Defend Your Network

With The World's Most Secure Large Format Printers[1]

Firewalls alone can't withstand attacks from sophisticated hackers. You need the world's most secure Large Format Printers[1] from HP to help protect your devices, data and documents.

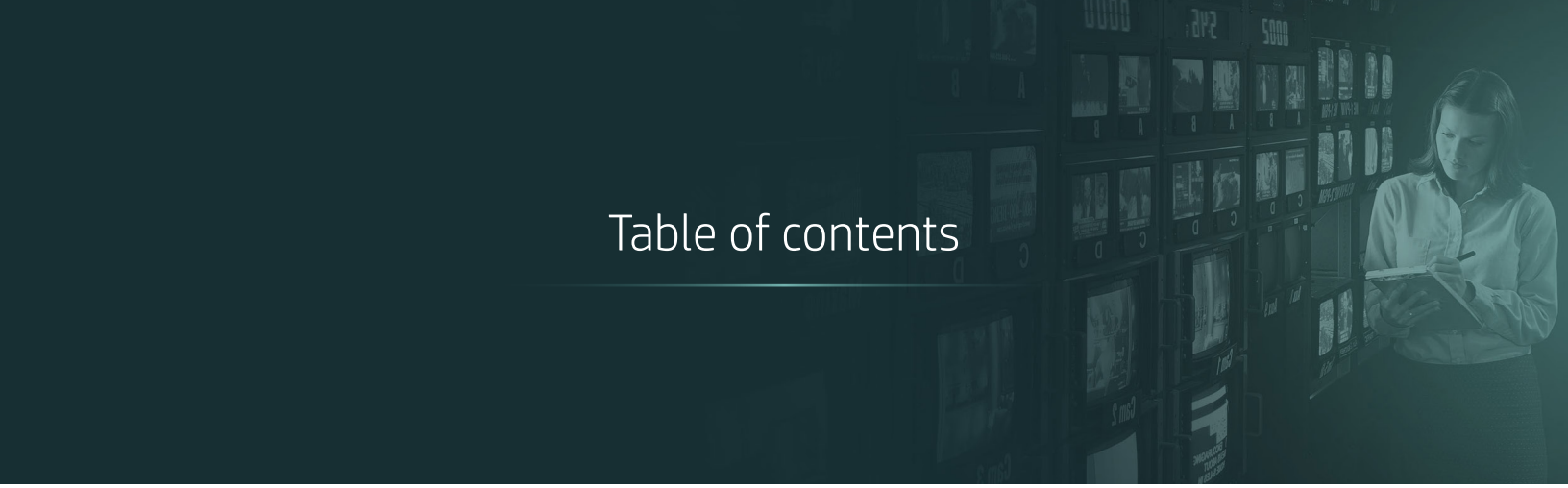


Table of contents

Only 22% of companies monitor printers for threats[2]

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 competitive information, a tarnished brand image and reputation, and litigation. Plus, regulatory and legal noncompliance can result in heavy fines.

HP can help

Defend your network with the world's most secure large-format printers.[1] HP can help you automate device, data, and document protection with a broad portfolio of solutions.

