We strengthen print resilience—so you can focus on your business

HP SECURE MANAGED PRINT SERVICES (MPS)

76%

of CIOs reported at least one ransomware attack in the past 24 months.[1]

40%

of CISOs admit their organizations are unprepared for a rapidly changing threat landscape.[2]

97%

of companies either have a zero-trust initiative in place or plan to implement one in the future.[3]

Secure printing anywhere with HP Secure MPS

Bug Bounty program

As the only printer manufacturer with a Bug Bounty program, you can count on HP to be on top of the latest threats.

Printer security deeply rooted in Zero Trust principles

Today, work happens anywhere. More people across more places need secure access to critical business systems, documents, and IT infrastructure. Distributed endpoints mean an expanded attack surface area that intruders are constantly scanning for the weakest link. To build cyber resilience, technology leaders are extending Zero Trust to every endpoint—including printers.

HP Wolf Enterprise Security fiercely defends your network and reputation with layered security defenses that start at the hardware level and extend across software and services, providing extensive print security from start up protection to ongoing detection.

It's the most comprehensive Zero Trust print framework[4] that delivers modern authentication and access control, policy-based configuration, strong data protection, and toolsets that enable active monitoring with the ability to act upon anomalous activity in real-time.

Partner with a leader in print security

HP is taking the lead to provide technologies and services that reduce the burden on IT, while improving security across your print environment. Only HP printers can automatically recover from attacks[5] and strengthen your ability to be resilient to evolving cyber-threats. HP Wolf Security experts take security a step further, by locating and then shoring up any potential vulnerabilities.

HP Secure MPS delivers end-to-end security assistance

Add HP Print Security Services to your HP MPS contract to get further layers of protection. Credentialed HP cybersecurity experts work with you to develop and deploy a custom plan to advance your print security to protect data and people—wherever they work.

DESIGN: ONE-TIME SERVICE

Print Security Advisory Service

Assess and recommend

- Assess your risks and vulnerabilities
- Build a comprehensive print security policy based on business needs and best practices
- Create a detailed roadmap for implementing a Zero Trust print framework

TRANSITION: ONE-TIME SERVICE

Print Security Implementation Service

Implement recommendations

- Let HP Technical Consultants take the burden off IT
- Implement recommendations based on Zero Trust principles, including device hardening, policy setting, and certificate deployment
- Device configuration sends syslogs to Security Information and Event Management (SIEM) tools

MANAGE: RECURRING SERVICES

Print Security Retainer Service

Reassess and align to best practices

- Reassess your print environment
- Highlight your progress and challenges in meeting compliance
- Provide ongoing advice and guidance

Print Security Governance and Compliance Service

Maintain and monitor

- Address unremediated devices
- Regularly analyze fleet security settings and identify suspicious patterns
- Produce monthly reports for proof of regulatory compliance
- Identify your top five risks

Secure every last endpoint—so trouble stays out

Critical gaps can occur at multiple points within your environment. Creating a complete printing and imaging security strategy requires coordinated protection of devices, data, and documents, plus comprehensive security monitoring and reporting solutions. With HP Secure MPS, you're more secure on every level from hardware to software, and services.

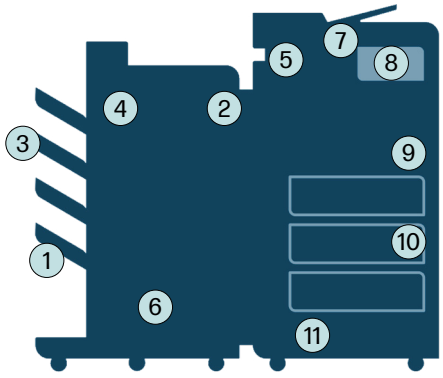
1. Mobile printing
Employees who print on the go may inadvertently expose data

2. Storage media
Sensitive information may be stored on internal drives or hard disks, which can be accessed if not protected

3. Output tray
The output tray is the most common place for sensitive documents to fall into the wrong hands

4. BIOS and firmware
Firmware that becomes compromised during startup, or while running, could open a device and the network to attack

