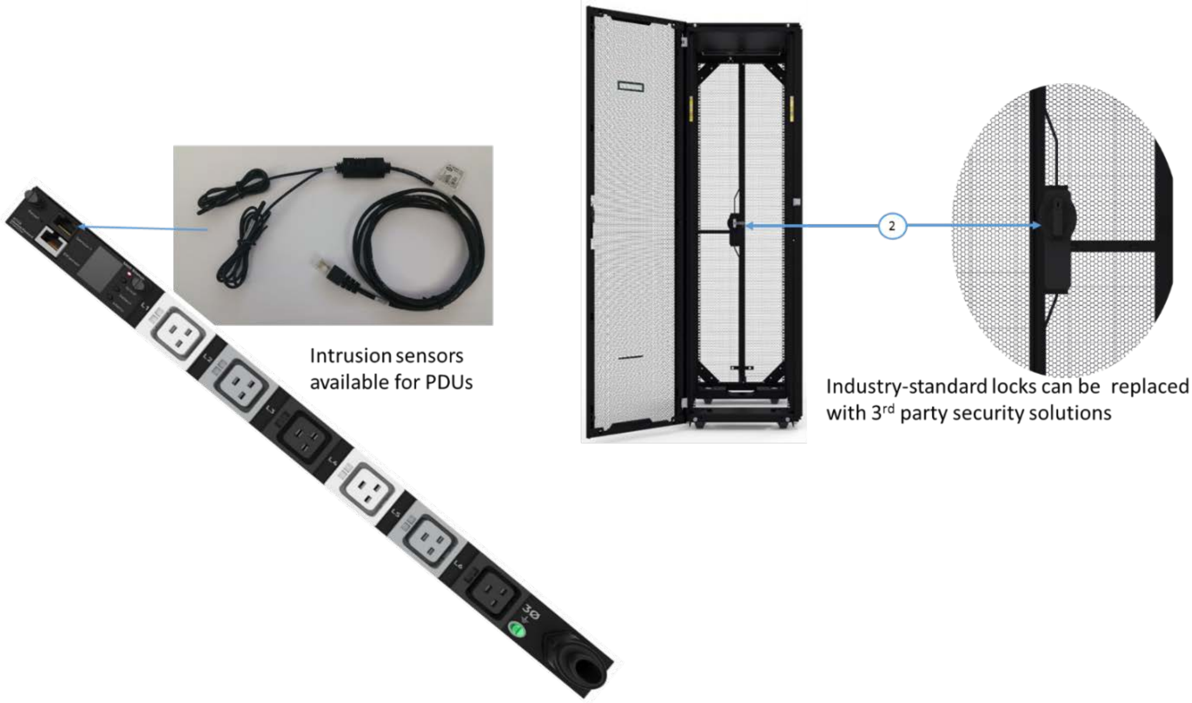

Intrusion sensors available for PDUs
2
Industry-standard locks can be replaced with 3rd party security solutions

