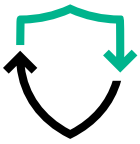
Hewlett Packard Enterprise

Business white paper

# A comprehensive view of IT infrastructure security

# Table of contents



In 2016, cyber-attacks cost businesses worldwide $450 billion. Breathe easy with HPE's standards-based safeguards and integrated controls across the technology stack—infrastructure and DC systems, data storage and backup, network access for the Intelligent Edge, supply chain, and services.

Cyber threats making you anxious? Move beyond adopting the usual responses with HPE's security approach that begins at the silicon and firmware layers and flows through the supply chain, manufacturing processes, development environment, hardware, data center, and the cloud.

## Introduction

HPE infrastructure technologies and services help enterprises accelerate time to value from their data and applications. Enterprises use our servers, storage systems, and network access products to deploy and manage mission-critical workloads on-premises and in hybrid cloud environments.

In this paper, Jaikumar Vijayan explains how HPE protects the apps and data of our customers. Our approach begins at the silicon and firmware layers and flows through the supply chain, manufacturing processes, development environment, hardware, data centers, and the cloud.

The organizations we serve are under increasing pressure from customers, consumers, and regulators to secure their digital infrastructure against compromise and disruption. Attacks have become more sophisticated, threat actors are getting smarter and well organized, and the effects of information security failures have become far more consequential in terms of information and financial losses.

In 2016, cyber-attacks cost businesses worldwide $450 billion in losses.[1] More than two billion personal records were stolen worldwide. Losses stemming from cybercrime will top $6 trillion by 2021 according to a 2016 report from Cybersecurity Ventures.[2] These losses included data destruction and theft, lost productivity, loss of intellectual property, theft of financial and personal data, breach remediation costs, and reputational damage.

The average costs to businesses from cybercrime increased from $3.8 million in 2015 to $4 million in 2016 according to research by the Ponemon Institute.[3] More innovative companies tended to bear higher losses: $9.5 million on average in 2016.[4]

Cyber-attacks are no longer targeted only at the OS and applications. Attacks are also happening at the database, firmware, kernel, and hardware level. Firmware-level attacks are a particular problem. In most modern hardware, millions of lines of firmware run before the OS even boots. Adversaries that manage to inject even a couple of lines of malicious code into firmware in the supply chain, at runtime, or via physical access can steal data, create denial of service conditions, or compromise the integrity of the entire system.

We have organized the paper into sections that describe the security controls that HPE has implemented at the following layers:

1. Infrastructure and data center systems
2. Mission Critical Solutions
3. Data storage and backup
4. Secure network access from the Intelligent Edge
5. Supply chain
6. HPE Pointnext

The objective of this paper is to highlight HPE's commitment to make sure that its technology stack, from the silicon layer upward, provides standard-based safeguards for building, deploying, running, and managing internet-scale workloads. We focus on the controls we have integrated into our products to help organizations identify, protect, detect, respond, and recover from security incidents in the manner prescribed by the National Institute of Standards and Technology (NIST) Cybersecurity Framework.

[1] "**Cybercrime costs the global economy $450 billion: CEO**," CNBC, 2017

[2] "**Hackerpocalypse: A Cybercrime Revelation**," Cybersecurity Ventures, 2016

[3] "**Data Breaches Now Cost $4 Million on Average**," Fortune.com, Time Inc., 2016

[4] "**2016 Cost of Cyber Crime Study & the Risk of Business Innovation**," Sponsored by Hewlett Packard Enterprise, conducted by Ponemon Institute, 2016

## Infrastructure and data center systems

**HPE cloud-centric systems for Hybrid IT environments**
A Hybrid IT environment combines the use of public cloud infrastructure and services with on-prem private cloud and dedicated computing resources. Hybrid IT environments allow enterprises to combine the economics and flexibility of the public cloud with the security and control that on-prem infrastructure provides for mission-critical workloads.

HPE's portfolio of industry-standard servers, including our HPE ProLiant Gen10 systems, represents our approach to securing Hybrid IT and traditional infrastructure. The servers integrate multiple technologies, starting at the silicon level, to protect against, detect, respond to, and recover from security threats to critical enterprise workloads in hybrid cloud settings.

