



HP Inc. Supply Chain Security

Safeguarding the Modern Supply Chain



Table of contents

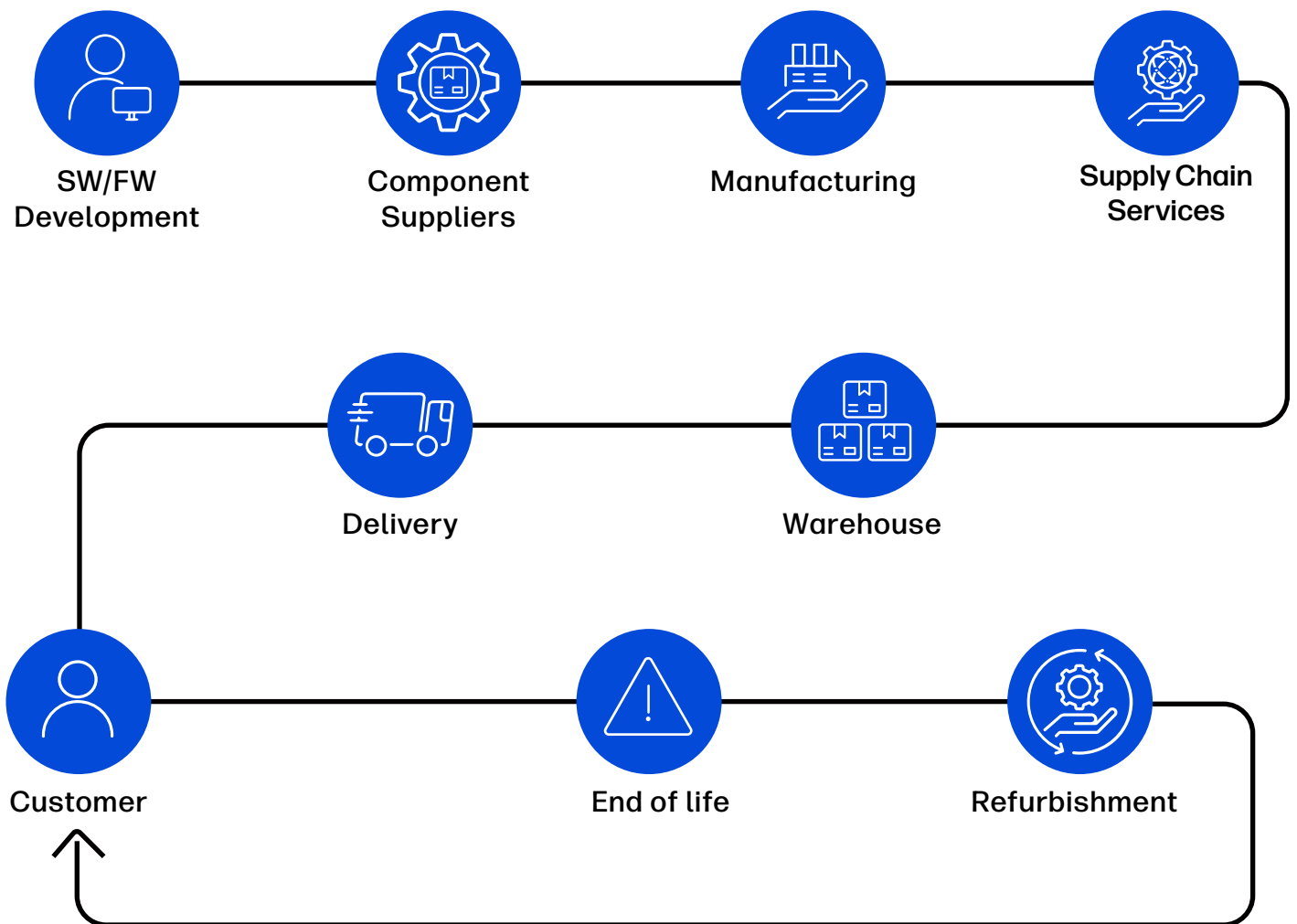


HP Supply Chain - Safeguarding the Modern Supply Chain	3
Overview	4
Security at HP	4
HP Security Development Lifecycle (SDLC)	4
Information security	5
Personnel security	5
Security from sourcing to distribution	5
Supplier relationship management	6
Resilience	6
Counterfeit prevention	6
Secure manufacturing environment	7
PC Software imaging security	7
Printer firmware loading security	7
HP Physical security protection	7
Delivery	8
HP packaging security and tracking	8
Supply Chain Services	8
HP product customizations	8
Image and Application Services	8
Dynamic Configuration Services	8
HP Sure Admin	8
Custom System Setting Services	8
Custom Security Asset Tagging	9
HP Tamperlock	9
Security integrated into our product	9
Personal computers	9
HP Endpoint Security Controller	9
Enterprise Security Edition	9
Sure Start Virtualization Protection	10
Firmware Lock	10
HP Platform Certificate	10
HP Sure Admin	10
HP Protect and Trace with Wolf Connect	10
Secure Operating System Recovery	11
Printers	11
Hardware Embedded Security	11
Operational Security	11
HP Original Cartridge	12
Refurbishment	12
Conclusion	13
Certifications	13

HP Supply Chain Safeguarding the Modern Supply Chain

“ One thing is clear: future supply chain disruptions won’t look like the past. The companies that thrive will be those that plan for every possibility. That means moving away from rigid, outdated planning models and embracing adaptive supply chain planning. ”

Ernest Nicolas,
Chief Enterprise Operations Officer



Threats can happen
anywhere along the lifecycle

Overview

Purchasing PCs, laptops, or printers is a long-term commitment, with many businesses extending device lifespans to meet environmental, social, and governance (ESG) goals. Choosing the right devices is essential but complex, requiring procurement teams to balance cost, performance, reliability, and resilience.

HP's December 2024 Wolf Security report highlights the growing importance of platform security—protecting hardware and firmware to strengthen cybersecurity defenses. In a global study, 81% of IT decision-makers agreed that securing these layers is critical, yet 68% admitted that hardware and firmware security is frequently overlooked in total cost of ownership (TCO) models. This oversight contributes to long-term security gaps, increased administrative burdens, and higher operational costs.