5. Capture
MFPs can easily capture and route jobs to many destinations, potentially exposing sensitive data



6. Management
Without adequate monitoring, security blind spots across your fleet may remain undetected

7. Cloud-based access
Unsecured cloud connectivity may expose data to unauthorized users

8. Control panel
Users can exploit printing and imaging settings and functions from an unsecured control panel

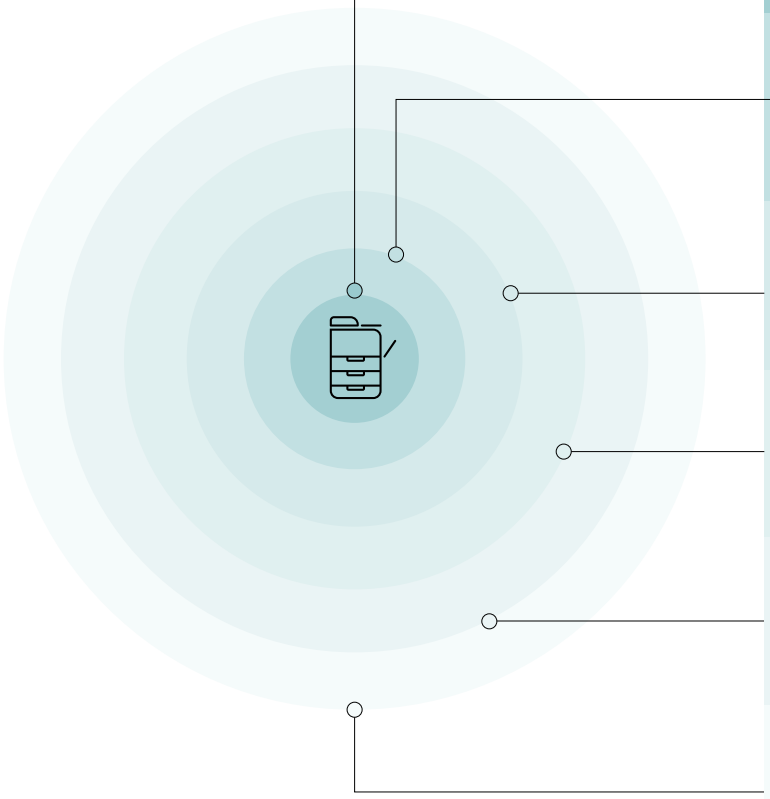
9. Ports and protocols
Unauthorized users can access the printer via unsecured USB or network ports or via older protocols (such as FTP or Telnet)

10. Input tray
Special media for printing checks, prescriptions, and other sensitive documents can be tampered with or stolen from an unsecured tray

11. Network
Printing and imaging jobs can be intercepted as they travel over the network

Comprehensive security comes from layering defenses

Your network firewall alone isn't enough to protect your endpoints. Only HP can guarantee your devices stay configured for security,[5] with the world's most secure printers, deeply rooted in Zero Trust principles. But print security isn't just about securing your devices. HP Secure MPS helps you build layers of defense from the hardware to the software, and services. HP Wolf Security experts can help you deploy a Zero Trust print strategy to secure data and documents, monitor for threats, and maintain your print security over time.



SECURE PRINTERS AND MFPS

- Zero Trust print framework
- Built-in malware protection
- Encrypted hard drives

DEVICE AND DATA HARDENING

- Admin passwords
- Firmware updates
- Configuration of interfaces and credentials
- Data-in-transit encryption
- Hard disk erase

MONITOR FOR THREATS

- Active fleet assessment and monitoring
- Security Information and Event Management (SIEM) integration

ACCESS CONTROLS

- Modern authentication and access controls
- Pull printing
- Role-based authorization

CUSTOM REQUIREMENTS

- Process and workflow changes
- Job tracking and accounting
- Anti-fraud, anti-counterfeit solutions
- Physical locks

NETWORK SECURITY

- Detection of suspicious network connections
- Automatic self-healing from attacks

Get started

Let us help you advance your security and reduce the burden on IT. With HP Secure MPS, you can be confident that you're getting the industry's strongest print security protections,[5] leveraging Zero Trust principles to strengthen cyber resilience. For more information, contact your HP representative today.

[1]Zero Trust Impact Report, Enterprise Strategy Group 2022.
[2]Cybersecurity Solutions for a Riskier World, ThoughtLab 2022.
[3]The State of Zero Trust Security 2022, Okta, 2022.
[4,5]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 published features as of February 2023 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.
[6]Includes data, of embedded device security features and availability of those features across HP Enterprise-class1 printers and MFPs, and competitor devices. This data is provided to support the relative claim of "most secure" printers. For more information, visit hp.com/go/MPSsecurityclaims or hp.com/go/securemps

Sign up for updates
hp.com/go/getupdated

Share with colleagues

Learn more
hp.com/go/SecureMPS