



HP Wolf Enterprise Security

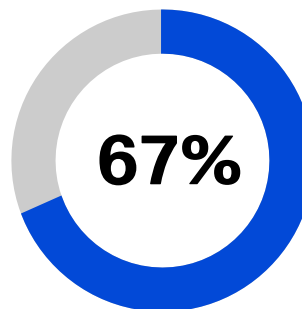
Protecting your Enterprise Printers against the threats you can't see

In today's hyper-connected workplaces, every document, device, and data stream plays a role in your organization's security framework. Yet printers and multifunction devices—often sitting in the open connected to critical networks—remain one of the most overlooked endpoints. These devices process, store, and transmit sensitive information daily, from employee records to financial reports and healthcare data. As cyber threats evolve and regulations tighten, an unsecured print environment can quickly become a doorway for breaches, compliance violations, and costly business disruption.

Global data privacy and security regulations—including GDPR in Europe, HIPAA in U.S. healthcare, and CMMC for U.S. defense contractors—now extend well beyond core IT systems to include every connected device that handles sensitive data, printers included. These frameworks require organizations to safeguard personal, financial, and confidential information throughout its entire lifecycle, from origin and capture to output.

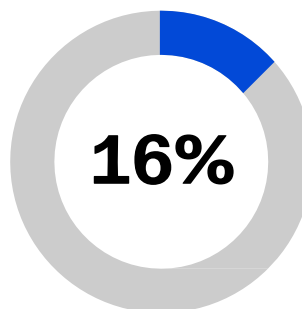
Non-compliance can lead to hefty fines, legal exposure, and loss of customer trust, but the impact often runs deeper: downtime, operational disruption, and long-term reputational damage. A single breach from an unsecured printer can compromise thousands of records, damage stakeholder confidence overnight, and cost organizations up to \$10.9M.²

1. Quocirca's Print Security Landscape 2024 research
2. 2023 IBM Security Cost of a Data Breach Report



Data Loss Incidents

Organizations have experienced print-related data loss due to unsecure printing practices.¹



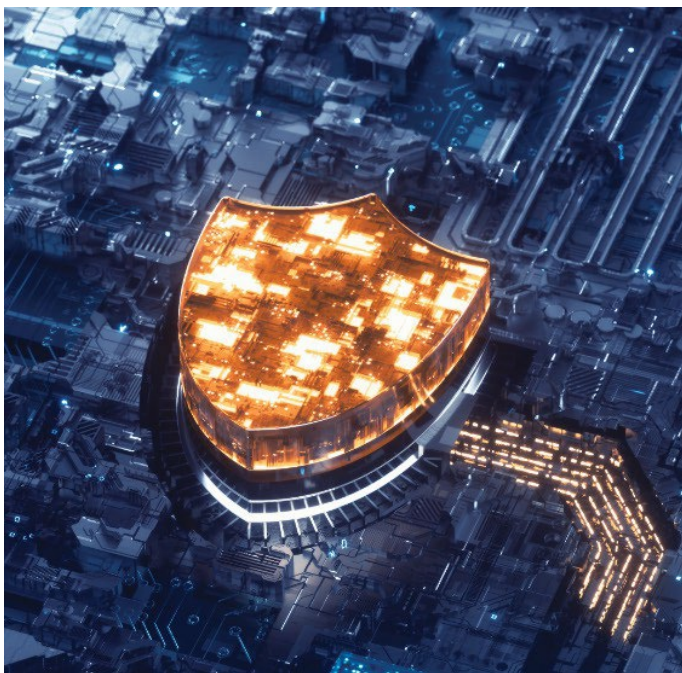
Security Confidence

Organizations are confident in the security of their print infrastructure, decreasing by 3% from the year before.¹

As AI-powered attacks evolve and new technologies like quantum computing emerge, securing every device—including frequently overlooked printers—matters more than ever.

Why Quantum Computing Changes Everything

Quantum computers are about to revolutionize technology, but they also pose a serious risk to today's security standards. Unlike traditional computers, quantum systems can break the asymmetric cryptography that protects your data, devices, and business operations.



Experts predict up to a 34% chance that quantum computers could defeat current encryption by 2034¹, putting sensitive information and device integrity at risk even sooner than previously expected.

56%

Professionals are concerned about “harvest now, decrypt later” attacks, where cybercriminals start collecting encrypted data now and decrypt it once quantum computing becomes viable.²

1. <https://globalriskinstitute.org/publication/2024-quantum-threat-timeline-report/>
2. <https://www.isaca.org/resources/quantum-pulse-poll>
3. https://media.defense.gov/2022/Sep/07/2003071836/-1/-1/0/CSL_CNSA_2.0_F_AQ_.PDF
4. <https://digital-strategy.ec.europa.eu/en/news/eu-reinforces-its-cybersecurity-post-quantum-cryptography>



The Threat to Printers and Endpoints

Printers are often overlooked, but they store sensitive documents, connect to critical networks, and can be exploited as entry points for attackers. Without quantum-resistant security, malicious actors could gain persistent, stealthy control over devices by targeting firmware and BIOS, bypassing traditional defenses.



