Sales Battle Card

HP DesignJet printers security

Security threats are evolving every day. Every device on a company's network is a vulnerability point, including network printers, and therefore large-format printers.

64%
of IT managers state their printers are likely infected with malware[1]

73%
of CISOs expect a major security breach within a year[2]

26%
of all significant data breaches reported by IT managers involved their printers[3]

Target clients

Organizations of all sizes, all geographies, and all industries with needs for securing their shared imaging and printing environments.

Contact target

- CISO (Chief Information Security Officer) or IT Security Leader
- CIO
- Security/compliance managers
- IT management and decision makers

Ideal client characteristics

- Increasing security requirements due to threats and regulatory compliance
- Can't accept the risks of an opening to their network to breaches
- Are facing costly compliance fines due to regulations involving the handling of customer data
- Use highly confidential data as part of their day-to-day business operations

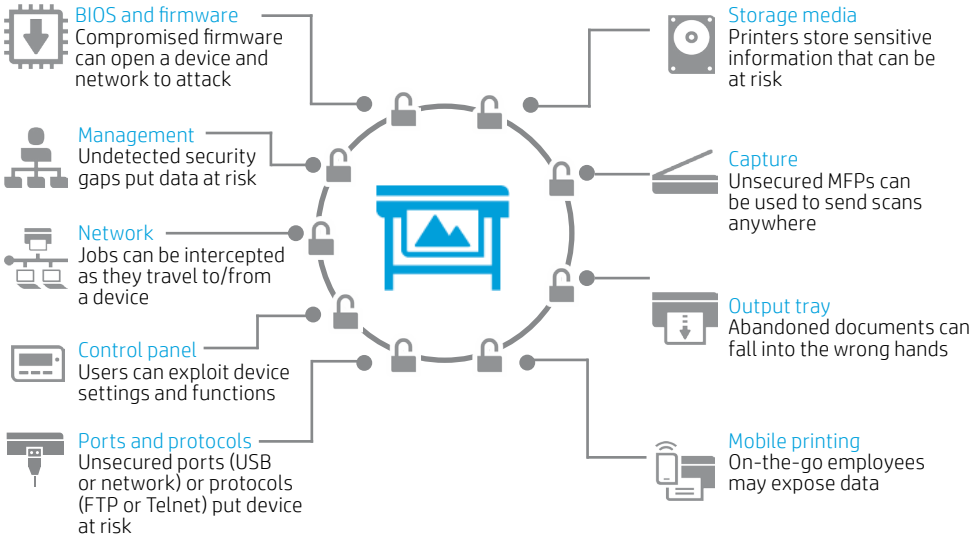
Market situation

Due to the growing sophistication and perseverance of cybercriminals, network firewalls are proving to be insufficient security measures. Organizations need to fortify their end points behind the firewall, including network printers.

Whether it's a malicious cyberattack, an accidental internal breach, or regulatory and legal non-compliance, the cost of resolving a security breach can be huge. Average annual cost is about $4 million[4] and can include fines, loss of business, damaged reputation, and class-action lawsuits.
Regulatory and compliance requirements are getting more complicated. Organizations need devices and solutions that help them stay compliant.

Client security challenges

Although many IT departments rigorously apply security measures to individual computers and the business network, printing and imaging devices are often overlooked and left exposed.



Client security needs

Your customers need easy ways to protect their devices, data, and documents. They also want streamlined print security management and compliance reporting to save IT time.

Device security

- Protect BIOS and firmware from attack and malware
- Firmware upgrade protection
- Secure device settings and passwords

Data security

- Data encryption in transit to and from the printer, and at rest when stored in the printer
- Support CA-signed digital certificates (PKI)
- Secure hard disk erase and disposal
- User authentication and access control
- Secure mobile printing solutions

Document security

- Secure pin printing solutions

Fleet security monitoring and compliance

- Get control of fleet security with multiple configuration and monitoring features
- Advanced reporting to help prove compliance

Client value proposition

- Minimize the risk of costly cyberattacks
- Protect sensitive data and documents
- Save time by automating fleet security management
- Keep your business in compliance with industry regulations—and get easy access to data for compliance reporting

Partner value proposition

- A growth opportunity, since clients are actively investing in print security
- Drives a value conversation so you can sell higher into the organization; security can shift the conversation from price to value-add

Qualifying questions

Ask your customer these questions:

- Do you have a security strategy for your imaging and printing devices?
- Are you handling sensitive information, such as employee identities or customer data?
- Do you encrypt print jobs?
- Are your printers protected from malware and viruses?
- How often do you apply printer firmware updates?
- Have you applied administrative passwords to your printers or can anyone walk up and change device settings?
- How much time does IT spend configuring your printers?

