

HPE supply chain security innovation: Enhancing trust and resilience from edge to cloud

Table of contents

4	Introduction
7	A trusted supply chain
8	Software security and integrity
9	Robust supply chain security requires a secure approach
10	Creating trusted environments
11	Verifying authenticity and tamper prevention
11	Building a zero trust-enabled architecture from silicon to cloud
12	Cybersecurity risk management in the supply chain
17	Hardware security
18	Improving end-of-lifecycle management
19	Summary

Introduction

At Hewlett Packard Enterprise, we deeply focus on supply chain and ecosystem security. We recognize that organizations strive to unify operations across increasingly complex and distributed hybrid estates, driving new requirements for flexible security solutions that can scale at the speed of business transformation.

As the digitization of supply chains is accelerating, organizations are more urgently addressing their digital risk. A recent study revealed that 73% of organizations were significantly concerned about the risks posed by the accelerated digitization of supply chain but that no one organization had resolved the risks.¹ As a supplier to our customers, we recognize the critical role that the HPE supply chain security plays in our customer relationships. We have grown our capabilities to respond to customer queries accordingly.

We also recognize that chief security officers (CSOs) and chief information security officers (CISOs) are tasked with responding to constantly evolving and expanding cybersecurity challenges, including:

- **Supply chain risks**

Supply chain attacks are a growing threat, as attackers target vulnerabilities in the software and hardware that suppliers and partners use, as well as attacks on physical supply chains during the manufacturing process.

- **Third-party vendor risks**

As organizations rely more on third-party vendors for critical business functions, the potential for cyberattacks through these relationships increases.

- **Advanced persistent threats**

These threats may be highly sophisticated, targeted attacks that exploit vulnerabilities and may remain undetected in a supply chain over an extended period.

- **IoT and edge security**

As Internet of Things (IoT) devices at the edge of networks grow exponentially, they can expand the attack surface for cybercriminals, leading to security risks for supply chains.

- **Cybersecurity talent scarcity**

There is a high demand for experienced cybersecurity resources due to the evolving threats and cybersecurity attacks that are causing a continuous shortage of qualified security personnel.

At HPE, we have designed a high-performing and trusted supply chain ecosystem with our partners, suppliers, customers, and employees to provide a foundational line of defense against cybersecurity risk against cybercriminals. HPE is committed to providing a highly secure supply chain as an important step toward reducing cybersecurity risks for our customers as they modernize their hybrid cloud environments from edge to cloud.

¹ ["Beyond the storm: how organizations can transition from survive to thrive in 2023,"](#) BSI Supply Chain Risk Insights Report, British Standards Institution, January 2023.



As interconnected third-party applications and systems communicate, organizations seek new strategies to close the security gap, and this is possible only through a combination of robust security policies, secure architecture, and deep collaboration with their supply chain partners.

Gartner predicts that by 2025, **45%** of organizations worldwide will have experienced attacks on their software supply chains, a three-fold increase from 2021.²

Now, more than ever, it is important to strengthen fundamentals and establish a security-first culture to build cyber resiliency effectively. Prepare for, withstand, recover from, and adapt to adverse conditions, stresses, attacks, or compromises to systems that may use or are enabled by cyber resources.

As workloads evolve, they are pushing the capabilities of legacy infrastructure and supply chains. While enterprises have worked hard to establish their security to meet the data demands of their hybrid operations, cybercriminals have become relentless in finding new ways to infiltrate IT systems and gain long-term persistence. In recent years, bad actors have increasingly targeted complex global supply chains that are now operating in increasingly complex global networks with different third-party suppliers. It has resulted in the supply chain becoming only as strong as the weakest link in a complex environment.

In 2022, supply chain security breaches increased by 38% year-over-year,³ fueled by the proliferation of distributed cloud architectures, complex networks, technology interdependencies, and connected devices at the edge. Each connection and interaction between these elements represent a potential attack vector that needs to be protected. Attackers increasingly employ advanced exploitation techniques that allow them to access large numbers of enterprises at once, resulting in widely propagated impact and, in some cases, long-term persistence.

According to recent research by the European Union Agency for Cybersecurity (ENISA), malware now accounts for up to 62% of cyber supply chain incidents, and two-thirds of attacks on customers take advantage of their trust in their suppliers.⁴

Today's reality is that organizations often fail to consider their extended supply chain when analyzing risks or selecting their IT partners. Third-party developers and technology partners are key actors in the supply chain of the IT systems, hardware, and software entering organizations. It's now crucial to consider how to secure your organization and question how secure the people and processes of the organizations that connect to their business, including the supply chain, really are.

² ["Gartner Top 9 Cybersecurity Trends in 2025,"](#) Gartner Inc., April 2025.

³ ["Check Point Research Reports a 38% Increase In 2022 Global Cyberattacks,"](#) January 6, 2023.

