HP Inc. Supply Chain Security

Safeguarding the modern supply chain

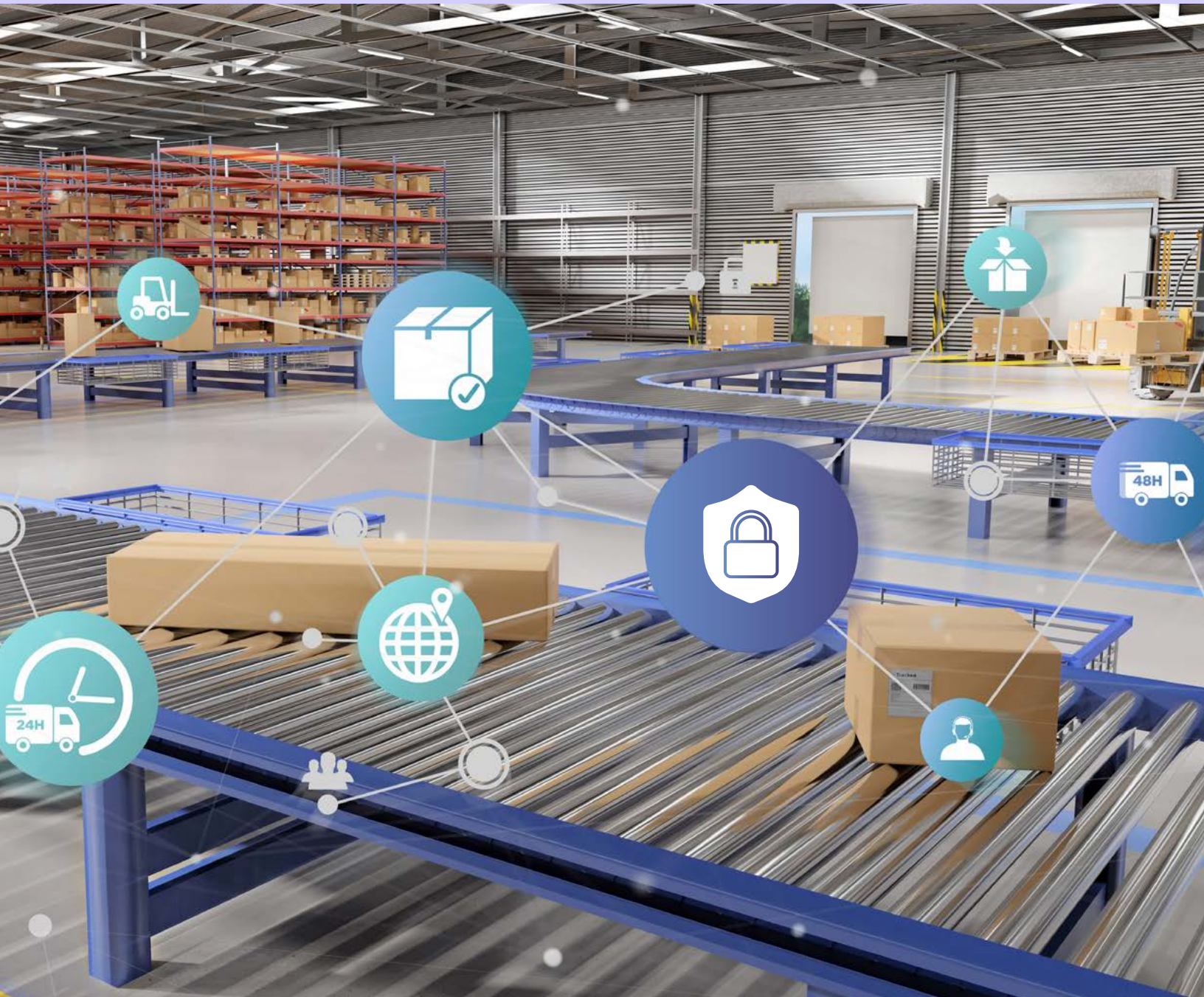


Table of contents

HP SUPPLY CHAIN - SAFEGUARDING THE MODERN SUPPLY CHAIN 3

OVERVIEW 4

SECURITY AT HP 5

HP Security Development Lifecycle (SDLC) 5
Information security 5
Personnel security 5

SECURITY FROM MANUFACTURING TO DISTRIBUTION 6

Supplier relationship management 6
Secure manufacturing environment 6
- PC software imaging security 6
- Printer firmware loading security 6

Counterfeit prevention 7
HP Platform Certificate 7
Physical security 8
Delivery 8
- HP Packaging Security and Tracking 8

SUPPLY CHAIN SERVICES 9

Image and Application Services 9
Dynamic Configuration Services 9
HP Platform Certificate 9
Custom System Setting Services 9
Custom Security Asset Tagging 9
HP TamperLock 9

