

HP DesignJet and PageWide XL Security Brochure



Protect your printers with the latest security standards



Firewalls alone can't withstand attacks from hackers. You need outstanding protection from HP to help protect your devices, data, documents, and network.

Table of contents

Printer security threats	03
Defend your devices, data, documents, and network	04
Protect your device	05-06
Protect your data	07
Protect your documents	08
Protect your network	09
How does self-healing work?	10
HP Wolf Security	11-12
Printers that protect, detect, and recover	13
HP DesignJet and PageWide XL portfolio	14
Competitive comparison	15
Legal footnotes and disclaimers	16

Printer security threats



Recognize hidden risks

Although many IT departments rigorously apply security measures to individual computers, printing and imaging devices are often overlooked and left exposed. When there are unsecured devices present, the entire network can be exposed to a cybersecurity attack.



Understand potential costs

If private information is jeopardized due to unsecured printing and imaging, the ramifications could include identity theft, stolen business information, a tarnished brand image and reputation, litigation, and loss of business productivity and efficiency. Plus, regulatory and legal noncompliance can result in heavy fines.



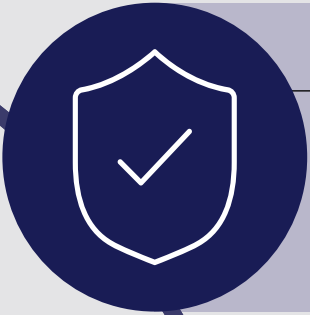
HP can help

Defend your network with security features embedded into our large format printers. HP can help you automate device, data, document, and network protection with a broad portfolio of solutions.

Defend your devices, data, documents, and network

Critical gaps can occur at multiple points within your imaging and printing environment. Once you understand these vulnerabilities, you can reduce the risks more easily.

Imaging and printing vulnerability points




Threats to your device

Control panel
Users can exploit device settings and functions.

Default password
Printers can come from the factory with simple default passwords that can be easily compromised.

BIOS and firmware
Compromised firmware can open a device and network to an attack.




Threats to your data

Data at rest
Printers store sensitive data that can be at risk.

Capture
Unsecured MFPs can be used to send scans anywhere.

Data in transit
Jobs can be intercepted as they travel to/from a device.



Threats to your documents

Output tray
Abandoned documents can fall into the wrong hands.

Ports and protocols
Unsecured ports (USB or network) or protocols (FTP or Telnet) put devices at risk.

Management
Undetected security gaps put data at risk.

Protect your device



HP Secure Boot

The BIOS is a set of instructions used to load critical hardware components and initiate firmware during startup. Thanks to HP Secure Boot, the integrity of the code is validated at every boot cycle—helping safeguard your device from attacks.

Allowlisting

Allowlisting automatically checks the firmware during startup to determine if it is authentic and digitally signed by HP. If an anomaly is detected, the device shuts down and notifies IT.

HP Connection Inspector

The HP Connection Inspector inspects outbound network connections typically abused by malware, determines what is normal, and stops suspicious activity. If the printer is compromised, it will automatically trigger a system restart.

HP Trusted Platform Module (TPM)

The HP Trusted Platform Module (TPM) strengthens the protection of encrypted credentials and data stored on your printer or MFP.

Protect your device

Unique admin password

All printers have a unique admin password by default, so your printer is always password-protected even without setup.

LDAP/Kerberos user authentication

These protocols allow you to authenticate the printer user through the company directory to ensure that the user only accesses authorized options and information.

Role-based access control

Role-based access control allows the administrator to restrict user access to sensitive areas and printer settings by configuring different roles and assigning them to such users.

Security event logging

Provides full visibility to quickly detect malicious threats. The security log records each event as defined by the audit policies set on each object.