HP follows proven security and privacy principles throughout the product lifecycle—from design and manufacturing to delivery, ensuring a secure supply chain. In addition to secure supply chain practices, our products feature industry-leading security features for protection, detection, and recovery, all designed to safeguard your devices. HP's cybersecurity program is built on a unified approach to supply chain and product security.

Our supply chain security follows the U.S. Government's NIST 800-161 Supply Chain Risk Management Practices, the Open Trusted Technology Provider™ Standard (O-TPPS), and guidance from top cybersecurity experts and HP's internal risk analysis team. Our Product Cybersecurity Standard establishes strict requirements to protect product integrity across the entire supply chain lifecycle.

Security at HP

HP Security Development Lifecycle (SDLC)

HP product teams follow the company's Security Development Lifecycle (SDLC) when developing new features and functionality, while HP cybersecurity specialists conduct reviews throughout the process. The SDLC process for products and components include:

- Comprehensive security reviews of architectures and designs
- Threat analysis of new features and products, including attack surface analysis
- Static and dynamic code analysis, adhering to secure coding practices from the Open Worldwide Application Security Project (OWASP)
- Application penetration testing based on threat assessments, using industry-leading vulnerability scanners

Through this process, HP identifies and mitigates security risks. HP's Product Security Response Team (PSRT) investigates vulnerability reports from suppliers, security researchers, and even the public. With support from HP development teams, PSRT ensures all verified vulnerabilities are addressed, releasing patches and security bulletins in a timely manner.

Information security

HP's internal IT environment is secured through controls such as system hardening, virus and malware protection and mitigation, strong password enforcement, multi-factor authentication, email attachment scanning, system and application patch compliance, intrusion prevention, firewalls, and robust disaster recovery and business continuity plans.

