Are you concerned about printer security?

You should be.

Jason Kuhn | Apr 17, 2018

Data

163 ZB

by 2025*

Clients

95%

By 2020, IoT will be in 95% of electronics for new product designs*

Threats

7.9B

records exposed in 2017*

*IDC forecasts that by 2025 the global datasphere will grow to 163 zettabytes (IDC, Data Age 2025, 2017),

*By 2020, IoT technology will be in 95% of electronics for new product designs. Gartner, Smarter with Gartner, Gartner Top Strategic Predictions for 2018 and Beyond, October 3, 2017.

*2017 saw more than 5,200 breaches that exposed nearly 7.9 billion records. 2017 Year End Data Breach QuickView Report by Risk Based Security / Cyber Risk Analytics, January 2018.

Risks and costs of unprotected printing environments

Cybercrime, internal breaches, compliance infringement, and more can hurt your business

94%

of financial firms say copier/printer security is important or very important*

43%

of companies ignore printers in their endpoint security practices*

61%

of organizations reported a print-related data breach in the past year*

$11.7M

average annualized cost of cybercrime*

Disclaimers:

94% of financial firms say copier/printer security is important or very important: InfoTrends, “Designing Hardware & Solutions,” Brendan Morse, October 2016.

61% of organisations reported at least a single print-related data breach in the past year: Quocirca, "Managed Print Services Landscape, 2016," quocirca.com/content/managed-print-services-landscape-2016, July 2016.

43% of companies ignore printers in their endpoint security practices: Spiceworks survey of 309 IT decision-makers in North America, EMEA, and APAC, on behalf of HP, November 2016.

$11.7M average annualized cost of cybercrime: Ponemon Study sponsored by HPE, “2017 Cost of Cyber Crime,” 2017. accenture.com/t20170926T072837Z__w__/us-en/_acnmedia/PDF-61/Accenture-2017-CostCyberCrimeStudy.pdf

The risk is real

It’s easy for hackers to break into unsecured printers

“I probe around for a multifunction printer and see that it is configured with default passwords. **Great, I am in…**”

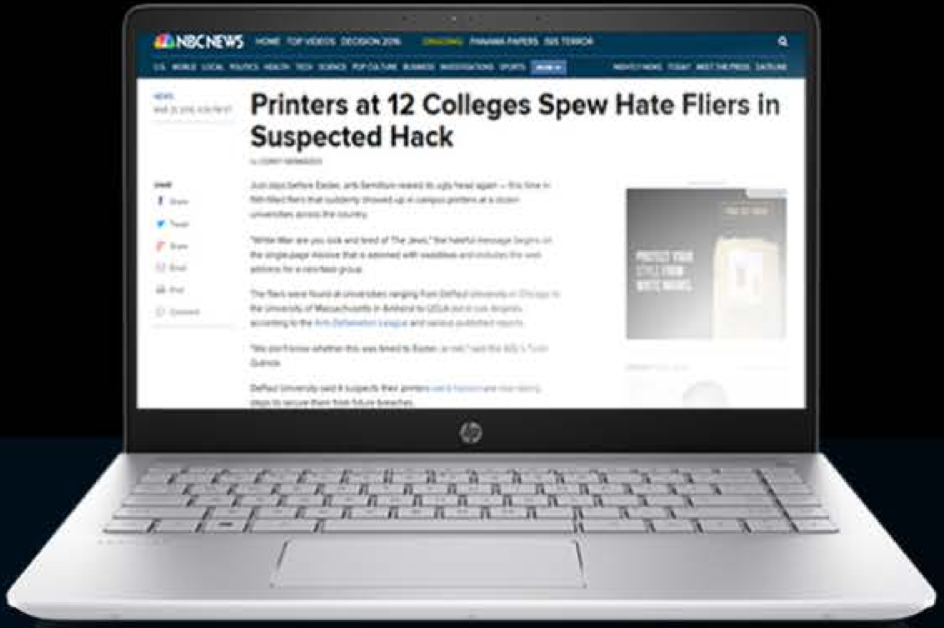
“We've compromised a number of companies using **printers as our initial foothold**. We move laterally from the printer, find Active Directory, query it with an account from the printer and bingo, **we hit GOLD…**”