⁴ enisa.europa.eu/publications/good-practices-for-supply-chain-cybersecurity



Niysaan Vlasak
Vice President
Operations — Engineering
and Enablement
Hewlett Packard Enterprise

Supply chain security is our priority

Cybersecurity is everyone’s responsibility. At HPE, we have created the foundations for our customer’s digital security, which highly depends on maintaining a secure supply chain. In recent years, most industries have experienced material shortages, which have increased counterfeit parts, as well as more frequent and sophisticated cyberattacks disabling supply chain operations and everyday business functions. Our responsibility in HPE Operations is to help protect against and mitigate these risks while providing a trusted supply chain — one that is designed with multiple layers of defense and comprehensive protective solutions, beginning at product design through end of life or disposal.

“Providing more secure products and services to our customers and helping to enable their secure operations is our priority. We believe that constantly strengthening, improving, and maintaining a more cyber resilient and secure supply chain environment is of essential value to our customers, thereby strengthening their supply chains and daily business operations. We will continue to invest in mitigating cybersecurity threats that may impact our products and services throughout the value chain, and we are committed to creating innovative solutions to ensure that our supply chain is more secure, resilient, and transparent.”

Cybersecurity risks in the supply chain may also take the form of counterfeiting, unauthorized production, and tampering, each of which can lead to significant financial loss, data destruction, and reduced productivity. Other possible outcomes include the theft of personal and financial data and stolen intellectual property, which incur significant remediation costs. Whatever the cause, there’s a constant threat to reputation and brand image. Although it may be difficult to measure, it is certainly significant. Ultimately, once a supply chain has been compromised, the security of the compromised device can simply no longer be trusted.

Led by the HPE Operations executive leadership, HPE has a deep commitment to facilitating a secure supply chain. With governance that encompasses cross-functional business groups, HPE provides end-to-end supply chain security to help safeguard the most important assets of our customers and partners:

their customers, employees, and data. Our Trusted Supply Chain program is governed by a cross-functional Center of Excellence within HPE Operations and supported by HPE senior leadership.

To meet this goal, HPE has focused on building trusted partnerships with our supply base. By providing our customers with the highest possible product cybersecurity assurance, they receive verifiably authentic, uncompromised products and solutions across a global and highly diverse supply base. We have developed a world-class supply chain that drives quality and security excellence. It is designed to reduce risk at every stage of the supply chain process to help ensure a more trusted ecosystem, which we strive to improve and innovate continuously. A Center of Excellence within HPE brings together workstreams to deliver on organizational priorities to drive secure practices and manufacturing across the HPE supply chain.

A trusted supply chain

Many types of cybersecurity breaches have surfaced over the past few decades, ranging from basic worms transferred via email to very sophisticated denial-of-service intrusions, ransomware, rootkits, and bootkits. However, we've seen increased frequency and sophistication of cyberattacks, particularly in the past five years.

HPE has invested significantly in supply chain security to prepare for the evolving threat landscape and the uptick in the frequency of cybersecurity attacks. Consistent with the reputation for quality and innovation in product security, HPE foresaw the potential impact of cybersecurity threats to our supply chain operations and, most importantly, our customers, and created a program dedicated to strengthening supply chain cybersecurity.

In 2019, HPE formed the Trusted Supply Chain program to mitigate cybersecurity risks and enhance operational process excellence. The HPE Trusted Supply Chain program is designed to address an evolving cyber threat landscape, meet, and surpass industry standards, and help ensure material integrity throughout the supply chain.

HPE has changed the industry paradigm for managing supply chain security and is equipped to deliver the value of our supply chain security capabilities to our customers, thereby helping to strengthen our customer's data security. To identify cyber threats proactively, mitigate any cyber risks, and improve operational processes, we developed a framework consisting of four pillars, as shown in Figure 1 — products and services; policies and standards; transparency; and cybersecurity.

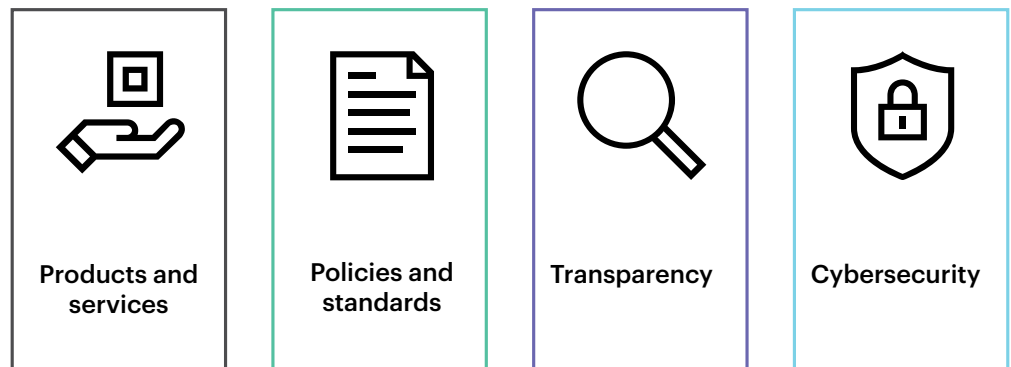


Figure 1. HPE supply chain security priority focus area

For each of the HPE supply chain security areas of focus, we prioritize our resources to continuously improve our supply chain and manufacturing processes within essential security themes. Through this framework, HPE can quickly identify new threats, and proactively mitigate any new risks while improving existing operational security processes. Each pillar has a unique focus and goal to strengthen security practices while providing a forum for developing innovative security programs and initiatives. Our Trusted Supply Chain program is governed by a cross-functional Center of Excellence within HPE Operations and supported by HPE senior leadership.