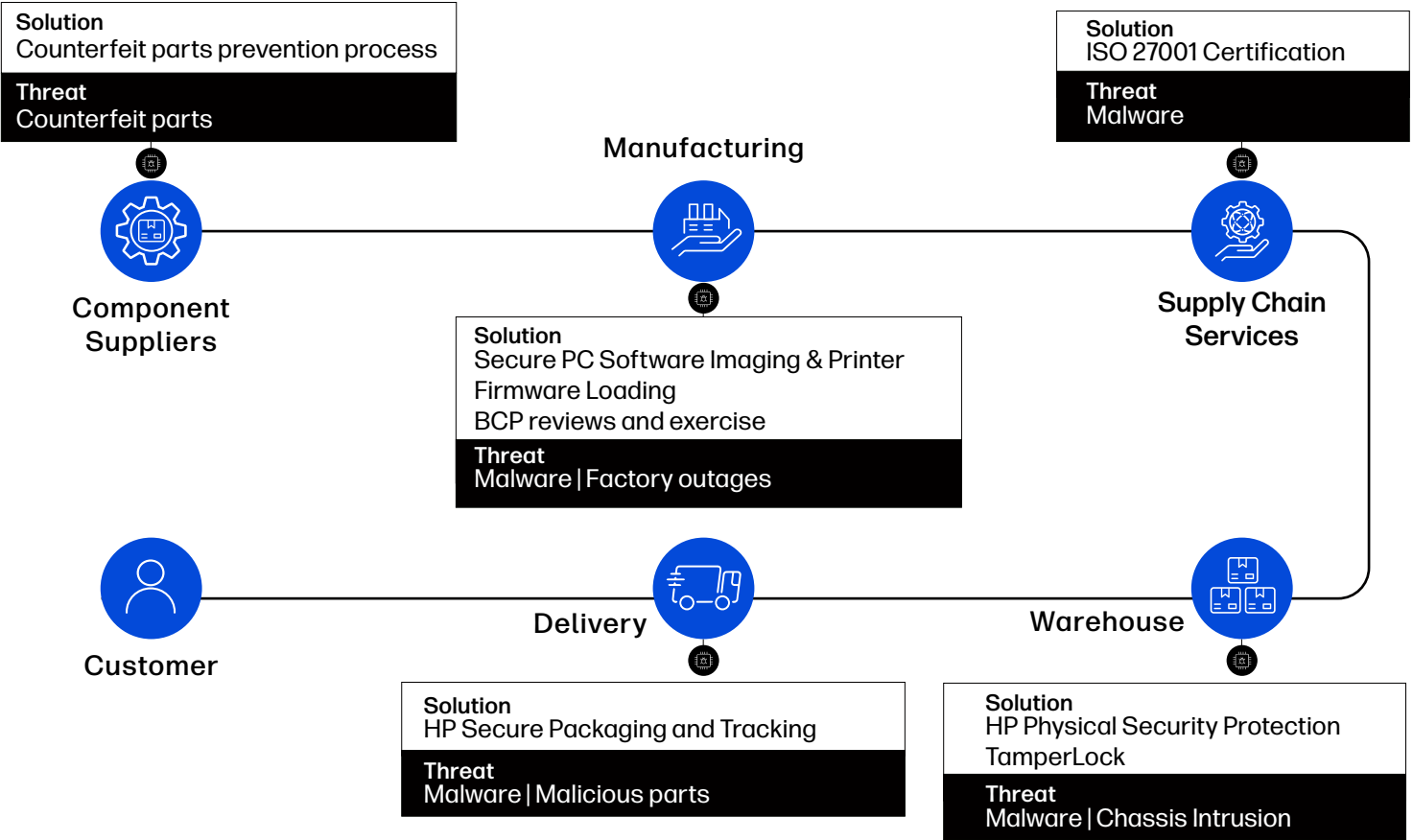
HP employs the best practices—including restricting access and limiting user account permissions—to reduce access to critical data. These practices ensure that access to sensitive information is only granted to individuals to a degree needed to perform their assigned duties.

Personnel security

Security is integrated into our corporate culture at HP. To promote a positive security culture, we recognize outstanding security behavior from our employees. HP security awareness standards include security awareness training, phishing exercises, newsletters, and targeted cybersecurity training for employees.

HP policy requires employees to go through pre-employment checks, dependent upon country laws and worker counsel requirements. This process includes security background checks, identity verification, and application information verification as applicable and permissible by law. HP employees and contractors sign confidentiality agreements that protect intellectual property, customer information, and other sensitive data not only during their tenure as employees, but also after they leave. HP suppliers and partners are held to the same high security standards.

Security from sourcing to distribution



Supplier relationship management

HP's supplier selection process begins with our procurement specialists working alongside our engineering team. Together, they take into consideration technical requirements, country and region needs, cost, financial health, manufacturing and supply chain capabilities, quality, and more. HP's documented standards hold our suppliers accountable to maintain a secure infrastructure, provide authentic parts from trusted suppliers, and maintain counterfeit avoidance programs.