Peter Kim
Industry-leading penetration Tester, Hacker, Author

“The Hacker Playbook 2: Practical Guide to Penetration Testing,” June 2015

The risk is real

Real-world events reveal an alarming trend


NBC NEWS
HOME TOP VIDEOS DECISION 2016 PANAMA PAPERS ISIS TERROR
U.S. WORLD LOCAL POLITICS HEALTH TECH SCIENCE POP CULTURE BUSINESS INVESTIGATIONS SPORTS
NIGHTLY NEWS TODAY MEET THE PRESS DATELINE
Share
Tweet
Share
Email
Print
Comment

NEWS

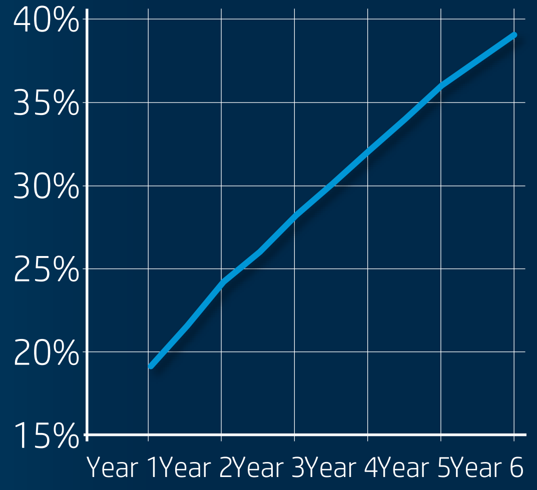
Printers at 12 Colleges Spew Hate Fliers in Suspected Hack

[illegible]

Hacker claims to have within minutes identified roughly

29,000 printers

that were connected to the Internet and could be exploited.*



Percent of breaches over time

The percentage of breaches involving a compromised end point device has **more than doubled** in the last 6 years*

Disclaimers:
29K vulnerable printers: Washington Times, "Hackers target US Universities sending anti-Semitic flyers to printers," 2016, http://www.antisemitismwatch.com/tag/the-washington-times
Percent of end-point breaches has more than doubled in the last 6 years: Verizon, 2016 Data Breach Investigations Report, 2016. www.verizonenterprise.com/verizon-insights-lab/dbir/2016