Software security and integrity

By 2025, it is estimated that software supply chain attacks will cost the global economy \$60 billion in loss and are expected to reach an astounding \$138 billion by 2031.⁵ The widespread availability of open-source software combined with the lack of software provenance have made software supply chains an attractive point of entry for cyberattacks. Advanced persistent threats from bad actors who seek to access software at any point in the lifecycle aim to implement malicious code to infiltrate networks and IT Infrastructure and persist undetected. These attacks are leading to widespread and very damaging consequences. Common attack pathways include the following, as shown in Figure 2.

Attack pathway	Attack vector
Code signing	False identification and impersonation of trusted sources for purpose of inserting malicious code and backdoors
Software updates	Compromise of vendor's update mechanism, leading to malware-infected updates
Open-source code	Insertion of malicious code into publicly available code

Figure 2. Summary of common cybersecurity attack pathways

In response to the evolving threat landscape, HPE has implemented a comprehensive set of mechanisms to help ensure our software is developed using highly secure practices to help protect our customers and partners. We continuously improve the protection of our software development processes within our supply chain. Additional measures and protective mechanisms that are integral to the HPE secure development lifecycle include:

- Architectural risk analysis and threat modeling is performed to identify, quantify, and address the security risks associated with an application.
- Reduce attack surfaces and utilize secure development best practices during software design and development.
- Static code analysis helps confirm the application is free of malicious code or backdoors that circumvent or bypass the security of the application, on an ongoing basis, and throughout the development process.
- Security testing from the inside-out is conducted on all HPE software and firmware, including unit testing, solution-level integration testing, penetration testing, and vulnerability scanning.
- We operate and maintain an extensive open-source review program with requirements to review and approve open-source software that may be used in our products.
- We conduct malware scanning and backdoor analysis on all codes before releasing software to our customers.
- Software, firmware, and system BIOS are digitally signed and then verified during production to help ensure its authenticity and integrity. HPE also uses secure hash algorithms so our customers can receive untainted software.

⁵ 2023 Software Supply Chain Attack Report, Cybersecurity Ventures, October 2023
[cybersecurityventures.com/software-supply-chain-attacks-to-cost-the-world-60-billion-by-2025/](https://www.cybersecurityventures.com/software-supply-chain-attacks-to-cost-the-world-60-billion-by-2025/)

- We continuously monitor for security vulnerabilities in our software supply chain and respond with security bulletins or patches, as appropriate.
- Identify, report, and track vulnerabilities as a Common Vulnerabilities and Exposures (CVE) Numbering Authority.
- HPE employees and software vendors must complete regular training on secure software development policies and requirements.

In addition to software development, HPE employs other protective measures throughout our supply chain operations:

- We maintain stringent factory controls, including access controls and physical security procedures, to prevent unauthorized access to the HPE supply chain.
- We limit access to the signing keys used to sign our software.
- Secure factory transmissions are established for HPE developed and third-party applications, transmitted through secure channels and hosted in a secure environment, continually running virus scans with automatic updates on regularly patched systems.
- The number of our software build environments has been reduced to help minimize the opportunity for infiltration.
- Quarterly assessments of our software suppliers are conducted to ensure adherence to HPE security policies and requirements.
- Software bill of materials (SBOMs) are created and maintained with secure system tools throughout the product lifecycle.

Robust supply chain security requires a secure approach

As threats, market requirements, or government regulations evolve, as seen with the US Executive Order 14028: Improving the Nation's Cybersecurity, HPE Software security best practices delivered through our software security program enable swift and effective compliance capabilities. HPE has implemented processes and tools to help ensure that SBOMs are obtained from our approved suppliers, managed in a secure system, and delivered to our customers at their request.

As other regulations and legal frameworks evolve, such as the European Union's Cyber Resilience Act, the HPE Software security program is designed to incorporate requirements and meet our customer's compliance needs easily.

HPE utilizes a risk management framework to help prevent cyberattacks through software deployment. HPE's secure development lifecycle covers a range of factors that include how we secure the transfer of information, permissions, and access to data along the software development process as well as the necessary security protocols to ensure that our software is free of malicious code.

HPE regularly conducts comprehensive threat assessments focused on software development activities to help mitigate the risk of unforeseen security issues. We take the view of the attacker based on their motivations, techniques, and goals while analyzing the vulnerabilities to determine potentially exploitable threats.