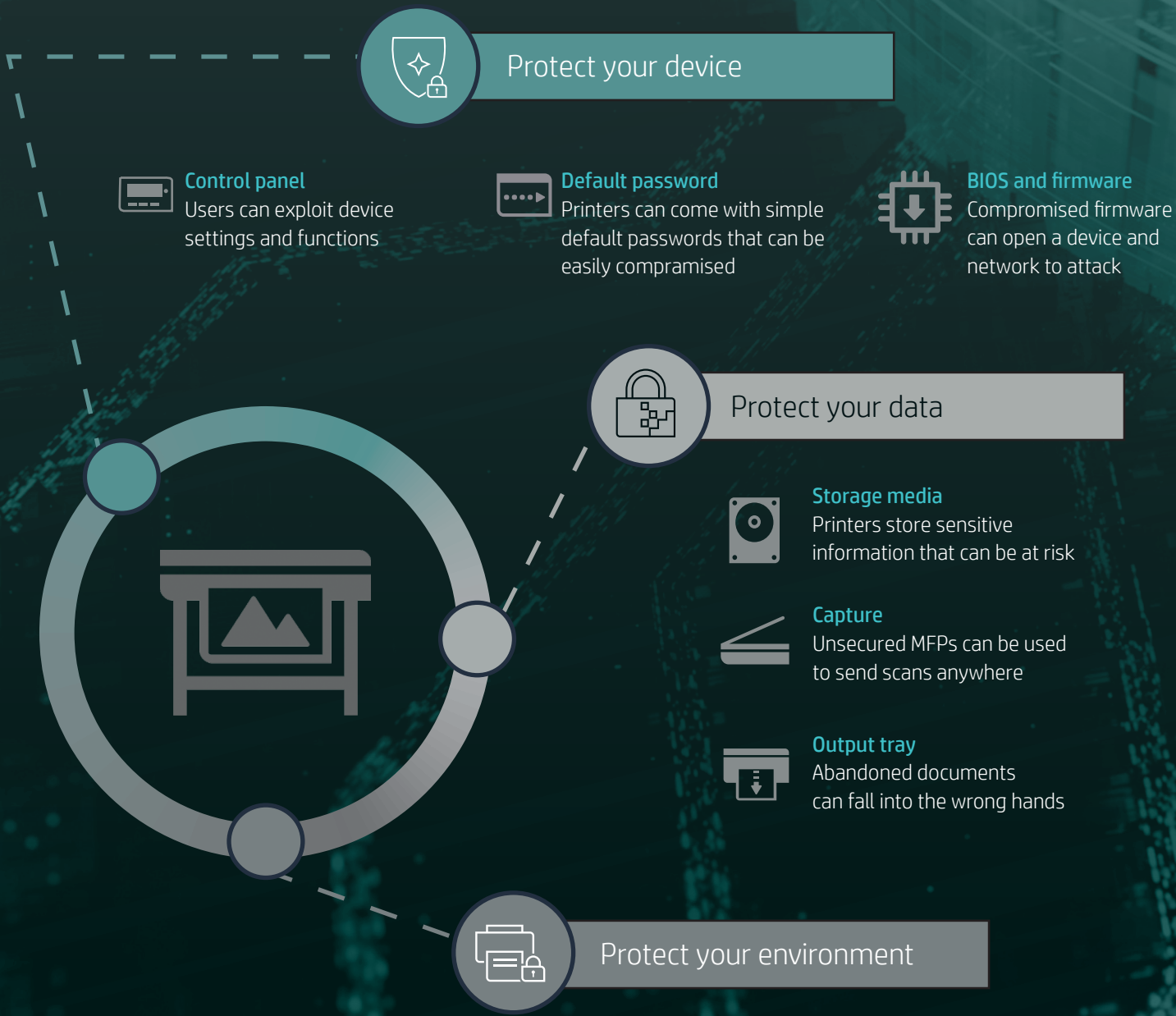
"TESTAMENT TO ITS LONG-TERM INVESTMENT IN PRINT SECURITY, HP HAS THE BROADEST AND DEEPEST PORTFOLIO OF SECURITY SOLUTIONS AND SERVICES IN THE MARKET."

– QUOCIRCA, JAN 2017[3]

Defend your devices, data, and documents

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

IMAGING AND PRINTING VULNERABILITY POINTS



Protect your device

Control panel
Users can exploit device settings and functions

Default password
Printers can come with simple default passwords that can be easily compramised

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

Protect your data

Storage media
Printers store sensitive information that can be at risk

Capture
Unsecured MFPs can be used to send scans anywhere

Output tray
Abandoned documents can fall into the wrong hands

Protect your environment

Management
Undetected security gaps put data at risk

Network
Jobs can be intercepted as they travel to/from a device

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

CONTENTS

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 to safeguard your device from attack.

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

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 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 settings of the printer 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.

CONTENTS

80%

of organizations reported at least one type of security threat/breach, either external or internal, within the last 18 months[2]

Protect your data

At rest

Self-encrypted hard drive

Protects sensitive business information stored on the hard drive with built-in encryption.

Secure File Erase

Ensures that no data is left behind in the printer after your files are deleted from the hard disk.

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.

CONTENTS

Protect your documents

Pull printing

Celiveo Enterprise is a fully integrated secure printing and tracking solution.[4] This access control-based function has 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.