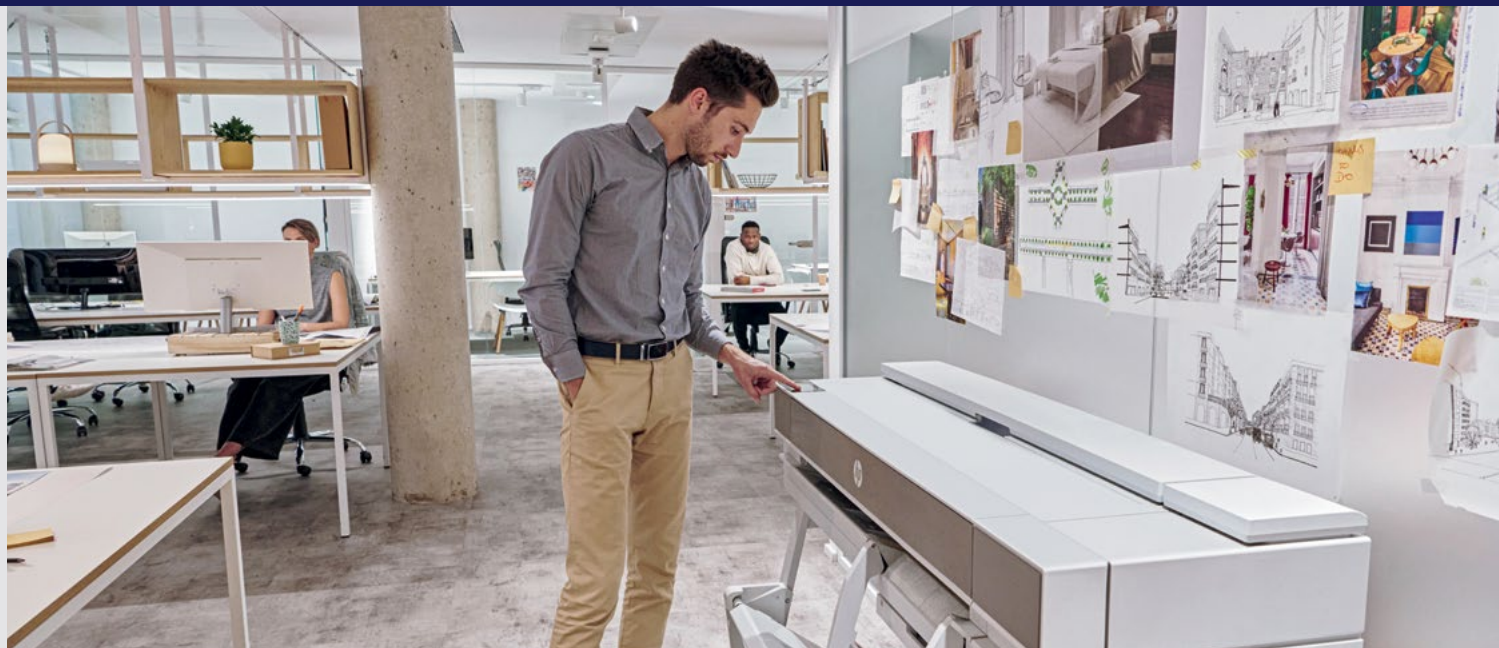
Run-time Intrusion Detection

Run-time Intrusion Detection continuously monitors the kernel memory and detects corruption or tampering attempts. Once detected, the device will self-heal by rebooting into a good state.

HP Sure Start

HP Sure Start is an advanced hardware-enforced solution providing comprehensive firmware and software settings that validates the digital signature of the BIOS.

Protect your data



At rest



Self-encrypted permanent memory

Protects sensitive business information stored on the permanent memory with built-in self encryption¹.



Secure file erase

Ensures that no data is left behind in the printer after files have been deleted from the permanent memory.



Secure disk erase

Erases all information from the printer's hard disk, making it impossible to recover sensitive data.

In transit



Encrypted communications

Standard encryption protocols 802.1x or IPSec use encrypted network standards to protect data traveling over the network when printing from drivers or submitters.