The HPE product security team oversees compliance with the HPE cybersecurity policy for software developers and provides the governance structure for the HPE secure development lifecycle (SDL). The SDL serves as the management system for continuous improvement starting when the software is first conceptualized, built by our software engineers, deployed to our systems and customers, updated after release, and through the improvement or retirement processes. As vulnerabilities are identified in acquired software, they are entered into our vulnerability tracking tool and then evaluated, rated for criticality, and tracked to ensure all necessary corrective actions are taken.

Figure 3 describes the HPE SDL showing each stage from the initial product concept to sustaining the product until its end of life.

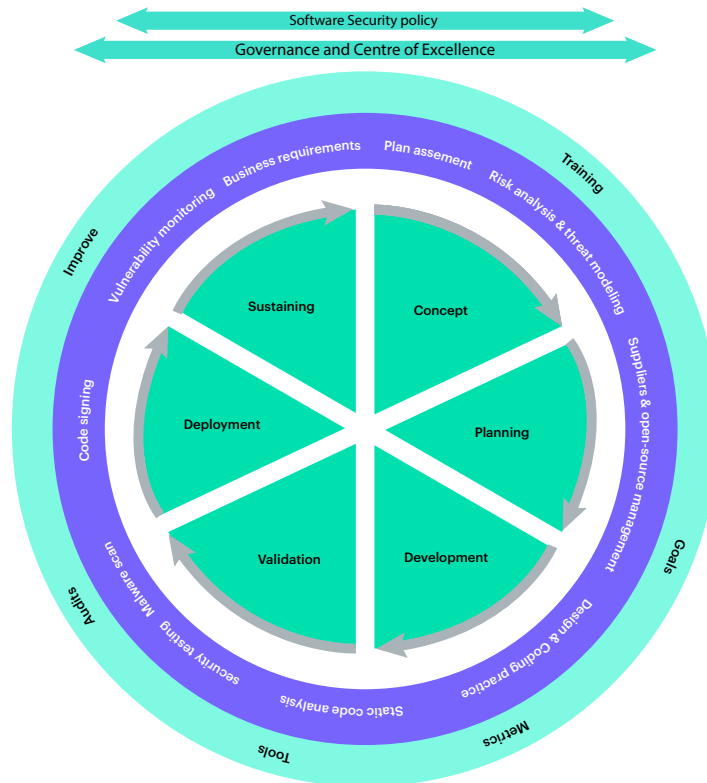


Figure 3. The HPE secure development lifecycle

Creating trusted environments

With sophisticated cybercriminals targeting the manufacturing process and supply chain, today's threat landscape impacts every phase of the technology lifecycle. Continuous cybersecurity protection is now a critical requirement for organizations seeking to adopt and evolve to zero trust security-enabled architectures and business models.

Mitigating cybersecurity risks and preventing attacks in the supply chain is essential to provide secure products and services. At HPE, we believe our customers need more than this to enable a secure and trusted operating environment effectively. Our customers require comprehensive assurance of the provenance, security, and trustworthiness of all the hardware, firmware, and software needed to operate holistically for a given workload.

Verifying authenticity and tamper prevention

As part of our trusted supply chain program, HPE has enabled platform certificates for selected HPE server models since 2021. Platform certificates are an industry-standard technology, and they help provide reassurance that servers have not been tampered with while in transit between the factory and the customer site. The platform certificate is created and digitally signed by HPE during manufacturing and is stored on the server.

As a promoter and a member of the Trusted Computing Group (TCG), HPE enables an open standards-based, TCG-compliant implementation of platform certificates. It provides the means for our customers to cryptographically validate the state of their HPE servers at any point in their lifecycle using the [platform certificate verification tool](#). HPE provisions servers with initial device identification to further enable a zero trust environment, which allows the cryptographic authentication of HPE servers and HPE Integrated Lights-Out (HPE iLO).

Building a zero trust-enabled architecture from silicon to cloud

The HPE approach to delivering a zero trust-enabled architecture has been

designed to provide improved integrity verification from silicon to cloud while continually monitoring and providing security capabilities that protect infrastructure, operating systems, software platforms, networks, and workloads without signatures, significant performance trade-offs, or vendor lock-in. HPE delivers zero trust-enabled cloud-native building blocks with integrity verification that's initiated in our supply chain and is anchored in the silicon root of trust from HPE. It starts from the time of manufacture — with zero trust-based confirmation initiated at first boot before anything connects to the network. Here are some cornerstones to provide a secure foundation for the zero trust-enabled architecture built into the HPE infrastructure lifecycle:

- Provision of security anchors for zero trust-enabled architecture
- Development of infrastructure with features that help ensure trusted status
- A common foundation of risk management practices, controls, and assurance activities
- Secure software development framework

By assembling products in highly secure manufacturing facilities, HPE provides increased levels of security for a growing number of organizations with very high-security needs. These organizations operate in critical infrastructure market sectors and require verifiable cyber assurance and zero trust assurances. These assurances help the organization follow evolving and emerging security and privacy regulations. They also enable the organizations to gain a competitive advantage underpinned by a robust enterprise-wide commitment to a secure supply chain while extending security through product design, sourcing, and finishing.