Today's printers act a whole lot like PCs

Yet only 16% of companies think printers are a high security risk.*

Hardware

Email

Network access

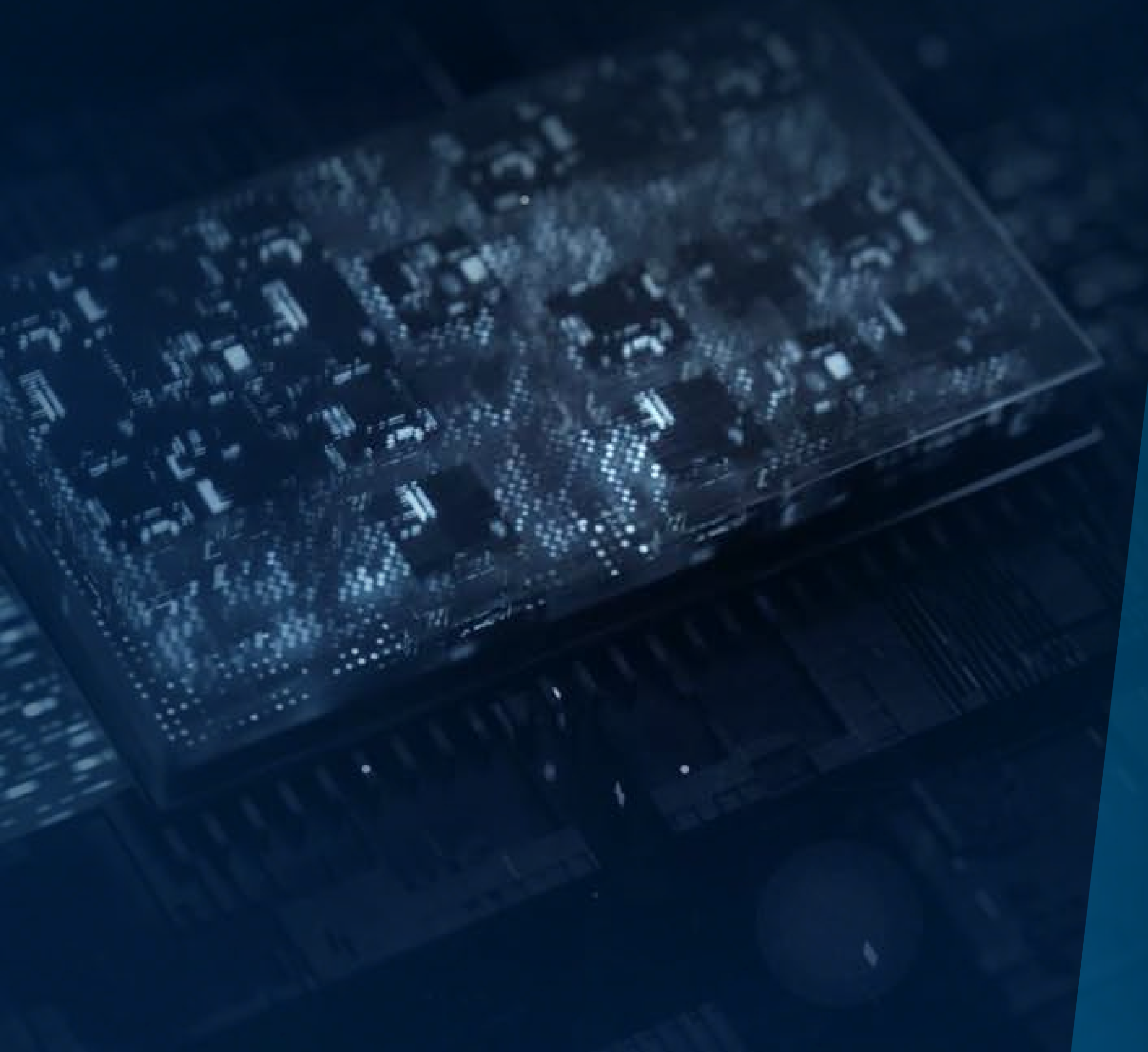
Firmware and software

Internet

Disclaimers:
16% of companies think printers are a high security risk: Spiceworks survey of 309 IT decision-makers in North America, EMEA, and APAC, on behalf of HP, November 2016.

Hardware and firmware

Modern malware targets



Software exploit

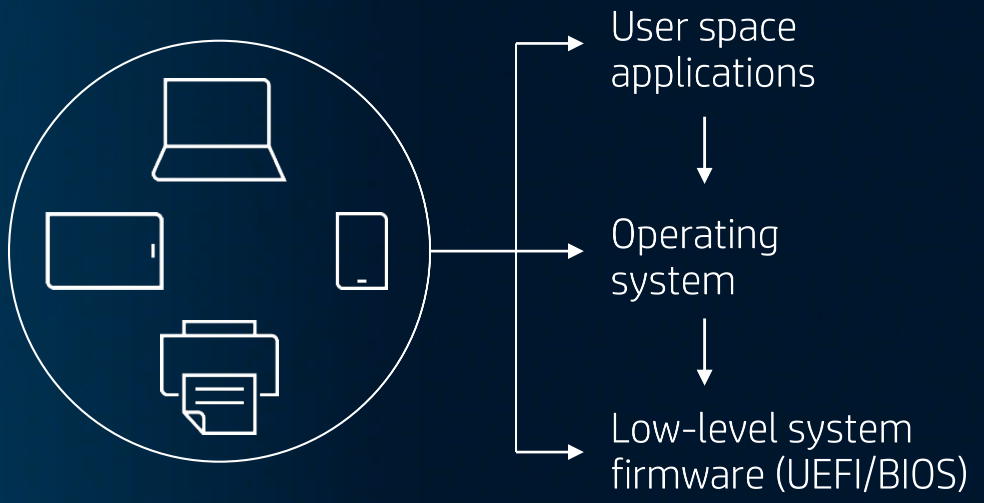
- Buffer overflow
- Misconfiguration
- Code injection (SQL)
- Open network ports and application vulnerability

Simple physical access exploits

- USB based attack

Human exploit

- Phishing email



User space applications

Operating system

Low-level system firmware (UEFI/BIOS)