Protect your documents



Pull printing



Pull printing is a function that provides end-to-end tracking and reporting to protect sensitive information and media, and reduce unclaimed print jobs. It helps boost productivity and keep abandoned documents from falling into the wrong hands. HP large format printers are also compatible with other third-party pull printing solutions.



HP SmartCard Solution²

Enhance security and improve productivity with unified printer authentication across your organization.



Encrypted PIN printing

When users send confidential print jobs, they can assign a PIN to the document on the printer driver. The document will then be held in the printer until the user enters the PIN at the device. This way the user can be sure their confidential document won't be left unattended.

Protect your network

Security monitoring and management solutions can help you identify vulnerabilities and establish a unified, policy-based approach to protect data, reduce risk, and maintain compliance. Prevent protection gaps and help avoid costly fines.



Protect your devices and network



HP Security Manager³ helps you reduce cost and resources to establish a fleet-wide security policy, automate device settings remediation, and install and renew unique certificates. The Instant-on security feature included with HP Security Manager³ automatically configures new devices when added to the network or after a reboot.

HP Command Center (HPCC) is a cloud solution that allows IT admins to create a security policy for onboarded devices. Using HPCC, they can assess and, if necessary, remediate device security settings to comply with pre-established company security policies.

Compliance audit reporting of print fleet security



Use HP Security Manager³ on premise and HPCC in the cloud to create proof-of-compliance reports that demonstrate the application of security policies to printers and the securing of customer data.

Non-compliant devices can hurt your business



Unprotected or under-protected endpoints create more opportunity for cybercrime. To help counter the growing threat, government bodies across the globe are implementing strict security regulations that require organizations to better protect customer information. It's crucial to deploy devices and solutions—like HP DesignJet printers and HP Security Manager³—that can help you meet compliance requirements and protect your business information from security threats.

How does self-healing work?

HP Security Manager⁴ runs a four-step security check cycle to keep your device secure.



Check operating code (BIOS) HP Secure Boot

Prevents the execution of malicious code during boot-up by allowing only HP-signed, genuine code to be loaded.



Check firmware Allowlisting

Allows only authentic firmware digitally signed by HP to be loaded.



Check printer setting HP Security Manager⁴

After a reboot, inspects and fixes any affected device security settings.



Continuous monitoring HP Connection Inspector

Continuously monitors outbound network connections to prevent malware intrusion and automatically stop malicious activity.

Exceptional protection. Simple and secure.



HP WOLF SECURITY

HP Wolf Security^{4,5} now extends to HP Large Format DesignJet and PageWide XL Printers



To help print businesses like yours address future vulnerabilities and risks, HP Wolf Security delivers integrated endpoint protection and resiliency that starts at the hardware level and extends across software.

It's a breed of endpoint security, rooted in zero trust principles, that is continually evolving to help you stay ahead of modern threats.

Improve your security posture—with ease

While HP Wolf Security offers exceptional protection, it also enables systems to defend themselves and self-heal. Deploy and manage systems easily without compromising the breadth and depth of your security coverage.



Defend your growing business

Detect

Automatically detect issues or threats before you can spot them yourself.

Protect

Protect your business and maintain momentum with strong security that keeps you ahead of cyberthreats.

Recover

Automatically recover from attacks without burdening busy IT teams.

Three different levels of protection

HP DesignJet printers with HP Wolf Security have varying degrees of protection already built into them. By purchasing an HP Wolf secure printer, you are sure to have the appropriate level of security for your needs.



HP Wolf Essential Security

Lay a secure foundation with hardware-powered protection.

HP Wolf Pro Security

Safeguard your business with proactive protection against cyber threats.

HP Wolf Enterprise Security

Stay ahead of evolving security threats while supporting hybrid work.

Printers that protect, detect, and recover

HP large format printers

Designed to help reduce risk, improve compliance, and protect your network end-to-end, HP large format printers provide embedded features and add-on solutions that can help you defend against attacks.