- HP requires supply chain partners and resellers to comply with all legal and regulatory requirements involving system security, global trade, and customer privacy
- Oversight – A dedicated Product Supply Chain Cybersecurity Compliance team provides governance and conducts risk identification and remediation activities
- Standards – HP's product cybersecurity standard for suppliers sets requirements for component sourcing, product design, manufacturing, storage, and transportation
- Validation – Programs and processes are in place to monitor implementation and to isolate and resolve issues

To ensure compliance, HP completes ongoing security reviews of our suppliers.

Resilience

Resilience is a fundamental part of HP's supply chain strategy. Our agile approach gives us the ability to adapt to challenges and potential disruptions while maintaining our commitment to deliver products and services to our customers.

HP's supply chain takes a holistic and interconnected approach. We work with global partners to purposefully develop manufacturing capacity in key locations around the globe. Together, we adapt as needed to adjust production to alternative locations to improve flexibility, reduce cost, and mitigate risks for our customers. We identify key components and ensure a multi-source strategy to safeguard availability of supply.

At HP, our focus on a resilient supply chain allows us to optimize our operations, remain competitive, and deliver what our customers need, when they need it.

Counterfeit prevention

HP's Counterfeit Part Detection and Avoidance System aligns with the Department of Defense Federal Acquisition Regulation Supplement (DFARS) 252.246-7007 criteria and follows the best practices to prevent or identify and eliminate counterfeit parts throughout our supply chain. We assess all component providers and manufacturing facilities for compliance with counterfeit prevention standards such as employee training, tracking parts from the supplier to the HP product manufacturing facility, inspecting and testing of electronic parts, and purging if counterfeit parts are identified. Our procurement processes verify that materials are sourced only from HP's approved vendors and match the bill of materials.

HP tracks all claims of counterfeit or tainted products for resolution. This includes, where applicable, investigating and assessing, determining root causes, preventing repeats, and removing non-compliant products from production and distribution channels.

HP reports threats and vulnerabilities to relevant governments to meet or exceed applicable regulations and industry reporting standards. We also report to our customers, partners, and stakeholders so they can take their own action in response.

Secure manufacturing environment

Manufacturing security begins with a secure factory environment. Our manufacturing facilities must meet our cybersecurity standards, which include system hardening, patch management, virus detection, protection and mitigation against malware, strong password enforcement, intrusion prevention, firewalls, and robust disaster recovery and business continuity plans. In addition, HP implements technology and process security measures that allow us to:

- Segment and isolate factory and supply chain networks
- Require access badges for employees and partners
- Audit for adherence to cybersecurity standards and manage remediation activities

PC Software Imaging Security

HP secures the loading and licensing of software images and firmware on all our PCs, which aligns with HP's strategic objective of producing highly secure products.

The software image is comprised of the OS, drivers, requested third-party applications, and diagnostic tools required to support the operation of the system. Software images are transmitted to factories via secure channels and hosted in a secure environment. The image load process is tightly controlled. The software image is hashed and checked at every step of the process, from development to loading on the PC. The image load process is ISO 27001:2013 certified.

Printer Firmware Loading Security

Like a PC's operating system, printer firmware coordinates hardware functions, runs the control panel, provides network security, and determines what features are available when printing, scanning, or emailing. Firmware installed in the factory is validated, so that only authentic, known, good HP code—digitally signed by HP—is loaded onto the device. During the device startup process, if the code signature is not validated, the device reboots to a secure recovery state and waits for a valid firmware update. A control panel message notifies the user of the identified invalid firmware code.

HP Physical security protection

At HP factories and warehouses, we deploy dedicated security teams, theft prevention personnel, strict access controls, alarm systems, video surveillance, motion detection, and restricted high-value storage areas. Regular security audits ensure these measures remain effective and ahead of evolving threats.

Want a closer look at how HP safeguards its physical supply chain? Explore our Global Physical Supply Chain Security whitepaper for an in-depth breakdown of our security strategies and protocols.

Delivery

HP Packaging Security and Tracking

HP has the technology and processes in place to provide security against tampering during production, storage, and transportation, all the way to the end customer. For products in transit, we track and monitor shipments to review anomalies, such as route deviation or unscheduled stops, to ensure products arrive securely at their intended destination. HP offers additional physical security features like HP TamperLock and HP Sure Admin which are described in more detail below.