Figure 4 shows the security attestation service from HPE GreenLake cloud, along with the layers of security we are designing into the platform from the device level up to the workload level.

HPE GreenLake platform

Security attestation service - Stronger integrity improves trust

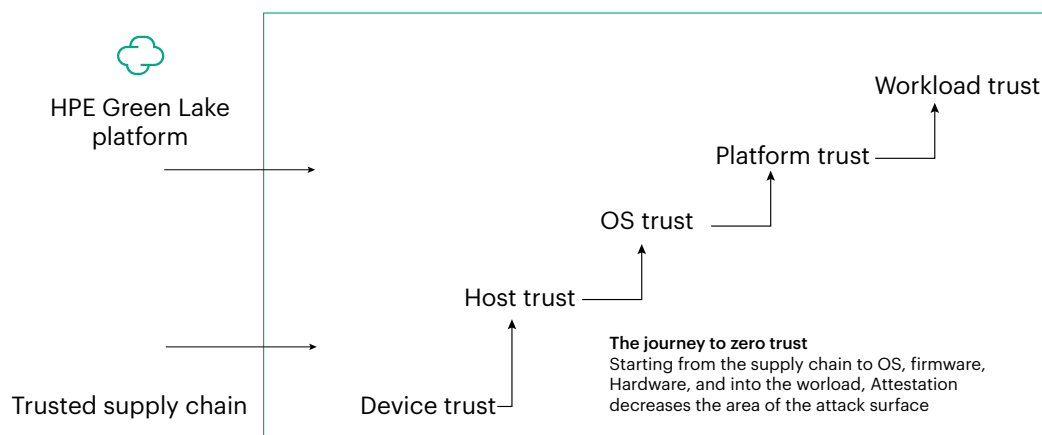


Figure 4. The zero trust journey with the HPE GreenLake security attestation service

Cybersecurity risk management in the supply chain

HPE aligns and deploys expertise across the supply chain to ensure that the right security measures are applied and that the business partner ecosystem interacting with the HPE supply chain has appropriate security measures in place. Our supply chain cybersecurity risk management practices are applied to critical aspects of the supply chain including sourcing components from material suppliers, warehousing, production and distribution processes.

Stringent cybersecurity controls are applied to sourcing and manufacturing processes for new product development as well as the ongoing sustainment of our products and replacement parts. HPE applies highly robust supply chain security controls that include ongoing assessments, risk-based security audits, program monitoring, inspection of electronic parts, component traceability and materials control processes.

Supply chain resiliency

In recent years, the global pandemic and geopolitical environment have brought increased attention to the availability of critical components, as well as the integrity of manufacturers. To mitigate any cybersecurity risks and for a continuous supply of components, HPE maintains a global network of trusted suppliers. It continuously optimizes the diversity of our supplier base so that we can provide products and services to our customers in all geographic locations.

HPE can predict, manage, and respond to potential supply chain disruptions using an artificial intelligence (AI)-powered modeling solution that can advise on supply constraints for raw materials and commodities before they occur. Our solution considers multiple layers of suppliers' geographic locations. It uses advanced probabilistic models to predict various potential supply chain disruptions stemming

from geopolitical events, weather and natural disasters, and other economic intelligence on a global level.

The insight into early detection and strategic maneuvering helps HPE to provide quality products to our customers and avoid predictable delays. HPE's capability to leverage cutting-edge technologies such as AI in a complex, global supply chain environment strengthens the resiliency of our supply base and, most importantly, reinforces the resiliency of our customer's business operations.

Trusted sourcing

HPE employs an extensive and comprehensive process for evaluating and assessing suppliers as part of the supplier's lifecycle management process. The supplier selection and approval process consist of reviewing the supplier's engineering and technical capabilities, quality control processes, and physical site security, as well as a series of other cybersecurity assessments. Once approved, HPE leverages an approved vendor list (AVL) with trusted suppliers for sourcing components. We continuously monitor an array of credible sources for reports of suspect counterfeit parts, malware, questionable sources of supply, and potential bad actors, and we respond as appropriate.

Restricted suppliers

HPE maintains a list of restricted suppliers and does not use components from those organizations, nor any of their subsidiaries or affiliates, in any product designed and/or manufactured by HPE. We also share this restricted supplier's requirement with our suppliers. To learn more about the HPE list of restricted suppliers, contact your HPE account representative.

Practices to reduce cybersecurity risk

HPE cybersecurity supply chain risk management (C-SCRM) practices help our customers reduce their risk exposure to security threats, data breaches, and other security incidents that may arise from using HPE products and services. By implementing rigorous and comprehensive C-SCRM practices, HPE can identify and mitigate potential security risks throughout our supply chain. This leads to improved business outcomes, reduced risk, and liability, and, most importantly, greater peace of mind for customers.