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. With encrypted PIN printing, document data is encrypted when the document is sent to the printer to protect document confidentiality through the 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.[2]

Protect your printing environment

Update devices with the latest firmware/OS

HP JetAdvantage Security Manager helps you reduce cost and resources to establish a fleet-wide security policy, automate device settings remediation, and install and renew unique certificates.[5] The Instant-on Security feature included with HP JetAdvantage Security Manager automatically configures new devices when added to the network or after a reboot.

Compliance audit reporting of print fleet security

Use HP JetAdvantage Security Manager to create proof-of-compliance reports that demonstrate the application of security policies to printers and the securing of customer data.

Compliance infringement 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 JetAdvantage Security Manager—that can help you meet compliance requirements and protect your business information from security threats.

How does self healing work?

HP Security Manager runs a four-steps security check cycle to keep your device secure:

1. 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.**

2. Check firmware

Whitelisting

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

3. Check printer settings

HP JetAdvantage Security Manager

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

4. Continuous monitoring

HP Connection Inspector

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

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 your printers and network.

HP DesignJet XL 3600 MFP series

The most immediate, robust,[6] MFP for demanding environments.

For more information, please visit:

HP DesignJet XL 3600 MFP series

HP DesignJet T1600 Printer series

Meet deadlines with the fastest print speed, and with a radically simple printing experience.

For more information, please visit:

HP DesignJet T1600 Printer series

HP PageWide XL Printer series

The fastest large-format printing. High quality printing quality made simple and secure.

For more information, please visit:

HP PageWide XL Printer Series

HP DesignJet T2600 MFP series

A seamless experience for unprecedented collaboration, with the best network protection.[1]

For more information, please visit:

HP DesignJet T2600 MFP series

HP DesignJet T1700 Printer series

Empowering HP DesignJet printer for CAD/GIS workgroups.

For more information, please visit:

HP DesignJet T1700 Printer series

HP DesignJet Z6 PostScript® Printer series

High-definition prints, fast.
More quality with fewer inks.

For more information, please visit:

HP DesignJet Z6 PostScript® Printer Series

HP DesignJet Z9+ PostScript® Printer series

Professional photo prints fast, simple.
More quality with fewer inks.

For more information, please visit:

HP DesignJet Z9+ PostScript® Printer Series

CONTENTS

HP printer portfolio

	HP DesignJet T730 Printer	HP DesignJet T830 MFP series	HP DesignJet T1600 Printer series	HP DesignJet T1700 Printer Series
DEVICE				
HP Secure Boot	●	●	●	●
UEFI Secure Boot	●	●	●	●
Connection inspector	●	●	●	●
Whitelisting			●	
Unique admin password	●	●	●	●
TPM			●	
LDAP/Kerberos User Authentication	●	●	●	●
Role Based Access Control			●	●
Front Panel Access Lock			●	●
Security event logging	●	●	●	●
SNMP v3 compatibility	●	●	●	●
DATA				
Self-encrypted HDD	n/a	n/a	●	●
No HDD	●	●		
IPSec compatibility			●	●
TLS/SSL	●	●	●	●
Secure File Erase			●	●
Secure Disk Erase			●	●
802.1x compatibility	●	●	●	●
NTLMv2	n/a	●	●	
Encrypted PIN printing			●	
IPv4 & IPv6 compatibility	●	●	●	●
CA/JD certificates	●	●	●	●
Disable interfaces	●	●	●	●
DOCUMENT				
PIN printing			●	●
Integrated Celiveo Enterprise Solution			●	●
Integrated API Netgard® MFD			●	●
FLEET SECURITY MANAGEMENT				
HP Web JetAdmin [7]	●	●	●	●
HP JetAdvantage Security Manager	●	●	●	●
SIEM integration			●	

CONTENTS


HP DesignJet T2600 Printer Series
HP DesignJet XL 3600 Printer Series
HP DesignJet Z6 & Z9+ Printer Series
HP DesignJet Z6810 Printer
HP PageWide XL Printers
SSL Only