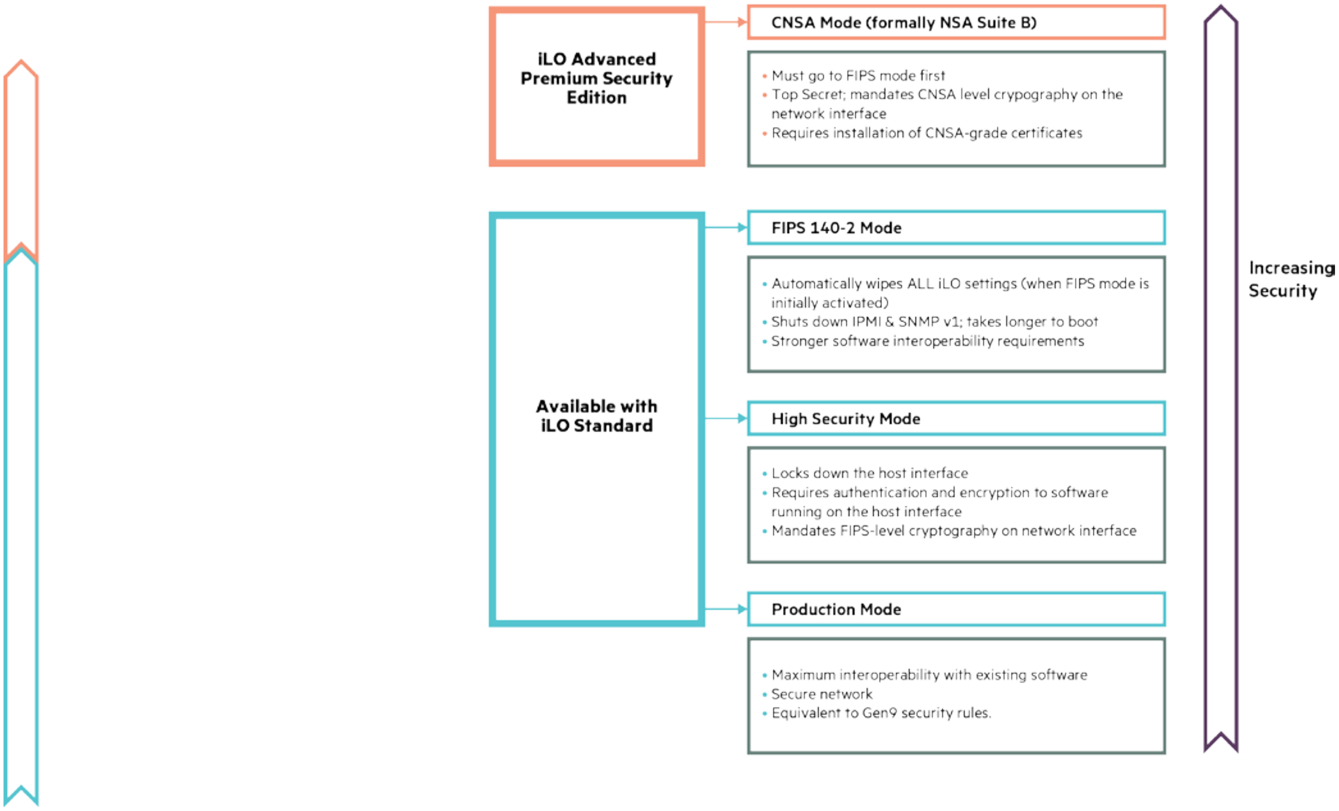
Figure 4. HPE G2 Advanced and Enterprise racks include the ability to have third-party secure locks and intrusion sensors attached to PDUs.

Understanding Gen10 security modes and potential consequences

Customers should consider how incorporating the advanced security capabilities might affect other aspects of their business. When you tighten security, there may be potential access and software interoperability challenges, or possible affects to performance.

With the baseline, iLO Standard that comes with every Gen10 server, customers have the ability to configure their server in one of three security modes. With the iLO Advanced Premium Security Edition license, customers that need the highest-level encryption capabilities of CNSA have a fourth security mode available to them (see Figure 5).

Essentially, as a customer moves up the scale in security, the server enforces stronger encryption rules for webpages, SSH, and other network communications. Both ends of the network communication have to support the encryption rules, or they cannot communicate. Various interfaces are also shut down to limit potential security threats.


iLO Advanced Premium Security Edition
CNSA Mode (formally NSA Suite B)
FIPS 140-2 Mode
Available with iLO Standard
High Security Mode
Production Mode
Increasing Security

- Must go to FIPS mode first
- Top Secret; mandates CNSA level crypography on the network interface
- Requires installation of CNSA-grade certificates

- Automatically wipes ALL iLO settings (when FIPS mode is initially activated)
- Shuts down IPMI & SNMP v1; takes longer to boot
- Stronger software interoperability requirements

- Locks down the host interface
- Requires authentication and encryption to software running on the host interface
- Mandates FIPS-level cryptography on network interface

- Maximum interoperability with existing software
- Secure network
- Equivalent to Gen9 security rules.

Figure 5. Customers have the option of four different security modes with Gen10 servers and the iLO Advanced Premium Security License

Production mode

The HPE Gen10 servers ship in production mode, which allows the broadest interoperability with existing software. It maintains the same level of security protocols as available with the Gen9 severs.