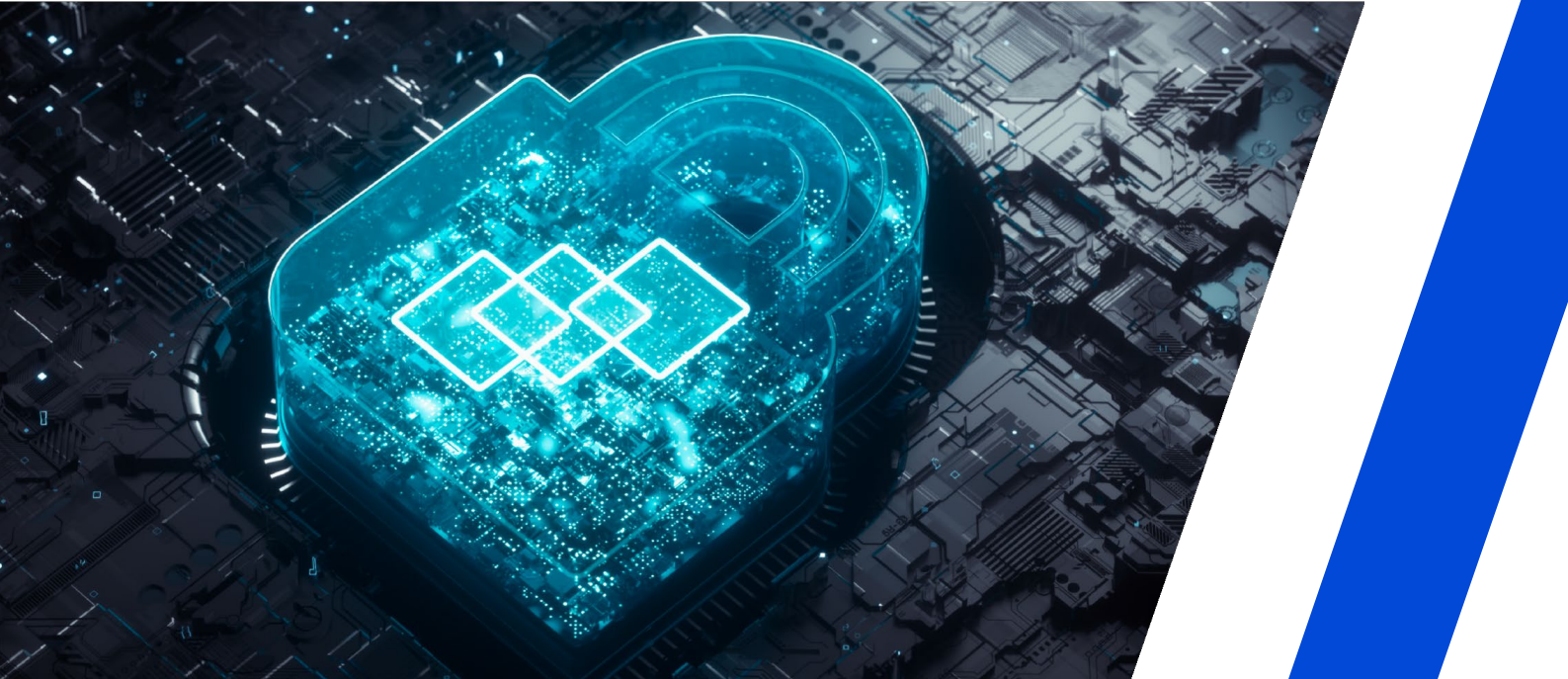
HP's Quantum-Resistant Printers: Leading the Way

HP is pioneering the world's first printers designed to defend against quantum computer attacks. Our devices feature hardware-enforced quantum-resistant cryptography, protecting firmware integrity. HP printers integrate seamlessly with Zero Trust architectures, providing continuous protection at the device level and helping organizations meet fast-approaching regulatory requirements.



Why Quantum Resistance Matters Now

Post-quantum cryptography regulations and standards are still evolving, but the urgency is starting in the US and Europe. The US National Security Agency (NSA) has set 2027 as the expectation for all new systems to adopt quantum-resistant CNSA 2.0 cryptography.³ This means organizations must transition to quantum-resistant devices and cryptography sooner to remain compliant and secure. The European Commission and Member States have published a roadmap and timeline for transitioning to post-quantum cryptography to strengthen long-term cybersecurity, with the protection of critical infrastructure targeted to transition no later than the end of 2030.⁴



Setting the standard for Enterprise Print Security

HP stops what others can't see™

Detect, protect and recover

HP printers have the industry's strongest and most intelligent security¹, with key technologies that are always on guard, continuously detecting, isolating, and stopping threats while adapting to new, zero-day attacks—as AI weaponization expands and quantum computer threats loom. Only HP Enterprise printers automatically self-heal from attacks across the entire life of the printer by triggering a recovery reboot without requiring IT intervention.

