Original HP: Secure printer cartridges you can trust[1]

HP office devices and Original HP printer cartridges

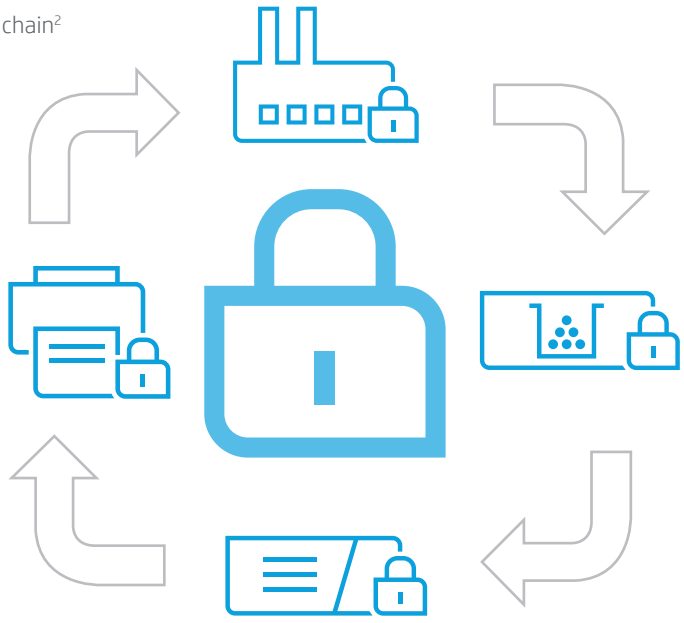
HP incorporates security into every step of the design, supply chain, and production process. By using only Original HP cartridges in your HP device, you can help protect the integrity of your data.

1 Supply chain security

- Focus on security throughout the supply chain
- Protection of the Original HP chip from replacement or alteration
- World-class manufacturing by HP and partners
- Digital tracking through HP supply chain[2]
- Customer verification of package at point of purchase[2]

2 Cartridge chip security

- Designed for security
- Tamper-resistant HP proprietary firmware
- Secure smart card technology
- Printer verification of supply authenticity
- Chips manufactured in secure facilities



3 Cartridge packaging security[2]

- Tamper-resistant packaging
- Security label on box
- Zip-strip sealed inner package
- Tamper-evident label

4 Printer hardware security[1,2]

- HP Sure Start
- Whitelisting
- Run-time intrusion detection
- HP Connection Inspector
- Fleet security management
- Firmware integrity validation
- Secure boot
- Run-time code protection

Original HP office printer cartridges are designed for security[1]

Supply chain security

HP is vigilant about recognising and mitigating security risks in the supply chain to help reduce the risk of malicious code entering the chip. Measures are taken to help protect the chip from being replaced or altered while in the supply chain. 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.

From chip design to programming and installation, packaging and tracking, various security features help provide product integrity for the customer.

Cartridge chip security

HP chips are designed for security: Only Original HP supplies contain a chip with HP proprietary firmware that is designed from the bare metal 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 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 microprocessors 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 for maximum data integrity with best-known resistance to tampering and hacking. Non-HP chips may use general purpose microprocessors, which can be vulnerable.

Printer verification of authenticity: Smart card technology includes a printer verification of authenticity for confidence that supplies are Original HP.

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

Cartridge packaging security[2]

Specialised 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 that is tracked through the HP supply chain. HP adds further security with 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 about HP anti-counterfeit measures for ink and toner cartridges, see hp.com/go/anticounterfeit.

Printer hardware security[1,2]

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 JetAdvantage Security Manager** (purchased separately) checks and fixes any affected device security settings.

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 http://h20195.www2.hp.com/v2/GetPDF.aspx/4aa6-4973eew.pdf and http://h20195.www2.hp.com/v2/GetPDF.aspx/4aa6-8436eew.pdf.

For more information on HP office printer cartridge security, see hp.com/go/SuppliesThatProtect.

[1] HP office-class printing systems include Enterprise-class devices with FutureSmart firmware 4.5 or above, Pro-class devices, and their respective Original HP toner, PageWide, and ink cartridges. Does not include HP integrated printhead ink cartridges. See: http://h20195.www2.hp.com/v2/GetPDF.aspx/4aa6-8436eew.pdf and hp.com/go/SuppliesSecurityClaims.

[2] Digital supply-chain tracking, hardware, and packaging security features vary locally by SKU.

Learn more
hp.com/go/SuppliesThatProtect

4AA7-6186EEW, March 2020, Rev. 4