High security mode

High security mode (previously called AES/3DES mode) increases the sophistication of the encryption ciphers compared to production mode and uses the same encryption ciphers as FIPS mode. However, it does not require the same initialization steps that FIPS mode does, so the boot times are not increased. It also locks down the host interface by requiring authentication from the host OS side——there is no assumption that all communications from the host OS side are authorized. High security mode enforces stricter security policies such as requiring valid iLO5 credentials to use RBSU or other host-based utilities (previously this was a separate setting called UDC LOCK).

FIPS mode

FIPS Mode not only implements validated encryption ciphers but also closes down insecure interfaces that do not meet the government standard. Because interfaces like IPMI and SNMP v1 are shut off, potential attack surfaces are reduced. When entering FIPS mode, all the iLO5 settings are reinitialized to operate as a FIPS validated environment. The designated security officer must reset the configuration according to procedural documents. (See the HPE iLO5 User Guide and FIPS validation certifications that explain the steps necessary for FIPS-approved modes of operation, http://csrc.nist.gov/groups/STM/cmvp/documents/140-1/140sp/140sp2574.pdf).

Because FIPS mode has more rigorous internal checks, the time required to boot iLO5 or to generate certificates increases compared to High security mode.

Software interoperability may be an issue with some (older) client software, for example, web browsers that use lower-grade cipher suites. (FIPS Mode will interoperate with other clients operating in a validated mode.)

CNSA mode

CNSA mode is an option that supports only a subset of the FIPS validated crypto algorithms—the customer must activate FIPS mode first, then CNSA encryption ciphers can be activated so that only the CNSA subset of FIPS-validated crypto algorithms are used.

Because it is based on FIPS mode, CNSA mode has the same internal checks and slower boot times that FIPS mode does.

Interoperability is more of an issue in CNSA than in FIPS, because there are fewer cipher suites/encryption algorithms supported in CNSA mode. Customers should consult tool documentation to determine if the tools support iLO5 in CNSA mode. CNSA certificates are also required to negotiate the ciphers required. CNSA mode certificates are specialized ECDSA certificates, and happen to be much faster to generate than the RSA certificates iLO5 normally uses in other modes.

HPE NIST infrastructure

This paper has focused primarily on the server hardware, options, and rack-level infrastructure that can make your environment more secure. However, that is clearly only a small slice of what you need to consider for your enterprise as IT architectures evolve from traditional IT data centers to private cloud and converged or hybrid cloud-based infrastructures.

HPE is in the process of creating the artifacts and documentation that will facilitate the customer's efforts to achieve an accreditation or certification by using HPE's secure equipment stack. HPE has designed its HPE NIST Infrastructure (HNI) solution to help you secure your private cloud or converged environment by providing an entire solution stack to include the hardware (network, server, and storage), software, process, and documentation that will help you comply with NIST Special Publication 800-53. NIST 800-53 is a publication that recommends and documents security controls for federal information systems and organizations. The HNI solution stack uses HPE ProLiant Gen10 servers, Arista networking, and 3Par storage, and has proven to provide robust performance, in addition to passing penetration scans and vulnerability testing. This solution stack, combined with an organization verifying the facilities and procedures for IT administration (flashing firmware, updating software, etc.), will allow an organization to benefit from a secure infrastructure aligned to the NIST 800-53 standards.