HP complies with TAPA Facility Security Requirements (FSR) and Transportation Trucking Security Requirements (TSR). These requirements include secure handling and storing, tamper-evident packaging, hard-sided trailers that can be locked, GPS tracking with door-opening detection, and approved secure parking sites for long breaks by trucking personnel. In addition to the TAPA Supply Chain Security Standards, HP also enforces and audits our own Supply Chain Security Standards that exceed the TAPA requirements.

Supply Chain Services

HP product customizations

HP offers over 40 customization services that are performed in the factory, during the build process, to save customers both time and money. Please refer to HP's Configuration Services website for additional information.

Image and Application Services

Image and Application Services install customer-specified software images and applications onto HP PC products during the manufacturing process. Customers can provide their ready-to-install PC software image or request us to build and load it for them. We systematically scan, test, and validate the software images prior to mass distribution. For PCs purchased with an embedded OS recovery drive, we can load the customer-desired image on an embedded drive, so it is available for quick image restore.

Dynamic Configuration Services

HP's Dynamic Configuration Services allow customers to extend their imaging environment into HP's factories or staging centers through a secure VPN connection—giving them direct control over key configuration activities for new PCs prior to shipment. With this connection, customers will be able to directly manage and configure their images, applications, domain join, HDD encryption, BIOS settings, and unit personalization.

HP Sure Admin

HP Sure Admin, a “no-password required” BIOS management mechanism, can be installed and setup using customer specific keys.

Custom System Setting Services

Factory Custom System Setting Services configure PC BIOS parameters as per customers' requirements. Through customization of BIOS settings, we help ensure seamless deployment of PC units into the company environment for immediate productivity.

Custom Security Asset Tagging

HP Labeling and Tagging Services are available globally on most HP commercial notebooks, workstations, thin clients, desktops, and retail point of sale (RPOS) solutions. HP’s factory process provides labels that are printed consistently and affixed securely according to manufacturer standards and customer requirements.

HP Tamperlock

HP TamperLock solution combines hardware-enforced security with sensors to detect if the PC case has been opened. Policies on a detected event can include blocking boot until valid BIOS administration credentials are entered, clearing the Trusted Platform Module (TPM) to delete all user keys such as BitLocker keys, and powering off the system when the cover is removed.

Security integrated into our product

Personal computers

PCs are vulnerable to physical attacks when moving through the supply chain or when unattended. Nine out of ten Chief Security Officers believe that physical security of systems is challenging to operations. HP PCs are engineered with industry-leading security technologies to protect systems from design to end-of-life.

HP Endpoint Security Controller

The heart of HP PC security is the Endpoint Security Controller (ESC). Many HP security capabilities utilize the ESC. The ESC is a dedicated chip that validates the integrity of the BIOS and other firmware to enhance the security of every HP business-class PC. HPs’ ESC includes Quantum Resistant cryptography and is ANSSI certified. Governments advise firms to adopt postquantum cryptography for cybersecurity to futureproof against quantum threats and regulations.

Enterprise Security Edition

HP Enterprise Security Edition (ESE) includes multilayered safeguards to protect the PC firmware from physical access cyberattacks. The advanced physical protection bundle gives IT admins visibility into unauthorized firmware and component tampering after leaving the factory and protects the PC firmware from malicious actors.

CAPABILITY	WHAT IT DOES	BENEFITS
 Sure Start Virtualization Protection	Pre-boot protection from malicious or compromised third-party hardware	Prevents third-party firmware from compromised PC
 Firmware Lock	A user-controlled lock executed at the firmware level	Provides stronger protection than an Operating System level lock when PC is unattended
 Platform Certificate	Provides IT admins visibility and detection of unauthorized modifications of device hardware and firmware	Detects supply chain attacks or physical tampering once the device has left the factory

Sure Start Virtualization Protection

Hardware virtualization on the PC isolates and protects critical BIOS code, preventing unauthorized modifications or malicious attacks aimed at tampering with the system's firmware by isolating it within a protected virtual environment; essentially acting as a self-healing mechanism to restore the BIOS to a known good state if compromised.

Firmware Lock

A user-controlled firmware lock can be implemented by your IT organization prior to shipping the system to the user. This stops the system from booting and prevents any malicious firmware code attacks while the system is in transit. HP Sure Admin's cryptographic password-less authentication process is used for the user to unlock their PC.