The program serves as an additional mechanism to find potential cybersecurity gaps and deficiencies nonconforming with our cybersecurity standards and best practices. Achieving this places HPE in a strong position to evaluate and understand risks and work together with a diverse ecosystem of suppliers to mitigate risks.

The HPE supply chain cybersecurity team maintains a robust program for developing policies and standards for HPE operations and our supplier's operations that address current risks and threats in the industry. Our C-SCRM program includes a supplier's risk management process and continuous monitoring of the supplier's cybersecurity compliance. Cybersecurity audits and assessments of our suppliers and manufacturing centers are regularly conducted. It helps reduce our customers' cybersecurity risk by helping ensure that the components and services that make up HPE products are secure and free from vulnerabilities that attackers can exploit.

HPE supports and encourages innovative solutions and the development of new cybersecurity practices by recognizing outstanding performance. We have developed an annual recognition program for suppliers and manufacturing centers who exhibit exemplary cybersecurity practices. This program helps promote continuous improvements that help eliminate or mitigate cybersecurity risks in the supply chain.

Counterfeit part detection and avoidance

The HPE counterfeit part detection and avoidance process within our supply chain risk management framework complies with regulations, standards, and best practices requirements. HPE is also an active member of the Government Industry Data Exchange Program (GIDEP) for monitoring and reporting suspected and confirmed counterfeit parts. If any of our suppliers are aware of, or have a reason to suspect that, any electronic part or end item, component, part, or assembly containing electronic parts may contain suspect counterfeit parts, they are required to report it. The supply chain cybersecurity team expeditiously investigates any reports of suspect counterfeit, and if a counterfeit part is confirmed, HPE will report the incident to customers, suppliers, manufacturers, the GIDEP program, and other applicable government officials, as necessary.

Our anti-counterfeit (ACF) investigation and enforcement function confronts all touchpoints of the counterfeit business, from the smallest vendors to the largest fabricators, distributors, and producers of counterfeit packaging and components. We work with law enforcement agencies and governments globally to combat the production, distribution, and sale of counterfeit goods.

Secure manufacturing

To provide best-in-class service to our customers worldwide, HPE manufacturing centers are strategically located and protect against cyber threats by preventing physical and informational resources from unauthorized access. As components arrive at the manufacturing centers, parts are inspected for evidence of tampering, as well as quality defects, and then stored in secured locations with restricted access to prevent tampering opportunities.

Hardware cybersecurity assessment

The HPE supply chain cybersecurity team conducts a risk assessment on every hardware product and option at multiple points in the development and manufacturing process. This assessment encompasses checking the components on the BOM against credible sources of information to ensure that each component is cyber secure. This cyber risk assessment takes place at the beginning of the product development process and again in the validation phase as an extra precaution to detect if there are any nonconforming and suspected counterfeit parts.

During the assembly process, every system is functionally tested and undergoes a series of inspections to ensure products are properly configured and secured according to the customer's specifications. HPE follows a 3C strategy for this process, which includes:

- **Configuration:** To check that the product was built according to specification
- **Connectivity:** To determine if all components are properly connected
- **Communication:** To check that all the interfaces are functioning at the expected speed and fidelity

HPE builds, manages, and controls the test executive process, diagnostics development, and test scripts. In addition, HPE owns and designs the infrastructure and content repositories so that no external entities can access sensitive product information during the assembly and testing process. Firmware and software are flashed to ensure that no tampering takes place before the assembly process. Finally, when this extensive provisioning process is complete, finished products are securely packaged.

Packaging

HPE uses security labels with high-tech features enabling product authentication with a high degree of confidence. Product packaging can be and is often sealed with a tamper-evident tape and/or security label for package integrity during transport. Some features allow customers to authenticate products themselves.

— NIST Cybersecurity Framework

HPE is tracking Cybersecurity Maturity Model Certification (CMMC) requirements and implements controls to protect sensitive data including Controlled Unclassified Information (CUI) when required. In addition, HPE applies the NIST Cybersecurity Framework within our C-SCRM program to manage cybersecurity risks and to comply with U.S. federal regulations.

— FIPS Validated Encryption

HPE has an ongoing program dedicated to ensure encryption algorithms and modules are validated to the Federal Information Processing Standard (FIPS) 140-3 standards. Select HPE products are Common Criteria certified.

— US FedRAMP

HPE maintains Federal Risk and Authorization Management Program (FedRAMP) certified cloud offering for HPE Aruba Networking Central and will also be expanding certified offerings for HPE GreenLake.

The packaging tape affixed outside the shipping box is an additional security feature so that the products are secure and untampered. HPE labeling includes the innovative use of holograms, allowing customers to check the authenticity of spare parts they procure while protecting against installing unauthorized, inferior, or counterfeit components and parts into HPE products and solutions.