The following is a description of some of those controls.

- **Silicon Root of Trust**—HPE servers are industry-standard systems which include a unique digital fingerprint, which we call a Silicon Root of Trust, in the silicon of each server. The Root of Trust verifies certain security functions and provides the ability to test and verify the integrity of other such functions. This makes sure that a server never boots up if its firmware has been compromised or tampered with any way. Because system firmware is anchored to the Root of Trust, a system will not boot up even if an attacker replaces the entire Unified Extensible Firmware Interface (UEFI) and HPE Integrated Lights Out (iLO) code. In many modern computers, the UEFI has replaced BIOS as the first module to run when the system boots up. iLO is a proprietary HPE technology for remotely managing servers.
- **Runtime firmware validation**—HPE Gen10 servers support a threat detection feature that provides runtime protection of key system firmware. The HPE iLO chipset that performs the security checking process during boot up continues the same verification on a continual basis while the server is running. The HPE iLO chipset, with its Silicon Root of Trust, runs a daily verification check on HPE iLO firmware and UEFI BIOS, giving customers an opportunity to quickly detect firmware compromises.

- **Secure recovery from corrupted firmware**—If a firmware problem is detected, administrators have the option to restore the affected firmware to its last known good state or to a factory default setting. In the unlikely event of a firmware compromise, the HPE iLO chipset automatically loads its own authenticated firmware from an integrated backup stored in nonvolatile memory. If the system firmware is compromised, HPE iLO tries to recover from a backup copy or alert the administrator.
- **Data protection**—Hewlett Packard Enterprise provides support for the Commercial National Security Algorithm (CNSA) suite. CNSA is a suite of cryptographic algorithms that is used by federal agencies to protect national security systems (NSS)—including those classified as TOP SECRET—and by the vendors that develop products used in NSS. This is the very highest level of security, designed to protect the most sensitive data. It has replaced the Suite B cryptography that the United States' National Security Agency previously used to protect NSS.[5]
- **Trusted Platform Module**—HPE servers support Trusted Platform Module (TPM) 1.2 and 2.0 technology to store the encryption keys, digital certificates, and passwords that are used to authenticate the platform and to validate the software running on them. TPM modules are also used with a measured boot process to monitor the OS initialization process and make sure the OS startup has not been compromised.
- **Protection against physical compromise**—Chassis intrusion detection and rack cabinet door detection controls alert against physical tampering or unauthorized access to servers. A physical connection from the chassis board and hood enables detection of any physical intrusion into the chassis and provides security during the shipping, receiving, distribution, and operation of HPE systems.
- **Product integrity and assurance**—Industry-leading security management and security innovations in HPE server, storage, and network products comply with federal standards such as FIPS 140-2, Federal Information Security Management Act (FISMA), Federal Risk and Authorization Management Program (FedRAMP), and Common Criteria Certification.

  Industry standards implemented in HPE hardware products include UEFI Secure Boot, the Core Root of Trust Measurement (CRTM), and TPM 1.2 and 2.0.
- **Reference architectures and configurations**—Hewlett Packard Enterprise uses reference architectures and configurations to deliver complete, reliable, and fully validated infrastructure configurations for a range of Hybrid IT platforms.

  Our **HPE Reference Architecture for secure and compliant backups and replication** and **HPE Reference Configuration for HPE Helion CloudSystem Enterprise security with Micro Focus SecureData** reference architectures offer repeatable and workload tested configurations. This comes with built-in security features that have been developed over years of experience in enterprise customer environments.

  The reference architectures greatly reduce the need for organizations to deal with the technological complexities of planning and implementing infrastructures for diverse workload requirements.

[5] **cryptome.org/2016/01/CNSA-Suite-and-Quantum-Computing-FAQ.pdf**

## Mission Critical Solutions

Organizations use HPE mission-critical systems to run large transaction processing, batch processing, and database and analytics applications. Our mission-critical systems portfolio is built around HPE Integrity servers running the HPE NonStop, HP-UX, OpenVMS, Linux®, Windows® and VMware® Operating Environments.