HP PageWide XL & Pro Printer Series

For more information, please visit:

[HP PageWide XL & Pro Printer series](#)



HP DesignJet XL 3800 MFP Series

For more information, please visit:

[HP DesignJet XL 3800 MFP series](#)



HP DesignJet XL 3600 MFP Series

For more information, please visit:

[HP DesignJet XL 3600 MFP series](#)



HP DesignJet T2600 MFP Series

For more information, please visit:

[HP DesignJet T2600 MFP series](#)



HP DesignJet T1700 Printer Series

For more information, please visit:

[HP DesignJet T1700 Printer series](#)



HP DesignJet T1600 Printer Series

For more information, please visit:

[HP DesignJet T1600 Printer series](#)



HP DesignJet T850/T950 Printer Series

For more information, please visit:

[HP DesignJet T850/T950 Printer series](#)



HP DesignJet Smart T918/908/858 Printer Series

For more information, please visit:

[HP DesignJet T918/908/858 Printer series](#)



HP DesignJet Z9+ Pro 64-In Printer Series

For more information, please visit:

[HP DesignJet Z9+ Pro Printer series](#)



HP DesignJet Z6 Pro 64-In Printer Series

For more information, please visit:

[HP DesignJet Z6 Pro Printer series](#)



HP DesignJet Z9+ Postscript® Printer Series

For more information, please visit:

[HP DesignJet Z9+ PostScript® Printer series](#)



HP DesignJet Z6 Postscript® Printer Series

For more information, please visit:

[HP DesignJet Z6 PostScript® Printer series](#)

HP DesignJet and PageWide XL portfolio

	HP DesignJet T850/950 and Smart Tank T858 36-in Printer series	HP DesignJet T850/950 MFP and Smart Tank T908/T918 36-in MFP Printer series	HP DesignJet T1600/2600 Printer series	HP DesignJet T1700 Printer series	HP DesignJet Z6 & Z9+ Printer series	HP DesignJet Z6 Pro & Z9+ pro 64-IN Printers	HP DesignJet XL 3800 Printer series	HP DesignJet XL 3600 Printer series	HP PageWide XL Printer series	HP PageWide XL Pro Printer series	
Device	Secure Boot	☑	☑	☑	☑	☑	☑	☑	☑	☑	
	Connection Inspector					☑	☑		☑	☑	
	Allowlisting	☑	☑	☑	☑	☑	☑	☑	☑	☑	
	Unique admin password	☑	☑			☑	☑		☑	☑	
	TPM			☑		☑	☑	☑	☑	☑	
	Runtime intrusion detection						☑				
	Sure start (with self healing)						☑				
	Security event logging	☑	☑	☑		☑	☑	☑	☑	☑	
	SNMPv3 disabled by default	☑	☑	☑	☑	☑	☑	☑	☑	☑	
	Self-encrypted disks	N/A	N/A	☑	☑	☑	☑	☑ (a)	☑	☑	☑
Data	Disable network ports and protocols	☑	☑	☑	☑	☑	☑	☑	☑	☑	
	LDAP/Kerberos user authentication			☑		☑	☑	☑	☑	☑	
	Role-based access control			☑	☑	☑	☑	☑	☑	☑	
	Front panel access lock			☑	☑	☑		☑	☑	☑	
	Self Encrypted Non-Volatile Memory	N/A	☑	N/A	N/A	N/A	N/A	☑	N/A	N/A	
	Removable HDD	N/A	N/A	☑				☑	☑	☑	
	IPsec			☑	☑	☑	☑	☑	☑	☑	
	TLS/SSL	☑	☑	☑	☑	☑	☑	☑	☑	☑	
	Secure file erase			☑	☑	☑	☑	☑	☑	☑	
	Secure disk erase			☑	☑	☑	☑	☑	☑	☑	
Document	802.1x compatibility	☑	☑	☑	☑	☑	☑	☑	☑	☑	
	NTLMv2		☑	☑	☑	☑	☑	☑	☑	☑	
	Encrypted PIN Printing			☑	☑	☑	☑	☑	☑	☑	
	IPv4 & IPv6 Compatibility	☑	☑	☑	☑	☑	☑	☑	☑	☑	
	CA/JD Compatibility	☑	☑	☑	☑	☑	☑	☑	☑	☑	
	HP SmartCard Solution			☑			☑	☑	☑		
	PIN Printing			☑	☑	☑	☑	☑	☑	☑	
	Fleet security management	HP Web JetAdmin	☑	☑	☑	☑	☑	☑	☑	☑	☑
		HP Security Manager	☑	☑	☑	☑	☑	☑	☑	☑	☑
		HP Command Center	☑	☑				☑			
SIEM Integration		☑	☑	☑		☑	☑	☑	☑	☑	