Competitive Comparison

		HP HP DesignJet T1700 Printer / Z9+ and Z6 PostScript® Printer series	HP HP DesignJet XL 3600 MFP / HP DesignJet T2600 MFP and T1600 Printer Series	HP HP PageWide XL Printers	CANON CW 3600/3800 /9000	CANON imagePROGRAF TX-series TM-series
DEVICE	Secure Boot	●	●	●	●	
	HP Connection Inspector			●		
	Whitelisting	●	●	●	●	
	Unique admin password			●		
	TPM[a]		●	●	●	
	LDAP/Kerberos User Authentication[a]		●	●	●	
	Role Based Access Control	●	●	●	●	*
	Front Panel Access Lock	●	●	●	●	●
	Security event logging		●	●	●	
DATA	Disable network ports and protocols[a]	●	●	●	●	●
	SNMP v3	●	●	●	● [g]	●
	Self-encrypted HDD[a]	●	●	●	●	● [c]
	IPSec	●	●	●	●	●
	TLS/SSL	●	●	● [h]	●	●
	Secure File Erase	●	●	●	● [i]	●
	Secure Disk Erase	●	●	●	●	●
	802.1x compatibility[a]	●	●	●	●	●
	NTLM v2[a]	n/a	●	●		●
	Encrypted PIN printing		●	●		
DOCUMENT	Integrated pull-printing solution[f]	●	●	●	● [j]	
	PIN printing[a]	●	●	●		
FLEET SECURITY MANAGEMENT	Security policy based fleet management[a]	●	●	●		
	SIEM integration		●	●	●	

CONTENTS

EPSON SURE COLOR T-series	OCE PW 345 CW 500	KIP 660 860 970	KIP 7172	RICOH CW2201 SP
*				
				(b)
	(d)			
	(d)			
n/a(e)				

(a) Security features of competitive printers that does reflect in this table is because they are not specified in any of their datasheet/brochure. Not specified in datasheet/brochure IEEE802.1x enable/disable
(b) IEEE802.1x enable/disable
(c) Not available on the TM
(d) e-shredding / e-shredding [DoD 5220.22-M].
(e) NTLMv1
(f) Celiveo + API Netgard® MFD
(g) Only 3600 and 3800 have v3, while CW 9000 has v2
(h) Version 1.3, while all others have Version 1.2
(i) Secure File Erase and Secure Disk Erase are available only in 3600 and 3800; not available in 9000
(j) HP has integration with Celiveo and API Netgard. Canon, Richoh and KIP have it only with Netgard.
(*) Limited to 2 users (g) Only 3600 and 3800 have v3, while CW 9000 has v2

CONTENTS

Defend your network with the world's most secure large format printers[1]

CONTENTS

Sign up for updates | DesignJet Security

Share with your colleagues

1. Applicable to the HP DesignJet T1700 Printer series, HP DesignJet Z9+ PostScript® Printer series, and HP DesignJet Z6 PostScript® Printer series, HP DesignJet XL 3600 Multifunction Printer series, HP DesignJet T2600 Multifunction Printer series, and HP DesignJet T1600 Printer series. Advanced embedded security features are based on HP review of 2019 published embedded security features of competitive printers, as of February 2019.
2. Spiceworks survey of 501 IT decision-makers in North America, EMEA, and APAC, on behalf of HP, June 2018.
3. Quocirca, "Print security: An imperative in the IoT era," quocirca.com/content/print-security-imperative-iot-era, January 2017.
4. The HP DesignJet T1700 Printer series, Z9+ and Z6 PostScript® Printer series, and, HP Pagewide XL printers include the fully integrated Celiveo Enterprise solution.
5. HP JetAdvantage Security Manager must be purchased separately. To learn more, please visit hp.com/go/securitymanager.
6. Based on comparable printers using LED technology and capable of printing 4-6 D/A1 pages per minute and which represent more than 70% of the share of low-volume LED printers in the US and Europe according to IDC as of November, 2018. Fastest first page out and up to 10 times less energy consumption based on internal HP testing for specific use scenarios. Operational costs based on low-volume LED technology under $17,000 USD in the market as of November, 2018. Operational costs consist of supplies and service costs. For testing criteria, see hp.com/go/designjetxlclaims.
7. HP Web Jetadmin is available for download at no additional charge at hp.com/go/webjetadmin.

4AA7-4067ENW, December 2019