HP Platform Certificate

A digital certificate enabling customers to cryptographically authenticate the device, verify product provenance back to HP, and detect unauthorized modifications of critical hardware and firmware components. The Platform Certificate complies with the Trusted Computing Group's Platform Certificate Profile Version 1.1 Revision 19 and TCG PC Client Platform Firmware Integrity Measurement Version 1.0 Revision 43.

The platform certificate contains information about the product's build configuration as it left HP's factories. This is essential for mitigating risks of tampering during the supply chain journey from HP to the end user. Administrators can use the platform certificate during intake verification by comparing the components of the received product to those listed in the certificate. The certificate also contains details of the installed Trusted Platform Module (TPM) to securely facilitate provisioning of cryptographic secrets, keys, and certificates and verification of boot-time firmware configurations.

HP also offers a scripting library for integrating Platform Certificate into an enterprise intake verification process. For more information, please see the Client Management Script Library (CMSL) documentation at <https://developers.hp.com/hp-client-management/doc/client-management-script-library>

HP Sure Admin

HP Sure Admin protects PCs from attacks by providing password-less authentication to prevent malicious remote and local BIOS configuration changes. Using PKI, HP Sure Admin can be set up in the factory via HP Configuration Services, or by the customer themselves, after which all BIOS configurations can be done in a cryptographically secure manner. Local administration requires a two-factor authentication type experience where only pre-registered local admins with rights to modify settings on a particular PC are able and authorized to do so.

HP Protect and Trace with Wolf Connect

Managing a fleet of PCs is more challenging than ever in a hybrid work environment. Devices are spread across multiple locations, in various states, and hold both sensitive data and financial value. HP Protect and Trace with Wolf Connect makes it easier to locate, lock, and erase lost or stolen PCs, even if they are powered off or unable to boot.

Secure Operating System Recovery

Restoring a compromised operating system (OS) as soon as possible is key to maintaining device functionality. Because HP Sure Recover is integrated into the hardware and firmware of the device, users can easily restore their operating system to a reliable version.

This recovery can be done in two ways:

1. Local recovery – The system restores itself using an image stored on an embedded recovery drive or a dedicated partition.
2. Network-based recovery – The device downloads the latest approved OS image from a secure cloud location via a wired or wireless connection.

Initiating the recovery can be done using one of these methods: automatic, scheduled, or user initiated. When combined with HP Sure Start, HP Sure Recover can quickly restore not only the OS but also drivers and applications, fixing software corruption seamlessly.

For even faster recovery, devices can restore their OS offline using the embedded recovery drive, which is securely protected by the HP Endpoint Security Controller. HP Sure Recover supports the entire product lifecycle, from factory setup to decommissioning, ensuring devices remain secure and operational.

Printers

HP builds cyber-resilient printers that utilize a defense-in-depth approach to ensure multiple levels of security protection. We partner with independent third parties to conduct penetration testing to strengthen both our printers and the supplies we provide. HP printers have the industry's strongest security, with key technologies that are always on guard, continually detecting and stopping threats while adapting to new ones.

Hardware Embedded Security

The first step of the printer startup lifecycle is to load the BIOS. It is essential that this code is protected since it is the Root of Trust (RoT). HP Sure Start technology validates the integrity of the BIOS code and provides a self-healing capability if the BIOS becomes compromised. The BIOS is hashed and signed with a cryptographic signature that is verified during boot. The device can revert to the original image in the event the BIOS is compromised.

The second step in the startup lifecycle is to ensure that the device only loads HP-authentic code. HP provides dynamic allow list technology that ensures only authentic, untampered, and executable code can run on HP's printers. Allow lists are more effective than deny lists, which are used by antivirus scanners to identify the fingerprints of known malware.

Operational Security

HP Connection Inspector, an HP Labs-patented technology, helps printers stay one step ahead of malware attacks. The technology inspects outbound network connections to determine what is normal and stop any suspicious activity. If the printer detects a network anomaly, it automatically triggers a reboot to initiate HP Sure Start self-healing procedures, and if configured, sends security events to Security Information and Event Management (SIEM) tools, all without any intervention.