(a) FIPS 140-2 for TAA compliant units

Competitive comparison

	Canon TM 355 Z36	Canon TX 3100/ Z36	Canon TX 4100	Canon CW 3600 / 3800	Canon PW 3000 Series	Ricoh Im CW 2200	Kip 700 C Series	Kip 900 Series	Epson T5400M	Epson SC T5700M	Epson SC T7700D
Secure Boot				☑	☑						
Connection Inspector											
Allowlisting				(a)	(a)		☑				
Unique admin password	☑	☑	☑				☑	☑	(b)	(b)	☑
TPM				☑	☑						☑
Runtime intrusion detection				(a)	(a)						
Sure start				(a)	(a)						
Security event logging					☑	☑					
SNMPv3 compatibility	☑	☑	☑	☑	☑	☑	☑		(c)	(c)	(c)
Self-encrypted disks (FIPS 140-2)	☑	☑	☑	☑	☑		☑				☑
Disable network ports and protocols	☑	☑	☑	☑	☑	☑			☑	☑	☑
LDAP/Kerberos user authentication				☑	☑	☑	☑				☑
Role-based access control				☑	☑	☑	☑				
Front panel access lock	☑	☑	☑	☑	☑				☑	☑	☑
Removable HDD				☑	☑		☑	☑			
IPsec	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑
TLS/SSL	☑	☑	☑	☑	☑	☑			☑	☑	☑
Secure file erase	☑	☑	☑	☑	☑	☑	☑	☑			☑
Secure disk erase	☑	☑	☑	☑	☑	☑	☑				☑
802.1x compatibility	☑	☑	☑	☑	☑	☑			☑	☑	☑
NTLMv2					☑	☑					
Encrypted PIN Printing						☑		☑			
IPv4 & IPv6 Compatibility	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑
CA/JD Compatibility	☑	☑	☑	☑	☑	☑			☑	☑	☑
SmartCard Solution				☑	☑	☑					
PIN Printing	☑	☑	☑				☑	☑			☑
Security policy enforcement tool		☑	☑	☑	☑						
Cloud Fleet management tool		☑	☑	☑	☑				☑	☑	☑
SIEM Integration				☑	☑						

(a) Optional McAfee Application control

(b) Printer's serial number is used as the password

(c) Disabled manually

Legal footnotes and disclaimers

1. FIPS 140-2 for TAA compliant units
2. Supports US Govt NIPRNet Solution and US Govt SIPRNet Solution.
3. HP Security Manager must be purchased separately. To learn more, please visit hp.com/go/securitymanager
4. HP Security is now HP Wolf Security. Security features vary by platform, please see product data sheet for details.
5. All HP DesignJet printers have varying levels of security, but only select printers can claim HP Wolf Security. These include the HP DesignJet XL 3800 MFP, HP DesignJet T850 Printer/T850 MFP, and HP Smart Tank T858 printer and T908/T918 MFP. HP Wolf Security will become a standard feature on future HP DesignJet products.

© Copyright 2021, 2024 HP Development Company, L.P. The information contained herein is subject to change without notice. The only warranties for HP products and services are outlined 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.

4AA8-3169EEP, July 2024