SECURITY INTEGRATED INTO OUR PRODUCTS 10

Personal computers 10
- HP Endpoint Security Controller 10
- Hardware embedded security 10
- Operational security 10
- PC settings/device anti-tampering 10
- Secure operating system recovery 10

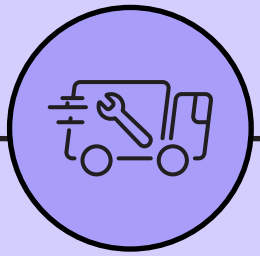
Printers 11
- Hardware embedded security 11
- Operational security 11
- Ink cartridge security 12
- Independent security validation 12

CERTIFICATIONS 12

HP Supply Chain - Safeguarding the modern supply chain

Security at HP

- HP Security Development Lifecycle (SDLC)
- Information security
- Personnel security

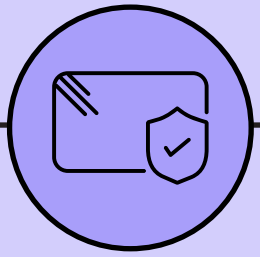


Security from manufacturing to distribution

- Supplier relationship management
- Secure manufacturing environment
- Counterfeit prevention
- Physical security
- Delivery

Supply chain services

- Image and Application Services
- Dynamic Configuration Service
- Custom System Setting Services
- Custom Security Asset Tagging
- HP TamperLock



Security integrated into our products

- Personal computers
- Printers

Overview

PricewaterhouseCoopers' 25th Annual Global CEO Survey (PWC Emerging techs and cyber trends – HP, 15th November 2022) showed that CEOs view cyber vulnerabilities amongst the most significant threats to future corporate growth. Over 25% of companies surveyed had handled data breaches costing more than US$1 million in the past three years. Additionally, up to 11% of CISOs and CFOs reported damages of US$10 million or more. Our HP Wolf Security Threat Insights Report also documented an increase in all forms of cyber-related assaults —from firmware attacks that take control of an entire system to software supply chain ransomware attacks. In an environment of hybrid workers and ever-growing external threats, endpoint devices are the first line of defense for the data and resources we need to protect.

HP follows proven security and privacy principles at every stage of the product lifecycle - from design to manufacturing, all the way to delivery, always with features and protection to keep your supply chain secure. In addition to the security built into our supply chain practices, we have industry-leading security features built into our products. Protection, detection, and recovery are designed and integrated into our devices. Aligned supply chain and product security strategies are the foundation of HP's product cybersecurity program.

HP's supply chain security is based on the US Government's National Institute of Standards and Technology (NIST) 800-161 Supply Chain Risk Management Practices, the Open Trusted Technology Provider™ Standard (O-TTPS), guidance from leading cybersecurity experts, as well as from HP's internal risk analysis group. Our Product Cybersecurity Standard identifies requirements that protect the integrity of our products throughout the entire supply chain lifecycle.

Security at HP

HP Security Development Lifecycle (SDLC)

HP's Security Development Lifecycle (SDLC) integrates security into every phase of our product development - hardware, software, and firmware - from the initial planning and design stages to testing, deployment, and maintenance. Our goal is to create products that are secure by design—ensuring potential vulnerabilities are identified and addressed at every step of the development process.

Product teams utilize HP's SDLC during the development of new product features and functionality while HP's cybersecurity specialists conduct reviews throughout the development lifecycle. HP products and components developed with SDLC include activities such as:

- Detailed security reviews of architectures and designs
- Threat analysis of new features and products along with an attack surface analysis
- Static and dynamic code analysis on our software, following secure coding practices from the Open Worldwide Application Security Project (OWASP)
- Application penetration testing using the results of our threat assessments and utilizing industry-leading vulnerability assessment scanners (e.g., Qualys and Nessus by Tenable)

Through this process, HP identifies and mitigates security risks.

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. Where permissible by country laws, HP works to ensure employees and contractors sign confidentiality agreements that protect intellectual property, customer information, and other sensitive data.

HP diligently strives to ensure HP suppliers and partners are held to the same high security standards.

Security from manufacturing 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.

- Compliance - 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.

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.

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 to 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.

HP Platform Certificate

HP Platform Certificate allows IT admins to assess the authenticity and integrity of a PC and its components, helping uncover any unauthorized changes that may pose a potential threat to the organization. This certificate can be used to verify that the PC is a legitimate HP device. Unauthorized changes could indicate that a PC has been tampered with while traveling through the supply chain, which would be a security risk to the organization. Giving IT the ability to authenticate the integrity of a PC increases the confidence in onboarding and connecting a remote fleet of PCs to the network by reducing the potential risk of a back door security breach.