HP security offerings for HP DesignJet printers

The security features built into HP DesignJet printers can help companies protect their devices, data, and documents. Plus, they help your customers more easily manage fleet security and compliance.

Secure printers

- **HP signed firmware packages**—firmware packages are digitally signed by HP Code Signing group. Every new firmware installation is verified
- **UEFI Secure Boot**—Validates the integrity of the operating system during startup
- **Hard disk drive encryption**—HP uses 256-bit Advanced Encryption Standard (AES) hard disk data encryption and decryption
- **Secure file erase and disk erase**— Are procedures to ensure actual data in storage systems are removed avoiding its recovering.
- **Control panel access lock**—Locks the printer's control panel in order to prevent unauthorized users from accessing it and changing the printer's settings.

Secure software

Beyond the device, HP offers solutions to detect, protect, monitor and manage the fleet and secure data and documents over time.

- **HP JetAdvantage Security Manager**—The industry's only policy-based print security compliance tool automates fleet security management[6]
  - Supports print security policy creation and deployment to the fleet
  - Risk-based reporting helps IT quickly view fleet status and prove compliance
  - Automated application and updating of unique CA-signed device certificates
- **HP Web Jetadmin**—Count on an award-winning, industry-leading, print management solution that can improve productivity and help reduce operation costs. Easy-to-use HP Web Jetadmin offers a simple, web-based interface to install, configure, troubleshoot, and manage both HP and non-HP networked and PC-connected print devices.[7]

Secure services

- **HP custom recycling services**—Make sure data is eliminated from hard drives before responsibly recycling old products. More details at hp.com/go/businessrecycling.

HP DesignJet security vs. the competition

		HP DesignJet (1)	Canon (2)	Epson (3)	Ricoh (4)
DEVICE	Network management security features through SNMP v3	✓	✓	⊘	✓
	Secure File Erase	✓	⊘ (6)	⊘	✓
	Secure Disk Erase	✓	✓ (5)	✓	✓
DATA	802.1x compatibility	✓	⊘ (6)	✓	✓
	Hard disk drive encryption	✓	⊘	✓	✓
	Internet Protocol Security (IPsec)	✓	⊘ (6)	✓	✓
DOCUMENT	Personal identification number (PIN) printing	✓	⊘	⊘	✓

(1) Models compared: HP DesignJet T930, T1530, T2530 MFP, T3500MFP
(2) Models compared: Canon iPF785, iPF770, iPF850, iPF770L36, M40 Scanner
(3) Models compared: Epson SC-T5200/D, SC-T5200F MFP
(4) Models compared: Ricoh MP CW2201SP
(5) for models that have HD
(6) M40 Scanner: Yes

Win

It's vital for businesses to take print security seriously. HP offers industry-leading products and solutions that can help protect devices, data, and documents.

[1] Ponemon Institute, "Insecurity of Network-Connected Printers," October 2015.

[2] Help Net Security, "Why enterprise security priorities don't address the most serious threats," July 2015.

[3] 26.2% of survey respondents experienced a significant IT security breach that required remediation, and more than 26.1% of these incidents involved print. IDC, "IT and Print Security Survey 2015" IDC #US40612015, September, 2015.

[4] Ponemon Institute, "Cost of Data Breach Study Global Analysis" 2016

[5] Quocirca, Managed Print Services Landscapes for 2014 and 2015.

[6] Competitive claim based on HP internal research on competitor offerings (Device Security Comparison, January 2015) and Solutions Report on HP JetAdvantage Security Manager 2.1 from Buyers Laboratory LLC, February 2015. HP JetAdvantage Security Manager must be purchased separately. To learn more, please visit hp.com/go/securitymanager.

[7] HP Web Jetadmin is free and available for download at hp.com/go/wja

Share with colleagues

4AA6-9616EEP, May 2017