Traceability and chain of custody

HPE manufactures products worldwide and maintains a diverse supply base to offer our customers high-quality products and services. Given the increase in cyber threats and supply chain attacks globally, there is also increased interest in component provenance and traceability, so HPE employs various mechanisms to provide authentic materials assurance that can be traced back to our trusted sources.

HPE has developed the capability to identify and track components using a commodity tracking process, in which a unique number is assigned to each component, identifying its source, and providing authenticity. In addition, HPE is also investing in the immutable, distributed ledger capability of blockchain together with our factories, suppliers, and logistics providers to provide a chain of custody and as-built data for our customers. These capabilities will add to the measures that detect suspect counterfeit parts and demonstrate the secure transition through the manufacturing supply chain.

Secure delivery

HPE delivers products to our customers by land, air, and sea in more than 150 countries. HPE logistics services focus on the secure delivery of components and products throughout the supply chain from our suppliers to our manufacturing facilities to our customers. HPE is selective about our logistics service providers (LSPs) and maintains security requirements for all LSPs worldwide. Many of our high-value products require unique handling procedures and security requirements, which are specified in the HPE Global Supply Chain Security Policy that our LSPs must adhere to, and details of our security requirements also feature in our contracts between HPE and our suppliers.

HPE logistics services have established a solid operating foundation built on the safety and protection of our products. HPE requires that our logistics service providers and their sub-contractors attain the appropriate certifications for their facilities and in-transit operations, including Transported Asset Protection Association (TAPA), Custom-Trade Partnership Against Terrorism (C-TPAT), and Authorized Economic Operator (AEO) certifications. LSPs must perform annual physical security assessments at facilities, transit lanes, and exchange points and notify HPE immediately if there are any noncompliance events.

HPE requires all LSPs to implement an information security management system and conduct regular information security assessments to further protect cybersecurity. Additionally, all LSPs must seal and lock each door on full containers or trailers prior to delivering them to their destination, and the LSPs must also record the seal numbers for future reference or potential audit purposes.

Security is important in every delivery, and HPE builds the safety and protection of our products into each delivery mechanism. We also recognize that our customers have varying degrees of security requirements for their delivery, which is why HPE offers a range of secure delivery service options that can be customized to meet our customer's unique security needs. HPE offers three levels of security services for delivery worldwide: standard, express, and premium as shown in Figure 5.

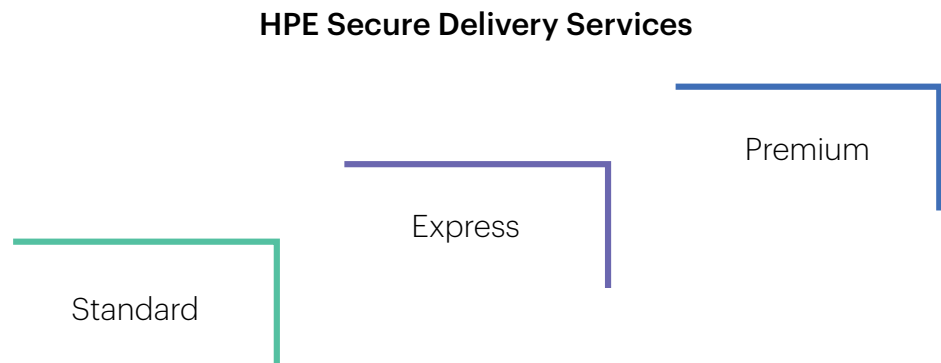


Figure 5. HPE offers three levels of security services including standard, express, and premium options



Customized delivery services can include exclusive use vehicles, dedicated and vetted drivers, pre-delivery site surveys, and armored trucks or armed escorts where additional security is requested. While HPE tracks and monitors all shipments worldwide, we also offer a VIP GPS tracking service so that our customers can track the exact location of deliveries in real-time using GPS technology. Sensors inside the trailer or container can be affixed to the shipping box and alert the receiver if the trailer was opened unexpectedly. Regardless of which service is selected, HPE has a solid foundation of safe and protective programs employed for every delivery while also offering our customers flexibility to tailor unique security features into their delivery.

Sustaining operations and spare parts

HPE provides customers with access to authentic, high-quality replacement parts and components that have been manufactured and tested by HPE or its authorized suppliers. This helps to increase the security of the replacement parts used in HPE products and protect against vulnerabilities that may be introduced by cyberattackers in the supply chain. HPE utilizes a network of approved suppliers authorized to sell HPE spare parts and adhere to our cybersecurity policies and standards as part of the C-SCRM program. We work with original equipment manufacturers (OEMs) to create specific HPE firmware, drives, and software that provide optimized performance, manageability, and security.

Hardware security

The silicon root of trust from HPE — HPE has developed a silicon root of trust that

creates a digital fingerprint in the silicon and helps ensure the server will not boot with compromised firmware. This feature protects against firmware attacks, detects previously undetectable compromised firmware or malware, and helps rapidly recover the server in case of such an attack.