World's first quantum-resistant printers²

HP printers are the industry's first printers to protect against future quantum computer attacks at the foundational hardware level below the printer operating system. The BIOS is a set of boot instructions used to load critical hardware components and initiate firmware. HP Sure Start technology with Quantum Resistance works behind the scenes validating BIOS integrity when powering up with embedded hardware enforced quantum-resistant digital signatures. If a compromised version is discovered, the device restarts using a safe "golden copy" of its HP validated BIOS. Quantum resistance protects the printers from hackers attempting to break today's standard asymmetric cryptography (RSA, Elliptic Curve Cryptography).

Hardware-enforced Runtime Intrusion Detection

HP's Memory Shield monitors device memory in real time, right when most attacks occur, to continually detect and stop attacks. Common Criteria Certification (ISO/IEC 15408)³ provides customers with independently validated assurance that a printer's security controls were designed, implemented, and tested against internationally recognized security requirements.

Zero-Day Attack Detection, Isolation, and Remediation

HP Memory Shield's Control Flow Integrity also monitors device memory code execution identifying anomalous code and memory behavior indicative of unknown malware and threats—zero-day attacks that are rapidly growing as threat actors "tweak" known malware giving it new life with Generative AI code manipulation. If a zero-day event occurs on HP Enterprise devices, it will self-heal and notify desired IT and Security staff.

AI-powered HP Connection Inspector—inspects network connections⁴

Stop malware from "calling home" to malicious remote servers, stealing data, and compromising your network. This feature evaluates outgoing network connections to determine what's normal, stops suspicious requests, and automatically triggers a self-healing reboot.

Allowlisting—confirms authentic, digitally signed firmware by HP

Because compromised firmware could expose your entire network to an attack, allowlisting helps ensure the code that coordinates your printer's functions, controls, and security has not been tampered with. Firmware is automatically checked during startup, and if an anomaly is detected, the device reboots to a secure, offline state and notifies IT.

Secure cartridges you can trust⁵

At every step of the design, supply chain, and production process for Original HP office cartridges, security is built-in with tamper-resistant chips, firmware and packaging.

Always-on security and effortless compliance

HP Security Manager⁶ helps you strengthen your print security by automatically assessing devices, enforcing consistent policies, and remediating vulnerabilities across the fleet. It simplifies compliance with centralized policy management, stronger certificate controls, and rapid fleet wide security checks. The result is a more secure, consistent, and lower effort print environment that reduces risk and IT burden.

HP stops what others can't see.™

HP Wolf Security. Built in. Always on. Future-ready.

Learn more: hp.com/go/PrintersThatProtect

1. HP Enterprise MFPs and printers are the first printers with quantum resistant digital signatures in the ASIC protecting initial BIOS firmware integrity and AI-embedded intelligence with HP Connection Inspector network behavior anomaly detection with self-healing, unique features in the industry
2. Based on HP's internal analysis of enterprise printers with preinstalled encryption, authentication, malware protection, post-quantum digital signature, and initial BIOS firmware integrity protection with automatic self-healing recovery finding that no other in-class Printers implement a quantum-resistant cryptographic scheme to protect the integrity of the initial BIOS and firmware as of March 2025
3. Common Criteria Certification is a third-party certification based on Common Criteria Information Technology Security Evaluation ISO/IEC 15408 Standard requirements as of May 2019-2024. Certification applicable to HP Enterprise and Managed devices running HP FutureSmart Firmware version 4.5.1 and later. For more information: <https://www.commoncriteriaportal.org/-files/epfiles/Certification%20Report%20-%20HP%20Intrusion%20Detection.pdf>, applies only to the specific printer models, firmware versions, and evaluated configurations identified in the official certification report. Certification does not imply endorsement of the product by any government or certification body, nor does it guarantee absolute security. The certification confirms conformance to ISO/IEC 15408 standards for the evaluated configuration under the Common Criteria Recognition Arrangement (CCRA). This certification is valid only when the product is deployed in accordance with HP's documented security guidance and within the evaluated configuration. Any changes to firmware, hardware, or security settings outside the evaluated scope may invalidate the certification. For details, refer to the official certification report and the Common Criteria Portal at <https://www.commoncriteriaportal.org>.
4. Behavioral / anomaly-based detection at the device edge: Rather than relying solely on signatures, Connection Inspector watches outbound network patterns (e.g., DNS lookups, destinations, frequency, timing, protocol mix). When behavior diverges from the printer's established profile—or matches suspicious patterns associated with command-and-control (C2) beacons—it is flagged as malicious or risky.
5. See ISO/IEC 20243 2018 Open Trusted Technology Provider™ Standard Certification Register certification.[opengroup.org/register/ottps-certification](https://www.opengroup.org/register/ottps-certification)
6. HP Security Manager is server-based software and must be purchased separately. For details, see Workforce Security Solutions. HP Security Manager brochure (link to brochure: https://h20195.www2.hp.com/v2/GetDocument.aspx?docname=4AA3-9275ENW&jumpid=va_b1js4fygki) For details, see hp.com/go/securitymanager.