Physical security

Facilities where HP products and orders are built, customized, or fulfilled must demonstrate compliance with several internationally recognized physical security standards such as those defined by the Transported Asset Protection Association (TAPA), American Society for Industrial Security (ASIS), International Organization for Standardization (ISO), and the Business Alliance for Secure Commerce (BASC).

HP factories have physical security protections such as dedicated site security and theft prevention personnel, access restrictions, alarm systems, video surveillance, motion detection systems, restricted high value cages, and regular physical security audits.

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 exceeds the TAPA requirements.

Supply chain services

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 PLATFORM CERTIFICATE

HP Platform Certificate is a service that creates a secure, cryptographic platform certificate corresponding to the device configuration at the factory, allowing IT to validate its system and component integrity as soon as it reaches their doorstep. This is done by providing cryptographic verifiable artifacts in a certificate signed by the HP Certificate Authority. PC integrity validation with HP Platform Certificate is seamless and scalable. HP securely delivers each HP Platform Certificate via an API, allowing IT to download multiple certificates simultaneously and providing the flexibility to integrate an automated process for downloading these digital certificates and verifying PC integrity into an organization's existing deployment process. HP Platform Certificate complies with existing TCG (Trusted Computing Group) standards.

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 products

Personal computers

HP PCs are engineered with industry-leading security technologies to protect systems from design to end of life.

HP ENDPOINT SECURITY CONTROLLER

HP PCs have a dedicated Endpoint Security Controller (ESC) that performs key security functions as a hardware-based platform Root of Trust (RoT). This RoT is part of a "Secure by design" architecture that powers many other security solutions detailed in further sections.

HARDWARE EMBEDDED SECURITY

HP systems are equipped with HP Sure Start for PCs, a solution that leverages the hardware-based platform Root of Trust (RoT) technology to ensure a secure system startup. HP Sure Start automatically detects, stops, and recovers from firmware attacks or corruption without IT intervention. Every time the PC powers on, HP Sure Start automatically validates the integrity of the firmware to help ensure that the PC is safeguarded from malicious attacks. Once the PC is operational, Runtime Intrusion Detection constantly monitors runtime firmware. In the case of an attack, the PC can self-heal in minutes using an isolated "golden copy" of the firmware and settings.

OPERATIONAL SECURITY

HP Sure Run, an OS software agent, which is monitored by the HP Endpoint Security Controller, continuously monitors and alerts on the operating status of critical processes, services, and applications. The HP Sure Run agent includes kill prevention capabilities, and if the process, service, or application is interrupted, then it is automatically reinstalled. Authorized applications, configured to be monitored by HP Sure Run, including antivirus software and custom applications, are automatically restarted if stopped by an attack.

PC SETTINGS/DEVICE ANTI-TAMPERING

HP Sure Admin protects PCs from attacks by providing passwordless 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 TamperLock combines the hardware-enforced security of HP ESC with sensors to detect and alert if the PC case has been opened. Configured events 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.

SECURE OPERATING SYSTEM RECOVERY

Incorporated into the system's hardware and firmware as a pre-boot solution, HP Sure Recover returns corrupted OS, drivers, and applications to their last approved images. This solution does it seamlessly using pre-boot wireless networking by accessing the configured image from a cloud location. Three recovery methods are available with HP Sure Recover: automatic, scheduled, and user directed. Coupled with HP Sure Start, HP Sure Recover can automatically remediate issues caused by corrupted software including OS, drivers, and applications rapidly and easily. This recovery can also be achieved offline for faster speeds or in case there is lack of network connectivity, by using the embedded OS recovery drive, which is securely protected by the HP Endpoint Security Controller.

Printers

HP builds cyber-resilient printers that utilize a defense-in-depth approach to ensure multiple levels of security protection. 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 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.

INK CARTRIDGE SECURITY

HP office printer cartridge chips are designed for security. Only Original HP Cartridges contain a chip with HP proprietary firmware, designed to be secure and resistant to tampering. Non-HP supplies include chips of unknown origin that may employ untrusted firmware.

Digital tracking through the supply chain for many office cartridges provides end-to-end supply chain validation for resellers and end users. Original HP Cartridges can be tracked and validated throughout their journey from the factory to their use in a printer.

INDEPENDENT SECURITY VALIDATION

HP is the first print vendor to complete all three levels of the Keypoint Intelligence-Buyers Lab (BLI) Security Validation Testing program for both multifunctional printers (MFPs) and traditional printers. HP has earned program seals for Device Penetration, Policy Compliance (using security management software), and Firmware Resilience for its HP FutureSmart v4+ Enterprise firmware platform for HP Enterprise and Managed Printers and MFPs.

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)

Please click the following link to see all HP certifications: HP certifications

For more information

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

4AA7-4216ENW, September, 2023.