The silicon root of trust technology verifies the integrity of boot-critical essential firmware consisting of BIOS, BMC, Complex Programmable Logic Device (CPLD), Management Engine (ME), and Innovation Engine (IE), which work together with Unified Extensible Firmware Interface (UEFI) secure boot to secure the integrity of the implementation environment. HPE hardware or firmware is compliant with NIST SP800-147b and NIST SP800-193. The silicon root of trust from HPE binds all the firmware into the silicon before the server is even built as part of the HPE secure compute lifecycle.

Trusted server offerings

HPE Trusted Supply Chain

In 2019, HPE launched the Trusted Supply Chain program to bring together our global supply chain operations and secure supply chain features to provide an increased level of security for a growing number of customers with high-security needs. The initiative is designed to support organizations in critical infrastructure market sectors and those demanding products that offer verifiable cyber assurances for compliance with evolving and emerging regulations and to build a competitive advantage.

The HPE Trusted Supply Chain product offerings provide a new first line of defense against cyberattacks with select servers built to tough security standards in secured facilities. It brings together security, processes, and people to deliver protection for the most sensitive applications and data even before the server is built.

The [HPE Trusted Supply Chain product](#) offerings and the [Global Server Security Optimization Service \(SSOS\)](#) start with corruption-free server manufacturing and auditing the integrity of every component (including hardware and firmware). By adding this optional security upgrade intended for organizations with enhanced security and compliance needs, the customer gets a server with an uncompromised lifecycle.

- **Hardened security built in:** HPE Trusted Supply Chain product offerings initiate high-security features during the manufacturing process and harden the protections designed into select HPE products with unrivaled supply chain visibility and standards compliance, providing a 360-degree view and mitigation plan for current and emerging cyber threats.
- **Trusted authenticity:** HPE Trusted Supply Chain doubles down on protection by helping ensure the product manufacturing process adheres to the strictest sourcing, inspection, and traceability standards.
- (Optional) **Country of Origin USA:** Assembled and tested in secure US facilities.

The HPE Trusted Supply Chain product offerings for the US and the Global Server Security Optimized Service include the following features:

- HPE iLO high-security mode enabled to activate the FIPS Validated Encryption module
- UEFI secure boot
- BIOS into server configuration lock with transit mode enabled (emailed password to email address on S4 Sales Order)
- Intrusion detection latch installed (as supported)
- Secure delivery services to end destination
- (Optional) HPE Trusted Supply Chain products are assembled in the US with a holographic sticker featuring the US flag affixed to the server chassis

Applying these server options to the selected HPE server models helps ensure it is hardened by turning on advanced safeguards in place against cyberattacks throughout the server lifecycle. An HPE iLO license provides a high-security mode capability, along with compatible intrusion detection device option kits for the full Global SOSS.



Improving end-of-lifecycle management

Throughout the supply chain, any materials that are found to be nonconforming, including counterfeit parts, are quarantined, purged, and segregated from acceptable materials at the factory and, subsequently, destroyed to prevent re-entry to the HPE supply chain.

HPE maintains comprehensive recycling and disposal policies to destroy data-containing devices so that any information part of the device is properly removed and is not at risk of being shared with nefarious third parties. In addition, recycling and disposal vendors are screened and approved before use and regularly audited to ensure compliance with local laws and HPE policies.

In addition to these risk mitigation policies, HPE also provides product features to ensure sensitive data is removed when a product is ready for recycling or disposal.

One-button erase enables selected HPE servers to be completely purged of all data with a single command and helps ensure that no data can ever be recreated. This feature is critically important at the natural end of life of a server because it uses crypto-erase technology compliant with NIST requirements so that no data can be recovered for nefarious purposes.

Summary

HPE is a leader in the ICT industry for supply chain cybersecurity. As a partner and supplier to our customers, we recognize the importance of secure software and hardware development, enabling the availability of parts from trusted sources, building products with advanced security features, and accessing data that is protected within secure environments.

As cybersecurity threats evolve, HPE continues to identify and mitigate cybersecurity risks within our supply chain and provide secure products so our customers can concentrate on their business goals. As we continue to innovate and advance how people live and work, we also continue to address cybersecurity as a critical priority and apply cutting-edge technologies to our products and supply chain ecosystem.

HPE continues to provide our customers with high-quality and secure products and invest in our supply chain operations, making it more secure, resilient, and transparent.

Learn more at

[HPE.com/us/en/solutions/security.html](https://hpe.com/us/en/solutions/security.html)

Visit HPE.com

[Chat now](#)

© Copyright 2025 Hewlett Packard Enterprise Development LP. The information contained herein is subject to change without notice. The only warranties Hewlett Packard Enterprise products and services are set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. Hewlett Packard Enterprise shall not be liable for technical or editorial errors or omissions contained herein.

a00134892ENW, Rev. 2

HEWLETT PACKARD ENTERPRISE

hpe.com