HP Wolf Security

Keep your business compliant, secure, and productive with end-to-end print security.

In today's rapidly evolving threat landscape, cyberattacks are becoming increasingly sophisticated and persistent. Modern cybercriminals no longer rely on obvious entry points; instead, they exploit overlooked vulnerabilities and hidden pathways within everyday devices—often operating undetected in areas others cannot see.

HP Wolf Security is engineered to proactively identify and neutralize these threats. Unlike add-on applications or third-party solutions, HP's security is built-in, always active, and seamlessly woven into the DNA of every device, providing continuous, uncompromising protection throughout the life of the printer and MFP.



70%

Of SMBs have experienced a print-related data loss or security breach in the past year¹.

63%

Of large organizations have experienced a print-related data loss or security breach in the past year¹.

\$4.4M

Is the global average cost of a data breach¹.



Protect your investment

Streamline device protection, simplify compliance and proactively close security gaps across your entire print fleet, all from a single trusted solution.



Free IT to do more

Built-in intelligence, Zero Trust Print Architecture with modern device, solutions and personal workflow access, and comprehensive data protection keep your environment resilient—lightening day-to-day maintenance so IT can stay ahead of what's next.



Keep business moving

Prepare for what's next with quantum-resistant printers, verified supply chain integrity, and secure device retirement—protecting your business at every stage.

How HP Enterprise Printers deliver unmatched security:

Embedded protection features:

- HP Sure Start: Most secure BIOS validation and protection with quantum resistant digital signatures at initial boot up and self-healing automatic recovery.
- Allowlisting³: Firmware and software code validation
- HP Memory Shield⁴: Hardware-based runtime intrusion detection with self healing, plus zero-day threat detection and self-healing with Control Flow Integrity
- HP Connection Inspector Technology: Continuous monitoring and network behavior anomaly detection with self-healing automatic recovery.

Firmware Vulnerability Assessment

- HP Firmware Security Tool: Upload device list into the tool and get an immediate fleet view of firmware version vulnerability status and visibility into devices requiring both firmware upgrades and device refresh for rapid upleveling of fleet security posture.

Security Policy Management:

- HP Security Manager⁵: Manages security policies, device identity certificates, and assesses the vulnerability of firmware across entire printer fleet.

Quantum Defense:

- Hardware-enforced quantum-resistant cryptography, protecting BIOS firmware integrity⁶.

1. <https://quocirca.com/content/unseen-risks-in-smb-print-security/>

2. <https://www.ibm.com/think/insights/cost-of-a-data-breach-healthcare-industry>

3. Allowlisting is an embedded security features available in HP Enterprise printers running firmware version 3.7 or newer to prevent security threats

4. Memory Shield™ is available on the HP Color/Mono LaserJet Enterprise M400 series, the HP Mono/Color LaserJet E40000 series and any future HP Enterprise LaserJet devices running FS 5.4 or later.

5. HP Security Manager must be purchased separately. For details, see hp.com/go/securitymanager.

6. Based on HP's internal analysis of business Printers with preinstalled encryption, authentication, malware protection, post-quantum digital signature, and initial BIOS firmware integrity protection with automatic self-healing recovery finding that no other in-class Printers implement a quantum-resistant cryptographic scheme to protect the integrity of the BIOS and firmware as of March 2025.

7. Many security features are not present on older devices or supported with older versions of FutureSmart firmware on Enterprise devices. HP strongly recommends all printers are running the latest versions of firmware to ensure the latest security fixes are present and running on your devices. Contact your HP representative or service provider for details.

Why Quantum Computing Changes Everything

Quantum computers will revolutionize technology, but they also pose a risk to today's standard asymmetric encryption that protects your data, devices, network communications, and business operations.

Why it matters now

Experts have predicted a 34% chance that quantum computers could defeat current encryption by 2034¹, putting sensitive information and device integrity at risk.

However, numerous indications in today's technology landscape point to a more rapid evolution of quantum compute capability than what experts have been predicting.

1. Both IBM and Google have identified their goal to achieve quantum advantage by the end of 2026^{2,3}.
2. There has been an increase in 'Harvest Now, Decrypt Later' (HNDL) attacks by nation-state threat actors since 2022 as they capture and store encrypted data today for later decryption and exploitation with a quantum computer.
3. Governments and industry leaders are already preparing—the U.S. National Security Agency has moved its target for quantum-safe encryption up from 2030 to 2027⁴. In Europe, the EU has launched a post-quantum cryptography roadmap, encouraging Member States to implement Post-Quantum Cryptography (PQC) across infrastructures by the end of 2026 with Critical infrastructures to be PQC-enabled by 2030⁵.

