Brief

Original HP Printer Cartridges

Supplies are a key element of your office printer security

Your office printer, supplies, and services work together to help protect your device and data. Security features at every step—including the cartridges you install in your HP device—result in end-to-end protection of the world's most secure printers.[1]

Supplies security[2]

Cartridge chip

- Functionality designed for security
- Tamper-resistant HP proprietary firmware prevents modification by third parties
- Secure smart card technology allows a secure transaction between the printer and cartridge

Supply chain

- Chips manufactured in EAL5+ certified facilities
- Digital tracking through HP supply chain[2]
- Tamper-resistant packaging

Dynamic supplies security

- Authentication strategies help protect against counterfeits
- Better printing results

Printer security

Device embedded features[1]

- HP Sure Start
- Whitelisting
- Run-time intrusion detection
- HP Connection Inspector

Self-healing

- HP Security Manager[3] checks and automatically restores printer settings

Firmware updates

- New security threats addressed
- Bug fixes
- New features and functionalities

Security services

Assessment tools available from HP Channel Partners:

- Quick Assess
- SMB Questionnaire

Services available Direct from HP:

HP Smart Device Services

- Remote device management
- Help protect against cyber threats

HP Print Security Advisory Services

- Print security strategy
- Governance and compliance

Supplies security + printer security + security services = **layered, defense-in-depth print system security**

Your office printer, supplies, and services: designed for security

Supplies security[2]

HP chips have functionality designed for security: Only Original HP office-class cartridges contain a chip with HP proprietary firmware that is designed from the ground up to be secure and resistant to tampering. Non-HP supplies include chips of unknown origin that may employ untrusted firmware. Given that there is a data interface from the chip to the printer, an attacker with the right skills and resources may be able to uncover and exploit a vulnerability, taking advantage of this interface to add malicious code.

HP chips contain tamper-resistant HP firmware: The HP proprietary firmware on HP office-class cartridge chips cannot be modified by third parties after production. Some non-HP cartridge and chip suppliers claim their chips can be reprogrammed, and even sell devices online that can modify data elements. Non-HP chips can use general purpose microcontrollers with firmware that can be modified or replaced.

HP chips use secure smart card technology: Original HP office printer cartridges introduced since 2015 use smart card technology that allows a secure transaction between the printer and cartridge. Non-HP chips may use general purpose microcontrollers, which can be vulnerable.

Supply chain security: HP is vigilant about recognizing and mitigating security risks in the supply chain to help protect the chip from being replaced or altered, and reduce the risk of malicious code entering the chip. HP and our partners have world-class manufacturing—carefully managing internal supply chains, working with partners who follow industry best practices on security, and partnering with security experts.

Manufactured in secure facilities: HP chips are certified as EAL5+ and/or manufactured in facilities where products achieved EAL5+ certification.

Specialized construction: Designs and glues contribute to tamper-resistant packaging. The security label on the box incorporates both manual and machine-readable elements, including an identifier for digital tracking through the HP supply chain. HP adds a zip-strip sealed inner package and, for some Asia Pacific countries and products, provides a tamper-evident label on the tear strip. To learn more, see hp.com/go/anticounterfeit.

Dynamic supplies security: HP Print security uses dynamic authentication strategies to help mitigate the risks of counterfeit or non-HP cartridges being used in an HP printer. HP also provides firmware updates that can improve, enhance, or extend the printer's functionality and features, protect against security threats, and may update Dynamic Security. See hp.com/go/learnaboutsupplies.

Printer security[1]

HP Enterprise-class printers include HP FutureSmart firmware, which provides integrity checking down to the BIOS. If the BIOS is compromised, HP Sure Start restarts the device with a safe "golden copy." Whitelisting automatically checks HP firmware during startup; if an anomaly is detected, the device reboots to a secure, offline state and notifies IT. Run-time intrusion detection monitors complex HP firmware and memory operations, automatically stops the intrusion, and reboots in the event of an attack. HP Connection Inspector evaluates outgoing network connections to determine what's normal, stop suspicious requests, and thwart malware by automatically triggering a self-healing reboot. After a reboot, HP Security Manager[3] checks and automatically restores printer settings to your security and compliance policies.

HP Pro-class printers include firmware integrity validation to protect against compromised firmware that could open the device and network to attack. Secure boot validates the integrity of the boot code and can trigger recovery mode. Run-time code protection prevents intruders from adding malicious code when the printer is running. All run-time code memory is write-protected and all data memory is non-executable. Learn more at https://h20195.www2.hp.com/v2/GetPDF.aspx/4aa6-4973ENW.pdf and h20195.www2.hp.com/v2/GetPDF.aspx/4aa6-8438ENW.pdf.

Security services

Assessment tools available from HP Channel Partners:

Quick Assess scans up to 50 HP network printers/MFPs against 15 common security settings, then reports on the level of risk within your print environment.

SMB Questionnaire assesses the organization's overall print security, from security ecosystem to purchasing requirements and policy management.

Services available Direct from HP:

HP Smart Device Services: The HP Smart Device Services platform enables remote device management capabilities and can help protect printers against cybercrime threats.

HP Print Security Advisory Services: HP-credentialed security experts can help you develop and execute a cohesive print security strategy to protect your business and address security governance and compliance. For more information, see hp.com/go/printsecurityservices.

1. HP's most advanced embedded security features are available on HP Enterprise and HP Managed devices with HP FutureSmart firmware 4.5 or above. Claim based on HP review of 2019 published features of competitive in-class printers. Only HP offers a combination of security features to automatically detect, stop, and recover from attacks with a self-healing reboot, in alignment with NIST SP 800-193 guidelines for device cyber resiliency. For a list of compatible products, visit hp.com/go/PrintersThatProtect. For more information, visit hp.com/go/printersecurityclaims. 2. HP office-class printing systems are select Enterprise and Managed devices with FutureSmart firmware 4.5 and up, Pro devices, LaserJet models 200 and up, with respective Original HP Toner, PageWide and Ink Cartridges. Does not include HP integrated printhead cartridges. Digital supply-chain tracking, hardware and packaging security features vary locally by SKU. See hp.com/go/SuppliesThatProtect and hp.com/go/SuppliesSecurityClaims. 3. HP Security Manager must be purchased separately. To learn more, please visit hp.com/go/securitymanager.

4AA7-6186ENW, March 2021, Rev. 7