### HPE NonStop

HPE NonStop systems deliver fault-tolerant computing performance for banks, telecommunication companies, transportation firms, and many other sectors. HPE NonStop systems run vital workloads with extremely high availability, confidentiality, and integrity requirements. Many HPE NonStop customers are in highly regulated verticals with complex data protection mandates. HPE NonStop servers meet these requirements in a variety of ways, including the following:

- **Strong access management**—The Platform and Safeguard layers of HPE NonStop OS provide authentication, authorization, user management, and access control services at the lowest levels of the system. We protect against insider theft and data misuse by making sure that users, groups, and objects have only the minimum required access to data and system resources. All user passwords are stored in encrypted form to protect against credential theft and misuse. In addition to these, HPE NonStop provides features such as Role Based Access Control (RBAC) and extensibility features such as the support for Security Event Exit Processes (SEEP).
- **Protection against system-level damage**—Applications run in nonprivileged user mode. To reduce the risk of unauthenticated applications, rootkits, and other malware running on the system, privileged kernel functions can only be invoked through a defined set of procedures.
- **Controls against unauthorized system access and settings changes**—The Safeguard component monitors for and audits logon attempts, object access, security setting changes and other events of importance from security perspective. Security administrators and auditors can use these tools to monitor and perform any forensic activities to investigate security events.
- **Encrypting data-at-rest and in transit**—HPE offers Volume Level Encryption (VLE) and Secure Tape products to encrypt data while at rest in disks or in backup storage devices. NonStop systems provide disk sanitization tools to destroy the data from storage devices when required. We use the secure shell (SSH) and Secure Sockets Layer (SSL) protocols for end-to-end encryption of data at the transportation layer.

  We work closely with ISVs to meet security requirements in areas such as enhanced audit management and user authentication.

- **Support for compliance reporting**—HPE offers XYGATE Compliance PRO, a system of GUI-based interface and reporting templates that demonstrate compliance with regulatory requirements such as PCI. In addition to the above products, HPE NonStop offers several other security products to help customers secure their environment through mechanisms such as keystroke logging, multi-factor authentication, integrating application logs and other solutions to protect the NonStop environment.

### HPE Integrity servers with HP-UX

Global banks, pharmaceutical companies, telecommunication firms, and other organizations use HPE Integrity servers with HP-UX to run mission-critical workloads. HPE Integrity servers use a variety of technologies to provide threat protection, detection, and response, including the following:

- **File and disk-level encryption**—Hewlett Packard Enterprise provides several encryption technologies to help ensure that only authorized applications can access your files and data. We support file-level and disk-level encryption, as well as HP-UX whitelisting for our HP-UX 11i Security Containment technology, which isolates compromised applications before they pose a threat to your data.
- **Host intrusion detection**—HP-UX Host Intrusion Detection System (HIDS) allows administrators to monitor, detect, and respond to attacks and intrusions on HP-UX systems. For example, HP-UX HIDS monitors system activity to detect patterns that suggest suspicious or malicious behavior, and issue alerts on such activity.
- **Role-based access control**—To protect identities in an HP-UX environment, we support role-based access control, integration with existing Lightweight Directory Access Protocol (LDAP)-based identity management infrastructure and centralized authentication, authorization, and accounting via Remote Authentication Dial-In User Service protocol (RADIUS)-enabled middleware and applications.
- **Common Criteria Certification**—Industry certifications, including Common Criteria Certifications, provide independent validation of HP-UX security model and represent the fourth component of our strategy for addressing the security requirements of HP-UX users.

### HPE Integrity Superdome X

Global manufacturing, retail, telecommunications, healthcare and financial services companies trust their critical business processing and analytics workloads to Superdome X. To protect the sensitive data and processes handled by these servers, Superdome X features a wide range of security technologies, including the following:

- Authenticated Updates: Firmware updates verify digital signatures before updating the system. The Superdome X firmware update process is completely secure, covered by secure protocols, and with a digitally signed bundle containing firmware for every operational component in the Superdome X enclosure to maximize protection. We use secure HPE signature and signature checking for firmware updates. If verification fails, the update is aborted, and the programmed firmware remains unchanged.
- Trusted Host feature and Role Based Access Controls: The Superdome X Onboard Administrator network access can be limited to no more than five specific IPv4 addresses, and there is role based access control to access the hardware and partitions. We include configurable strong password enforcement and minimum password length.
- Secure Development: All the infrastructure used to support the production processes leverage dynamically maintained virus scanning software to minimize the risk of any malware being introduced. During the manufacturing process, firmware and software packages are scanned for malware and viruses, then digitally signed by HPE Cybersecurity process to ensure firmware and/or software tampering is not possible.
- Other security features included are Certificate Management, Centralized Crypto Settings, Centralized User Management, Secure Out-of-Box, Audit Logs, Two Factor Security, and many more.

## Data storage and backup

This section describes the measures we have implemented to make sure that HPE 3PAR StoreServ storage array systems and HPE StoreOnce deduplication appliances meet enterprise security requirements for data storage and backup.

**HPE 3PAR StoreServ storage array systems**
HPE 3PAR StoreServ block storage is built on the following six pillars: authorization, authentication, availability, encryption, integrity, and auditability.

- HPE 3PAR has all these security principles/areas covered with the features built into it. Some of the significant HPE 3PAR security features are as follows:
  - **Self-encrypting drives**—To make sure that data is protected, HPE 3PAR StoreServ systems are configured with self-encrypting drives that encrypt data as it is written to the drives with no user intervention.
  - **Validated encryption for data-at-rest**—We protect the integrity of data-at-rest using FIPS 140-2 Level validated encryption, along with end-to-end T10-DIF error checking.
  - **FIPS-certified key management**—HPE 3PAR StoreServ storage supports local and external FIPS-certified key management to address enterprise data protection requirements, both on-premises and in the cloud.
  - **Certificate-based user authentication**—HPE 3PAR StoreServ storage systems support LDAP and X.509 certificate-based authentication of users and applications accessing storage.
- **HPE StoreOnce systems**—HPE StoreOnce systems ensure that crucial enterprise data is securely backed up and easily recoverable in the event of an attack or other disruption.

  HPE StoreOnce implements NIST FF1 AES-256 bit encryption for protecting data-at-rest. Some models support encryption of data in flight via IPSec. Additionally, the Secure Erase feature in HPE StoreOnce meets NIST SP 800-88 guidelines for media sanitization and supports up to seven passes to erase sensitive data.
- **Scalable encryption**—HPE scalable encryption technology is a differentiated offering that protects data stored in the server. Unlike competitor servers, which use self-encrypting drives that require management of separate keys in each drive, Hewlett Packard Enterprise offers reliable encryption through HPE Smart Array controller cards, which contain encryption cards and manage them at scale.
- **Strategic partnerships**—Where appropriate, we work with partners to extend and enhance our data storage and backup capabilities. Here are some examples:
  - **Veeam**—Improved data protection and recovery times for virtualized mission-critical environment is provided via integration of HPE 3PAR StoreServ with Veeam Backup and Replication software.
  - **Veritas**—Integration of HPE StoreOnce and Veritas NetBackup enables high-speed data restores high-availability and better disaster recoverability.
  - **Arista**—Arista data center switches work with HPE storage, server, and management products to enable converged infrastructure implementations.
  - **Scality**—Software-defined object storage is optimized for organizations in media, financial services, government, and other sectors.
  - **Cohesity**—It offers prevalidated, preconfigured, web-scale storage option for organizations seeking to consolidate secondary workflows.
  - **Micro Focus**—Micro Focus is a global software company that builds, operates, and secures the IT systems that bring together existing business logic and applications with emerging technologies.

## Secure network access from the Intelligent Edge

Hewlett Packard Enterprise enables organizations to safely harness the business benefits of IoT and enterprise mobility.

As the software components of our Aruba 360 Secure Fabric, HPE Aruba IntroSpect User and Entity Behavior Analytics (UEBA) technology and HPE Aruba ClearPass tools help organizations identify, connect, protect, and manage users, systems, smartphones, tablets, and other IoT devices.

Our 360 Secure Fabric capabilities combine visibility, control, and monitoring with attack detection, alerting and response at the network edge. The following are some examples of how we enable endpoint devices to access the network safely.