HP's Quantum-Resistant Printers: Leading the Way

HP has pioneered the world's first printers designed to protect against quantum computer attacks⁶. Our devices feature hardware-enforced quantum-resistant cryptography, protecting firmware integrity. HP printers integrate seamlessly with Zero Trust architectures, providing continuous protection at the device level and helping organizations meet fast-approaching regulatory requirements.

Begin planning today for your quantum resistant print fleet rollout over the next 3 years to ensure you have a quantum resistant print infrastructure to defend against tomorrow's quantum threats.

HP Wolf Security is trusted by Leading Organizations

The world's most secure printers. Leading industry experts IDC, Quocirca, and Keypoint Intelligence all agree that HP is an undisputed leader in Print Security⁷.



Secure your tomorrow, today.

Contact your HP partner to learn how HP Wolf Security can safeguard your organization

1. <https://globalriskinstitute.org/publication/2024-quantum-threat-timeline-report/>

2. <https://www.ibm.com/roadmaps/quantum/2026/>

3. <https://blog.google/innovation-and-ai/technology/research/quantum-echoes-willow-verifiable-quantum-advantage/>

4. https://media.defense.gov/2025/May/30/2003728741/-1/-1/0/ICSA_CNSA_2.0_ALGORITHMS.PDF

5. <https://digital-strategy.ec.europa.eu/en/news/eu-reinforces-its-cybersecurity-post-quantum-cryptography>

6. Based on HP's internal analysis of Printers with preinstalled encryption, authentication, malware protection, post-quantum digital signature, and initial BIOS firmware integrity protection with automatic self-healing recovery finding that no other in-class Printers implement a quantum-resistant cryptographic scheme to protect the integrity of the BIOS and firmware as of March 2025.

7. IDC Worldwide Print Security Solutions and Services Hardcopy 2025-2026 Vendor Assessment, Quocirca Print Security Landscape Report 2024, HP is the first and only print vendor to complete all three levels of the Keypoint Intelligence Buyers Lab Security Validation Testing program for printers, earning seals for Device Penetration, Policy Compliance and Firmware Resilience.

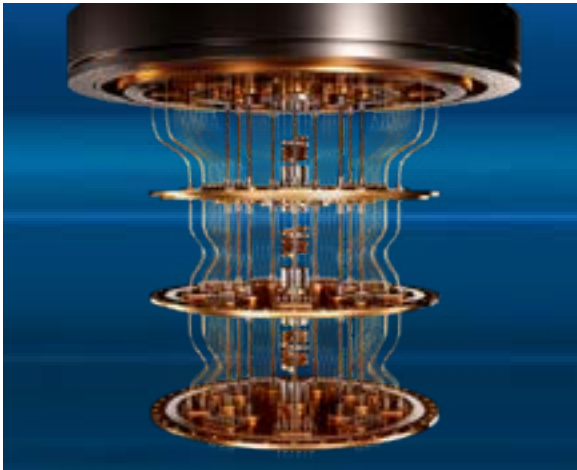




Quantum Resistant Today. Business Continuity and Investment Protection Tomorrow.

Hardware embedded Enterprise and business-class Pro security features*

Plan your quantum resistant device and fleet rollout today.



Hardware-enforced quantum resistance

HP Enterprise and Pro-class printers feature quantum-resistant digital signatures embedded at the ASIC hardware root of trust—below the firmware layer. HP's hybrid, NIST-standard protection delivers foundational defense against today's "Harvest Now, Decrypt Later" attacks and future quantum threats poised to break today's asymmetric encryption resident across IT infrastructure.

World's first quantum resistant printers¹

HP printers are the industry's first printers to protect against future quantum computer attacks at the foundational hardware level below the printer operating system. The BIOS is a set of boot instructions used to load critical hardware components and initiate firmware. HP Secure Boot (Pro) and Sure Start (Enterprise) technologies with Quantum Resistance work behind the scenes validating BIOS integrity when powering up with embedded hardware-enforced quantum resistant digital signatures. Quantum resistance protects the printers from hackers attempting to break today's standard asymmetric encryption (RSA, Elliptic Curve Cryptography).

Quantum compute is becoming very real, very quickly.

Fact #1:

When Classical Computing becomes Obsolete

Over 1,000 companies are racing to build a quantum computer that achieves 'quantum advantage'—outperforming the fastest classical systems so dramatically that traditional approaches become obsolete.

October 22, 2025: Google's Quantum Echoes algorithm and Willow chip represent a leap forward in quantum computing, achieving practical, verifiable quantum advantage.²

November 2025: IBM projects quantum advantage attainment by the end of 2026.³

Fact #2:

Tomorrow's Quantum Threats Break Today's Trust

Quantum attackers will soon dismantle RSA and Elliptic Curve encryption, enabling them to forge digital signatures and undermine the very foundation of secure data and communications.

Fact #3:

Make your printers a fortress, not a foothold.