Common imaging and printing vulnerability points

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

Management
Undetected security gaps put data at risk

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

Control panel
Users can exploit device settings and functions

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

Storage media
Printers store sensitive information that can be at risk

Capture
Unsecured MFPs can be used to send scans anywhere

Input tray
Special media can be tampered with or stolen

Output tray
Abandoned documents can fall into the wrong hands

Mobile printing
On-the-go employees may expose data

Building trust with device security

Design for cyber-resilience

Protect

Detect

Recover

Software security is **not enough**

Must start from the **firmware up**

Printing security requires an end-to-end approach

Device

Data

Document

Fleet security monitoring and compliance

Security services

Disclaimers:
HP Sure Start, whitelisting, run-time intrusion detection, HP Connection Inspector: For a list of compatible products, see hp.com/go/PrintersThatProtect.
HP Access Control must be purchased separately. To learn more, please visit hp.com/go/hpac.
HP JetAdvantage Secure Print: Pull printing works with any network-connected printer or MFP. On-device authentication is available for many HP LaserJet, PageWide, and OfficeJet Pro devices and selected non-HP devices. Some devices may require a firmware upgrade. Internet connection required for cloud storage and retrieval of print jobs. Print-job release from a mobile device requires a network connection and QR code. For more information and a list of supported printers and MFPs, see hp.com/go/JetAdvantageSecurePrint.
HP JetAdvantage Private Print is available at no charge and requires that the printer be connected to the Internet with web services enabled. It is supported on devices with touchscreens. Not available in all countries. Learn more at hp.com/go/JetAdvantagePrivatePrin
HP JetAdvantage Security Manager must be purchased separately. To learn more, please visit hp.com/go/securitymanager.
Trademarks:
Microsoft is a U.S. registered trademark of the Microsoft group of companies.

Printing security requires an end-to-end approach

Device

- Malware protection
- Self-healing features
- Certified compliant
- Secure erase and disposal
- Admin access controls
- Upgradeable firmware

Data

- Encryption in transit and at rest
- Device identity certificates
- Authentication and role-based access control
- Job tracking
- Data loss prevention
- Secure mobile printing

Document

- Pull print solutions
- Locking input trays
- Counterfeit deterrent solutions

Fleet security monitoring and compliance

- Firmware updates
- Automated monitoring and remediation
- Printer event data sent to SIEM tools
- Audit reporting

Security services

- HP Secure Managed Print Services
- HP Print Security Services

Secure the Device

HP Sure Start

Keeps the BIOS safe and self-heals

Whitelisting

Keeps the firmware safe

Run-time intrusion detection

Monitors run-time operations and self-heals

HP Connection Inspector

Monitors network connections and self-heals

HP Security Manager

Checks and remediates printer settings

Disclaimers:

Most secure printing: HP's most advanced embedded security features are available on HP Enterprise-class and Managed devices with FutureSmart firmware 4.5 or above and is based on HP review of 2017 published embedded security features of competitive in-class printers. Only HP offers a combination of security features for integrity checking down to the BIOS with self-healing capabilities. For a list of compatible products, visit: hp.com/go/PrintersThatProtect. For more information, visit: hp.com/go/printersecurityclaims.

Select HP LaserJet Pro, OfficeJet Pro, and PageWide Pro devices include embedded features that can detect and stop an attack. For more information, please visit hp.com/go/PrintersThatProtect.

HP JetAdvantage Security Manager must be purchased separately. To learn more, please visit hp.com/go/securitymanager.