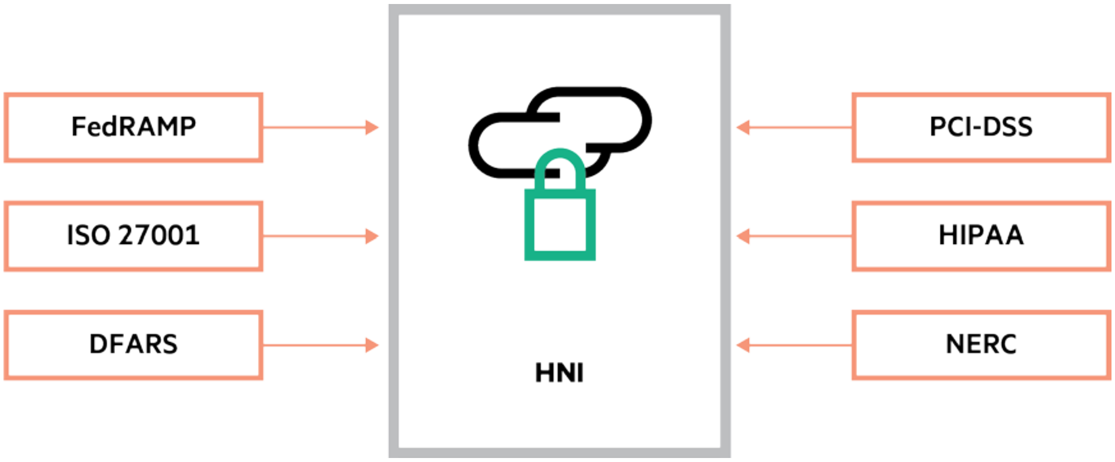


Figure 6. HNI addresses specific cyber-security needs by providing location-agnostic automated infrastructure prepared for customers to rapidly adopt as their security baseline.

HPE Pointnext services

HPE Pointnext, the HPE IT services organization, offers design and implementation services to further extend and complement HPE Gen10's security features, including the following services:

- Take the capabilities discussed in this paper and extend the hardening capabilities up into the OS, virtualization, and database levels in accordance with your specific policy and regulatory requirements, such as PCI DSS.
- Build out a completely hardened infrastructure environment that includes network and storage related security and data protection solutions.
- Design and implement comprehensive two- and three-factor authentication solutions to reduce risk of unauthorized access.
- Take advantage of Gen10's ability to send iLO5 alerts and verification check notifications by integrating with security logging and analytics tools to ensure rapid detection.

In addition, HPE Pointnext provides assessments, architecture design and integration services to remediate gaps, and transform or modernize your data center security environment—including people, processes, and technologies.

Conclusion

Security threats to your business data and systems are steadily increasing, with attacks being more complex and attack surfaces changing from network perimeter, software, and applications to the physical platform itself. Network firewalls, anti-virus scanning, and even security monitoring (SIEM) tools such as Splunk are not sufficient protection, because they operate at the data plane level and assume that underlying physical resources such as firmware are secure. HPE is committed to increasing the level of security in all three critical pillars of the security environment—protect, detect, and recover— so that customers can be confident that their server hardware infrastructure is secure from threats even at the firmware level. With the HPE Gen10 servers, customers can also be assured that any potential vulnerabilities will be addressed quickly, and that they can return to authenticated settings quickly if a threat is sensed.

The HPE Gen10 servers, with iLO5 made by HPE, offer the first industry standard servers to include a silicon root of trust that provides integrity checks to ensure that the server boot process is completely secure and authenticated within the hardware itself before initializing the UEFI and the OS. The silicon root of trust enables the detection of previously undetectable compromised firmware or malware. With the iLO Advanced Premium Security license, customers can enable daily automatic scanning of firmware and have automatic recovery to authentic good states if necessary. Combining the Gen10 server capabilities with selected server options, networking infrastructure, and rack hardware allows customers to design a resilient and hardened industry standard server infrastructure. Customers can also include HPE Pointnext services to ensure that the individual capabilities of their server infrastructure are integrated with policies, procedures, virtualization software, and applications in the most effective way to create a comprehensive security environment.

Resources, contacts, or additional links

HPE iLO documents in Hewlett-Packard Enterprise Information Library
hpe.com/info/enterprise/docs

Enterprise Secure Key Manager

General information	hpe.com/software/ESKM
FIPS certificate	csrc.nist.gov/groups/STM/cmvp/documents/140-1/140val-all.htm#2862
FIPS Security Policy	csrc.nist.gov/groups/STM/cmvp/documents/140-1/140sp/140sp2862.pdf.
FIPS certificate	csrc.nist.gov/groups/STM/cmvp/documents/140-1/140val-all.htm#2862
Common Criteria EAL2+	cybersecurity.my/mycc/mycprC068c.html

HPE Pointnext services
hpe.com/pointnext

NIST Special Publication 800-53
Security and Privacy Controls for Federal Information Systems and Organizations
http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf

HPE technical white papers
hpe.com/docs/servertechnology

Sign up for updates

Hewlett Packard
Enterprise

a00008733enw, June 2017