Tomorrow's quantum threats can turn printers into gateways for catastrophic breaches. By breaking encryption in microseconds, attackers inject rogue firmware, seize control, and spread ransomware across your network—making proactive quantum-safe security essential today.

Fact #4:

Quantum Hasn't Cracked the Code—Yet.

December 2025: No quantum computer has yet demonstrated the ability to break contemporary asymmetric cryptography.⁴

Fact #5:

They're Harvesting Your Data Today to Break It Tomorrow.

Since 2022, nation-state actors have increasingly hijacked internet traffic to collect encrypted data, storing it for future decryption when quantum computers become available—a tactic known as 'Harvest Now, Decrypt Later' (HNDL).⁵

Fact #6:

Secure the printer. Safeguard the business.

Quantum-powered attackers could shatter asymmetric encryption at the BIOS layer in microseconds, inject rogue firmware, and seize full control of printers. From there, they can escalate privileges, move laterally across the network, and launch ransomware attacks that cripple operations and compromise sensitive data.

Fact #7:

Quantum-Ready. Hardware-Hardened. BIOS Secured.

HP's hybrid ASIC-embedded cryptography combines today's RSA NIST³ standard with our NIST-standard LMS quantum-resistant algorithm to protect the BIOS validation process and secure digital signatures in any environment.



HP Enterprise Color LaserJet
7000-8000 Series

Learn more: hp.com/go/PrintersThatProtect

Sign up for updates
hp.com/go/getupdated

Share with colleagues



HP stops what others can't see.™

HP Wolf Security. Built in. Always on. Future-ready.

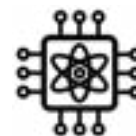
Future-ready fleet security for the Enterprise

Embedded enterprise-level print security features

Powering your peace of mind.™

Built in. Always on. Continuously monitoring for threats in the background, no configuration required.

The self-healing embedded security features address six primary steps in the bootup and runtime (in use and sleep modes) cycle of an HP Enterprise device in your environment.



Four, Five & Six. Continuous monitoring.

HP Memory Shield™ Hardware-enforced Runtime Intrusion Detection

Monitors memory activity to continually detect and stop attacks.

HP Memory Shield™ Control Flow Integrity (CFI)

Monitoring the execution flow of firmware code in real time CFI ensures that the program follows its expected control paths. If an unexpected or unauthorized call occurs—something not part of the device's "fingerprinted" normal behavior—it flags this as anomalous.

Blocking malicious code injections without relying on signatures

Unlike traditional antivirus, CFI does not depend on known malware patterns. Instead, it enforces a deterministic model of valid execution paths, making it effective against both known and unknown threats.

Triggering automatic self-healing

If an attack is detected, the printer immediately halts execution and reboots to a safe state. This process requires no IT intervention, minimizing downtime and risk.

Automatic Recovery Reboot

HP A3 and A4 Enterprise
MFPs and Printers



HP Enterprise Color LaserJet 8000 Series

One. Check operating code.

HP Sure Start™ with Quantum Resistance

Checks BIOS code and, if compromised, restarts from a safe "golden copy" of HP validated BIOS.

Two. Check firmware.

Allowlisting

Checks firmware during startup to determine if it is authentic code—digitally signed by HP.

Three. Check printer settings.

HP Security Manager™⁶

After reboot, checks and fixes any affected device security settings. If a new device connected to network, your security policy is automatically applied with "Instant-on."

Always-on protection

Prevents attackers from disabling the feature during a multi-stage exploit.

Zero-day protection

By monitoring control flow rather than relying on signatures, CFI can stop attacks that exploit previously unknown vulnerabilities.

AI-embedded HP Connection Inspector™

Network behavior anomaly detection and remediation inspects outgoing network connections to stop suspicious requests and thwart malware.

Learn more: hp.com/go/PrintersThatProtect

* HP LaserJet Enterprise 8000 Series and Managed E700/E800 Series and HP Color LaserJet Enterprise 5000/6000 and X500/X600 Series printers and MFPs manufactured as of November 1, 2025 are equipped with HP's proprietary quantum resistant-capable hardware ASIC and formatter including both NIST standard RSA and standard LMS post-quantum cryptographic digital signatures for initial BIOS firmware integrity. To enable quantum resistance, HP FutureSmart Firmware version 5.9.2.3 must be used to activate quantum resistant feature in the device. HP new Enterprise and Pro product introductions will be quantum resistant active from manufacturing.

¹ Based on HP's internal analysis of enterprise printers with preinstalled encryption, authentication, malware protection, post-quantum digital signature, and initial BIOS firmware integrity protection with automatic self-healing recovery finding that no other in-class Printers implement a quantum-resistant cryptographic scheme to protect the integrity of the initial BIOS and firmware as of March 2025.