**Safe access control with HPE Aruba ClearPass**
HPE Aruba ClearPass provides role-based and device-based network access control for a multivendor IoT world.

**Device authentication and authorization**
HPE Aruba ClearPass identifies, authenticates, and authorizes devices that are being used on your wired and wireless networks. It collects real-time information such as the type, OS, and other specific attributes of individual devices on your network.

**Policy enforcement**
HPE Aruba ClearPass Policy Manager enables enforcement of highly granular, context-aware security policies on devices in use on your network, including full quarantining in the event of a security violation.

**Advanced attack detection with HPE Aruba IntroSpect**
HPE Aruba IntroSpect delivers on-prem and cloud-hosted UEBA capabilities to detect anomalous behavior indicative of gestating attacks on users, systems, and devices that have evaded traditional security tools.

**Endpoint threat detection**
HPE Aruba IntroSpect helps detect insider threats and external attacks using supervised and unsupervised machine learning to baseline normal user and entity behavior on your network and to spot any deviations from that behavior.

HPE Aruba IntroSpect stand-alone UEBA technology consumes and analyzes both network and IT log information to identify anomalous and potentially harmful behavior on your network.

**Multilayered endpoint protection**
In combination, HPE Aruba ClearPass and HPE Aruba IntroSpect enable advanced attack detection and accelerated response capabilities that mitigate vulnerabilities and threats to your IoT environment.

HPE Aruba IntroSpect detects internal and external threats in your IT environment. HPE Aruba ClearPass controls endpoint access to your network based on specified policies and attack alert data from HPE Aruba IntroSpect as well as other products in the security ecosystem.

## Supply chain

Vulnerabilities in the supply chain can result in the introduction of counterfeit parts and malicious software in the manufacturing, warehousing, transit, and predeployment phases. The range of threats includes nation-state actors conducting espionage and denial of service campaigns through compromised devices introduced in the supply chain.[6]

A single vulnerability can prove disastrous. In 2016, for example, Apple had to purge its data center of multiple servers supplied by a third-party vendor after discovering at least one server loaded with malware-infected firmware.[7]

We implement multiple measures to prevent such tampering and maintain product integrity through the supply chain lifecycle. These measures include the following:

**Standards and assessments**
Suppliers of HPE products and services must comply with several standards and self-assessments based on policies and industry practices. These include Defense Federal Acquisition Regulation Supplement (DFARS) and ISO.

Proof points for compliance include risk-based security audits, regular program monitoring and reporting, inspection and testing of electronic parts, component traceability, and material control processes, including quarantining and purging of tainted components. Suppliers are required to ensure shipping and logistics processes are compliant with Customs-Trade Partnership Against Terrorism (C-TPAT) or comparable programs as determined by Hewlett Packard Enterprise.

**Firmware protection standards**
Hewlett Packard Enterprise has adopted and adheres to standards such as the NIST BIOS Protection Guidelines for Servers and the ISO specification for supply chain security management systems that mitigate risks of firmware taint, corruption, counterfeiting, and substitution.

**Provenance, sourcing, origin, and traceability**
Hewlett Packard Enterprise provides complete product and part traceability—including country of origin, supplier name, and conformance certification—for programmable logic components in its hardware. We require our suppliers to do the same.

**Control over custom silicon and HPE iLO firmware**
We build and therefore have complete control over the custom HPE silicon and HPE iLO firmware at the heart of our Silicon Root of Trust. This greatly reduces opportunities for tampering in the supply chain.

**Secure clean rooms**
We use a protected clean room to digitally sign every piece of firmware that goes into our systems.

We build our hardware chassis completely and then put a lid on it and seal it. An internal switch records if the chassis is ever opened, preventing undetected tampering of the sort that some governments and nation-state actors have indulged in over the last few years.

On high-risk components such as drives and memory, we use labels that are impossible to duplicate, making it easy to distinguish counterfeit products.

[6] "**Cyber Supply Chain Security and Potential Vulnerabilities within U.S. Government Networks**," National Conference of State Legislatures, 2016

[7] "**Apple Severed Ties with Server Supplier After Security Concern**," The Information, 2017

## HPE Pointnext

HPE Pointnext provides advisory, professional and operational services to our enterprise customers. HPE Pointnext experts help organizations transform and optimize Hybrid IT environments and enable transformations from edge to core to cloud.