Secure the Data

Authenticate users

Prevent unauthorized access

Encrypt the data

Prevent data theft and alteration

Monitor for threats

Identify issues and self-heal

Secure the Document

Workplace privacy

Maintain your print security defenses

Compliance

Secure document workflows

Anti-counterfeit

Deter document tampering and fraud

Getting started

Engage an HP Security Consultant

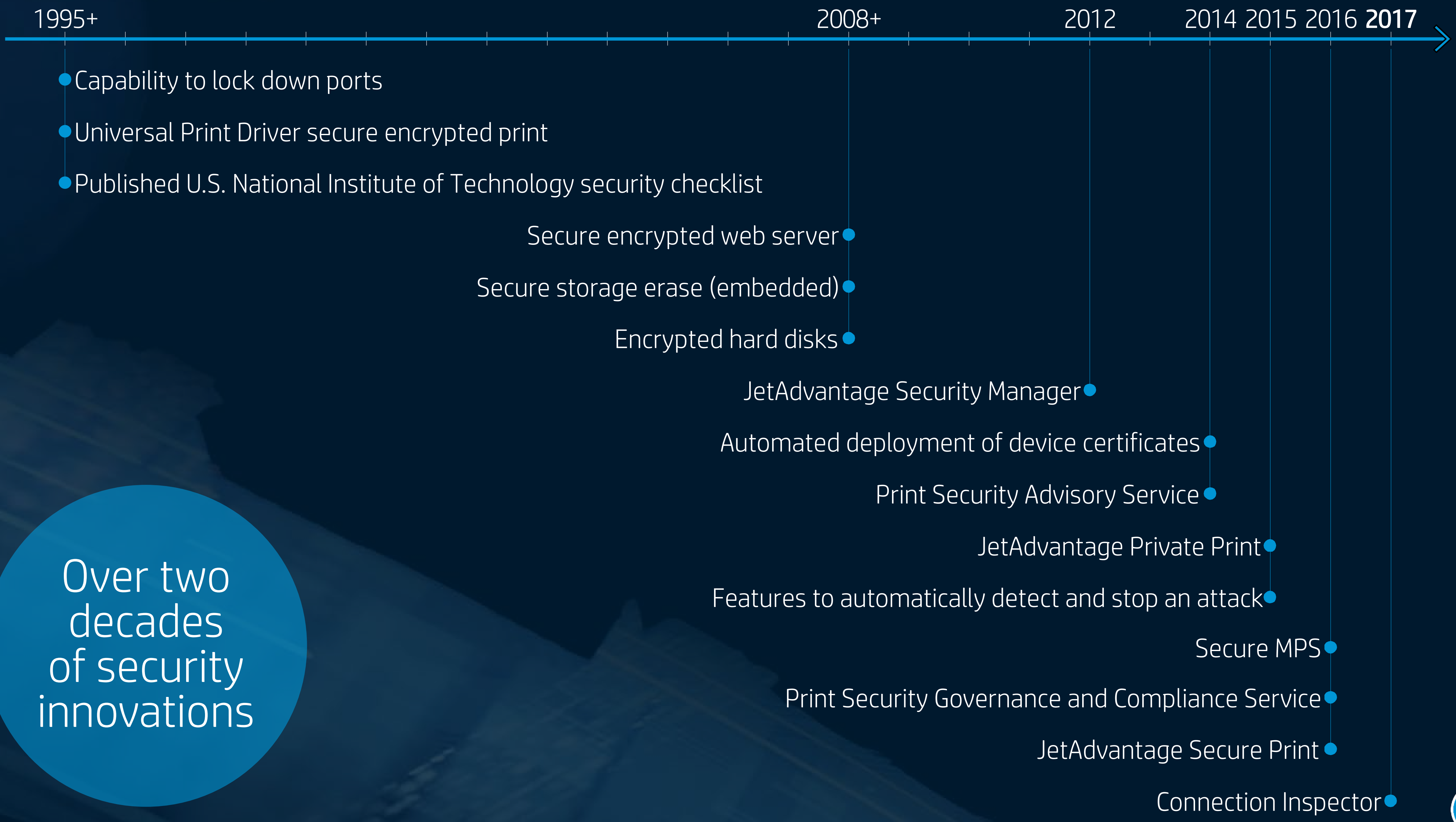
Bring in the experts

Run an assessment

Know your risks

Develop a plan

Secure your print fleet



1995+

- Capability to lock down ports
- Universal Print Driver secure encrypted print
- Published U.S. National Institute of Technology security checklist

2008+

- Secure encrypted web server
- Secure storage erase (embedded)
- Encrypted hard disks

2012

- JetAdvantage Security Manager

2014

- Automated deployment of device certificates
- Print Security Advisory Service

2015

- JetAdvantage Private Print
- Features to automatically detect and stop an attack

2016

- Secure MPS
- Print Security Governance and Compliance Service
- JetAdvantage Secure Print

2017

- Connection Inspector

Over two decades of security innovations

THANK YOU

Jason Kuhn