² [Google's Quantum Echoes algorithm breakthrough - The Keyword](#)

³ [IBM November Quantum announcement](#)

⁴ Shor's algorithm remains impractical because current quantum computers lack the millions of error-corrected qubits and stability needed to break RSA-sized keys (RAND Corporation; MITRE).

⁵ Nation-state actors have increasingly hijacked internet traffic to collect encrypted data for future quantum decryption—a tactic known as "Harvest Now, Decrypt Later" (HNDL)—since at least 2022. (Tech Monitor, QuantumXC, Keyfactor).

⁶ HP Security Manager is server-based software and must be purchased separately. For details, see [Workforce Security Solutions](#). [HP Security Manager brochure](#).



HP Enterprise - Quantum Resistant (QR) Enablement Process

Table of contents

Overview	2
System requirements	2
Limitations	2
Enable the Quantum Resistant (QR) feature	3
Formatter Part Numbers (A3 PCA Number)	4
Formatter Part Numbers (A4 Revision Number)	4
Supported Printers	4
More Information	6

Overview

Quantum computing will break today's NIST (National Institute of Standards and Technology) standard asymmetric encryption-based cryptography (e.g., RSA, Elliptic Curve) in minutes, undermining digital signatures and firmware integrity. This creates a "harvest-now, decrypt-later" risk where attackers store encrypted data today and decrypt it once quantum machines mature.

The U.S. Federal Government has committed that starting in **2027**, all devices for National Security Systems must use quantum-resistant digital code signing for firmware and software. This aligns with NSA's CNSA 2.0 guidance and NIST's finalized PQC standards (ML-DSA : NIST FIPS PUB 204 (Section 5.1) ML-KEM : NIST FIPS PUB 203 (Section 7.1)).

HP introduced the **world's first quantum-resistant printers** in our HP LaserJet Enterprise 8000 Series and Managed E700/E800 Series in addition to our HP Color LaserJet Enterprise 5000/6000 and X500/X600 Series, featuring both hardware and firmware layers that enable quantum resistance at the device level.

Quantum-resistant printers complement **HP's Zero Trust Architecture**, enabling secure device identity and firmware integrity checks across fleets. This ensures resilience against lateral movement attacks even in hybrid environments.

System requirements

- **Firmware:** HP FutureSmart 5.9.2.3 or newer.
- **Hardware:** Quantum Resistant-capable A3 formatter (PCA code ending in 13-18) and A4 formatter with an updated revision number listed below.
NOTE: If a supported formatter is not detected, the quantum resistant option will not be visible via the configuration page or security menu within the EWS.
- **Browser Access:** Ensure you can access the printer's Embedded Web Server (EWS) via a supported web browser.
- **Admin Rights:** You must have administrator credentials for the device in order to enable the quantum-resistant feature.

Limitations

After enabling quantum resistance, downgrading to any **non-Quantum Resistant (QR) firmware version is not allowed**. Only downgrades between different quantum-resistant firmware versions are allowed. This is a deliberate security measure to prevent downgrade attacks and maintain cryptographic integrity.

NOTE: This feature requires manual enablement for the products listed below. Future products will have this feature enabled by default, active in all Enterprise and select business-class Pro devices from HP factories.

Enable the Quantum Resistant (QR) feature

To enable quantum resistant (QR) via the supported device, follow these steps.

1. Open a web browser and enter the printer's IP address.
2. Log in using administrator credentials.
3. Select the **Security** menu.
4. Select **General Security** from the left pane.
 - a. Find the "Quantum Resistant Secure Boot Activation" section.

Quantum Resistant Secure Boot

The Quantum Resistant Secure Boot is currently disabled.

Enable

5. Click the **Enable** button.

NOTE: A warning will display stating this action cannot be reversed or disabled.



Activate Quantum Resistant Secure Boot

This operation will activate a feature designed to protect the firmware against potential quantum computer attacks. Click "Activate" to continue. Activating this feature will permanently enable Quantum Resistant Secure Boot.

Once activated, it cannot be reversed or disabled. Only firmware bundles that support this feature can be installed.

6. Click **"Activate"** to confirm.



The product is shutting down to complete the operation.

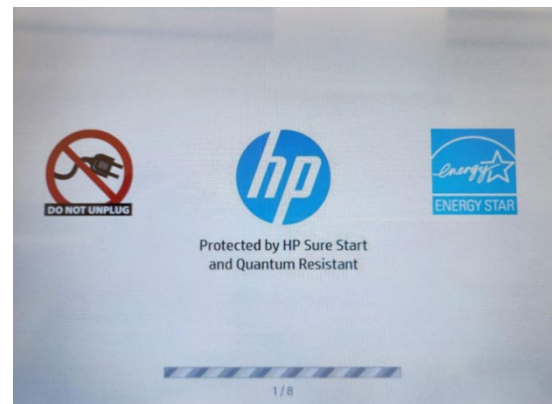
Please wait a few minutes, then refresh this page to see if the product has restarted. This web server will not be available until the product restarts.

7. Verify the status on the Configuration page in the Embedded Web Server (EWS), Security Menu or via the printer's control panel.