HPE Pointnext will collaboratively advise, define strategy and road maps, architect and design, integrate and transform so you have adaptive digital protection to compete in the digital economy. Our methodologies and blueprints are flexible to help you with the big picture transformations or with specific solutions to close gaps or improve current security controls, continuity and security operations.

The following section describes how each of these services help organizations implement better security.

**Risk, continuity, and compliance management**
HPE Pointnext enables organizations to align their risk, continuity, and compliance management programs with their business goals, risk appetite, recovery requirements, and regulatory mandates. For example, HPE Pointnext helps organizations conduct compliance, architecture and vulnerability assessments, and business impact assessments. We also provide disaster recovery and business continuity planning services.

**Infrastructure and access control**
HPE Pointnext helps organizations design and implement safe infrastructure and access controls to meet business requirements. Customizable reference architectures from HPE Pointnext help customers design and integrate security into cloud, IoT, mobile, and other environments.

HPE Platform Protection and Compliance Service enables organizations to assess and remediate the security readiness of their IT infrastructure. Services are available to integrate technologies such as HPE Aruba ClearPass and network access control products from third parties.

**Data protection and privacy assessment**
HPE Pointnext helps organizations assess and understand risks to their personally identifiable information (PII), intellectual property, and other sensitive data. We design risk-appropriate and budget-friendly controls to protect the confidentiality, integrity, and availability of your digital assets. HPE Pointnext covers the five Ps—people, policies, processes, products, and proof to enable comprehensive data security and protection.

## Other contributors to this business white paper:

Boliek, Lois H.
Bradley, Chris
Brockelman, Ken
Church, Nigel
Dasari, Shiva R.
De Clercq, Jan
Kapoor, Vikas
Leech, Simon
Lepore, Mark
Lunetta, Larry
Malik, Rashmi
Mayes, Brad
Moore, Bob
Young, Greg

Backup, Recovery, and Archiving (BURA) technologies from HPE Pointnext help organizations implement strategic initiatives for data backup and recovery. HPE Data Sanitization Service can help erase sensitive data from storage and other systems. Meanwhile, patch management services protect against known and emergent malware threats.

### Operational security and cyber defense

Infrastructure security controls can enable better security. However, in order for such controls to be truly effective, organizations need to have a full understanding of risk, based on an assessment of what they really need and how effectively their existing controls are working.

Our operational security (OPSEC) framework and family of operational security services help organizations implement controls in areas such as threat management, vulnerability management, and security monitoring. OPSEC services include HPE Foundational Care for HPE Gen10 security features, HPE Data Sanitization Service, HPE Asset Recovery Services, and workforce security programs.

### Using ITIL® to align security requirements

Our IT Infrastructure Library (ITIL) processes can help you assess and align your IT security requirements with business needs and make sure that security is an enabler of digital transformation and not a roadblock. We help define common goals and identify metrics for enterprise risk in a manner that is responsive to business needs.

### Enabling better incident detection and response through automation

We enable security administrators a way to centralize and correlate security information from across the enterprise using security information and event management (SIEM) and behavior analytics tools such as HPE Aruba IntroSpect.

## Conclusion

The security controls that HPE has implemented across its technology stack are designed to help organizations identify, protect, detect, respond, and recover to security incidents at internet scale. We also recognize the security risks posed by the complexity of the IT supply chain. The measures we have taken to protect the integrity of our software and components are unparalleled in the IT industry.

Hewlett Packard Enterprise seeks to make sure that its technology stack, beginning at the silicon and firmware layers and flowing through the hardware, data centers, and the cloud, provides standard-based safeguards for building, deploying, running, and managing internet-scale workloads.

Based on industry standards and best practices, our security approaches are certified to the highest U.S. government and international standards. Our goal is to make sure that your workloads run reliably on-premises, in the cloud, in hybrid environments and at the network edge.

Learn more at
**hpe.com/security**



**Sign up for updates**



a00006637ENW, October 2017, Rev. 1