HP Memory Shield helps detect malicious attacks on the printer and, if detected, automatically self-heals. The printer is locked down according to its factory image, preventing the execution of any calls or operations that are not manufacturer-defined. Memory Shield uses a hardware-protected solution called Runtime Intrusion Detection (RTID) to actively scan memory for anomalies. If an anomaly occurs, the device performs a reboot, flushing the memory of any potential malware and booting to a known good safe state. If this happens, a security event is generated and can be monitored by various security monitoring tools (e.g., SIEM tools). XGuard CFI from Karamba monitors the execution flow of the printer firmware to help detect and prevent potential zero-day attacks. If there is any change to the execution flow, HP's Memory Shield halts and reboots the device to a safe state.

HP Original Cartridge

Security doesn't stop at the printer. Modern printer cartridges contain microchips that enhance functionality by enabling consumable life tracking, image quality adjustments, and cartridge validation. While these advancements improve efficiency, reliability, and consistency, they also introduce potential attack areas.

Tamper resistance relies on multiple factors, including supply chain security, HP's secure smart card technology, cartridge packaging security (which varies by SKU), and the security features built into printer hardware and solutions.

- Secure smart card technology: Original HP office cartridge chips use the same secure smart card technology found in chip-based credit and debit cards. Since 2015, all Original HP office printer cartridges have incorporated this technology to maximize data integrity and protect against tampering and hacking. This ensures that HP's proprietary code on the chip cannot be altered or replaced. In contrast, non-HP chips may use general-purpose microcontrollers, which could introduce security risks.
- Tamper-resistant HP firmware: HP's proprietary firmware on cartridge chips is permanently programmed and cannot be modified.
- Printer verification of supply authenticity: Built-in verification features help ensure that only genuine HP supplies are used, providing added security and reliability.
- Manufactured in secure facilities: Original HP office-class cartridge chips are certified at Evaluation Assurance Level (EAL) 5+ and/or produced in facilities that have achieved this certification, meeting high-security manufacturing standards.

Refurbishment

Business and IT leaders are under more scrutiny than ever to maximize return on their technology investments, while maintaining employee productivity and satisfaction. Ensuring smooth computing and printing performance for teams is crucial, but continually tightening budgets often pose a challenge. Moreover, organizations have a responsibility to reduce their environmental impact and comply with increasing sustainability regulations.

All renewed HP PCs, printers, and peripherals undergo rigorous refurbishment and inspection processes, utilize genuine HP parts, and are backed by HP support. Our refurbishment partners are held to the same system security, global trade, and customer privacy standards as our manufacturing partners. The same dedicated Product Supply Chain Cybersecurity Compliance team provides governance and conducts risk identification and remediation activities for all our refurbishment partners.

Conclusion

Throughout the product lifecycle, from design to the moment it reaches the end user, HP takes a security-first approach. It's built into how we work with suppliers, how we develop our technology, and how we protect the people who rely on our devices. Whether it's our embedded Endpoint Security Controller or the standards we follow, like NIST 800-161 and ISO/IEC frameworks, our focus is simple: keep our products secure and meet our customers' expectations.

We understand that our customers' security needs evolve with new and emerging technology such as AI. That's why HP continues to invest in advanced hardware-based protections, real-time threat detection, and security-by-design practices that scale across industries and geographies. Whether you're navigating hybrid work models, pursuing ESG goals, or building digital-first environments, HP offers solutions to meet your company's needs. At HP Inc, we're not just thinking about today's challenges, we're building long-term resilient solutions you can trust.

Certifications

HP services and systems have been certified to recognized industry standards:

- ISO Information Security Management certifications: ISO/IEC 27001 and ISO/IEC 27701
- Supply Chain Security Certification ISO/IEC 20243
- Service Organization Control SOC 2 Type 2
- Secure Development Practices Assessment Certification (SD-PAC)
- Common Criteria Certification (CCC)
- Security Requirements for Cryptographic Modules (FIPS 140)
- CSPN Certified awarded by the ANSSI - (French National Agency for the Security of Information Systems)

Please click the following link to see all HP certifications: [HP Certifications](#)

For more information on HP Security, contact any of our worldwide sales offices or visit our website: hp.com/security

© Copyright 2025 HP Development Company, L.P. The information contained herein is subject to change without notice. The only warranties for HP 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. HP shall not be liable for technical or editorial errors or omissions contained herein.

4AA7-4216ENW, June 2025.