Security

Hard Disk Encryption Status:

Internal Disk:	Encrypted
Job Data Encryption Status:	Encrypted
Job Data Persistence:	Persistent (not volatile)
File Erase Mode:	Non-Secure Fast Erase (No overwrite)
Control Panel Password:	Disabled
Support Key:	V6GD-RSFG-TW5L
Host USB plug and play:	Enabled
Device USB:	Enabled
HP SureStart:	Present (Quantum Resistant: Configured)
Whitelisting:	Development
Runtime Intrusion Detection	Present



Quantum Resistant Secure Boot

Quantum Resistant Secure Boot has been enabled on this product and cannot be disabled. Only firmware bundles that support this feature can be installed. For information about firmware versions, visit the Software and Drivers website at <https://support.hp.com/>

Formatter Part Numbers (A3 PCA Number)

Product Model	Unsupported Formatter	Supported QR Formatter
E/D826xx, 8501 & 8601	3SJ33-60001	3SJ33-60013
E/D877xx & 8801	3SJ33-60002	3SJ33-60014
E/D731xx	3SJ00-60001	3SJ00-60015
E/D786xx	3SJ00-60002	3SJ00-60016
E730xx	3SJ00-60003	3SJ00-60017
E785xx	3SJ00-60004	3SJ00-60018

Formatter Part Numbers (A4 Revision Number)

Product Model	Unsupported Formatter	Supported QR Formatter
5700, X/D 55745xx	D6423.02 & E6430.00	F6510.00
5800, X/D 579xx, X580xx	C6315.01	D6507.00
6700 & X654xx	C6334.00	D6507.00
6800 & X/D 677xx	C6315.01	D6507.00

Supported Printers

A3 Products Model Numbers and Product Numbers

- **HP LaserJet Managed MFP E730xx**
 - 5QJ87A, 3SJ03A, 3SJ04A
- **HP Color LaserJet Managed MFP E785xx**
 - 5QJ83A, 5QJ81A, 5QK15A
- **HP Color LaserJet Managed MFP E786xx**
 - 5QJ90A, 5QJ94A, 5QK18A, 3SJ11A, 3SJ12A, 3SJ13A, 3SJ32A, 3SJ33A, 3SJ34A, A91S5A, A91S4A
- **HP Color LaserJet Managed MFP E877xx**
 - 5QK03A, 5QK08A, 5QK20A, 3SJ19A, 3SJ20A, 3SJ21A, 3SJ22A, 3SJ35A, 3SJ36A, 3SJ37A, 3SJ38A, A91S6A, A91S7A

- **HP Color LaserJet Ent Flow MFP and MFP 8801x**
 - 9S183A, 9S184A, AQ1E2A, BD5G8A
- **HP LaserJet Managed MFP E826xx**
 - AG8Z1A, A91S3A, A91S2A, 5QK09A, 5QK13A, 5QK21A, 3SJ07A, 3SJ08A, 3SJ09A, 3SJ28A, 3SJ29A, 3SJ30A
- **HP Color LaserJet Ent Flow MFP and MFP 8501x & 8601x**
 - 9S187A, AJ7J3A, AQ1E4A, BD5H0A, 9S185A, 9S186A, AQ1E3A, BD5G9A
- **HP LaserJet Managed MFP E731xx**
 - 5QJ98A, A91S1A, A91S0A, 5QK02A, 5QK19A, 3SJ00A, 3SJ01A, 3SJ02A, 6BS57A, 6BS58A, 6BS59A

A4 Products Model Numbers and Product Numbers

- **HP Color LaserJet Enterprise 5700 & HP Color LaserJet Enterprise X55745xx**
 - 6QN28A, 6QP97A, A8ZQ5A, 9Z0H9A
- **HP Color LaserJet Enterprise MFP 6800 & HP Color LaserJet Enterprise MFP X677xx**
 - 6QN35A, 6QN36A, 6QN37A, 6QN38A, 76H10A, 76H11A, 6QQ01A, 6QQ02A, 6QQ03A, 76H08A, 76H09A, 49K86A, 49K88A, 49K87A, 49K90A, 49K91A, 49K92A, A8ZQ7A
- **HP Color LaserJet Enterprise MFP 5800 & HP Color LaserJet Enterprise MFP X579/580xx**
 - 6QN29A, 6QN30A, 58R10, 6QP98A, 6QP99A, 76H07A, A8ZQ6A, 7E357A, 7H5W6A, 7H5W7A
- **HP Color LaserJet Enterprise 6700 & HP Color LaserJet Enterprise X654xx**
 - 6QN33A, 58M42A, 6QQ00A, 49L02A, 49L04A

More Information

The activation process modifies the OTP (One-Time Programmable) memory and hardware fuses, making rollback technically infeasible.

Labels outside of product packaging will be marked with a “PQC” (Post Quantum Cryptography) label as shown below:



© 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.

