Keypoint Intelligence: Printer/MFP Security in the IoT Era

Jamie Bsales
Director, Solutions Analysis
jamie.bsales@keypointintelligence.com

June 2019

KEYPOINT INTELLIGENCE

Buyers Lab + InfoTrends = KEYPOINT INTELLIGENCE

Keypoint Intelligence is a brand built upon two great companies, Buyers Lab and InfoTrends. We are a collective force of unrivalled capabilities trusted all over the world to provide true end-to-end solutions and services which include in-depth product information, game changing insights, and responsive web tools that drive business growth.

Together, we empower confident decisions.

KEYPOINT INTELLIGENCE

Security Breaches 2018-2019

BBC NEWS
HSBC fined for personal data loss
msnbc
A LOST LAPTOP, A $54 MILLION LAWSUIT
130,000,000 CREDIT CARD #'S STOLEN
U.S. CONSUMERS SHOPPING IN FEAR AFTER 130 MILLION IDENTITIES STOLEN

LabCorp discloses data breach affecting 7.7 million customers…19 million patient records stolen from Quest Diagnostics

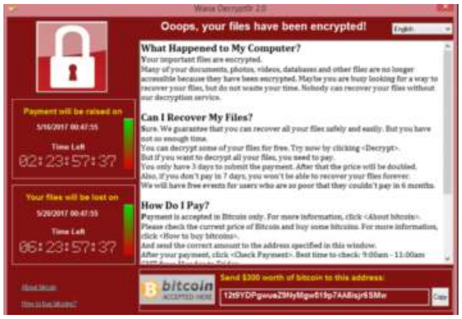
T-Mobile Hacked In Data Breach That Hit 2 Million Customers

Saks and Lord & Taylor point-of-sale systems compromised … information of 5 million customers exposed

Panera Bread database leak leads to exposure of 37 million customer records

Costs are Significant

- **Baltimore estimates cost of ransomware attack at $18.2 million**
- **The average estimated business cost of a ransomware attack (including ransom, work loss and time spent responding) $900,000**
- ***Experts estimate that more than half of businesses paying ransomware demands may not receive their data in return***


Wana Decrypt0r 2.0

Ooops, your files have been encrypted!

Payment will be raised on
5/16/2017 00:47:55
Time Left
02:23:57:37

Your files will be lost on
5/20/2017 00:47:55
Time Left
06:23:57:37

What Happened to My Computer?

Your important files are encrypted.
Many of your documents, photos, videos, databases and other files are no longer accessible because they have been encrypted. Maybe you are busy looking for a way to recover your files, but do not waste your time. Nobody can recover your files without our decryption service.

Can I Recover My Files?

Sure. We guarantee that you can recover all your files safely and easily. But you have not so enough time.
You can decrypt some of your files for free. Try now by clicking <Decrypt>.
But if you want to decrypt all your files, you need to pay.
You only have 3 days to submit the payment. After that the price will be doubled.
Also, if you don't pay in 7 days, you won't be able to recover your files forever.
We will have free events for users who are so poor that they couldn't pay in 6 months.

How Do I Pay?

Payment is accepted in Bitcoin only. For more information, click <About bitcoin>.
Please check the current price of Bitcoin and buy some bitcoins. For more information, click <How to buy bitcoins>.
And send the correct amount to the address specified in this window.
After your payment, click <Check Payment>. Best time to check: 9:00am - 11:00am

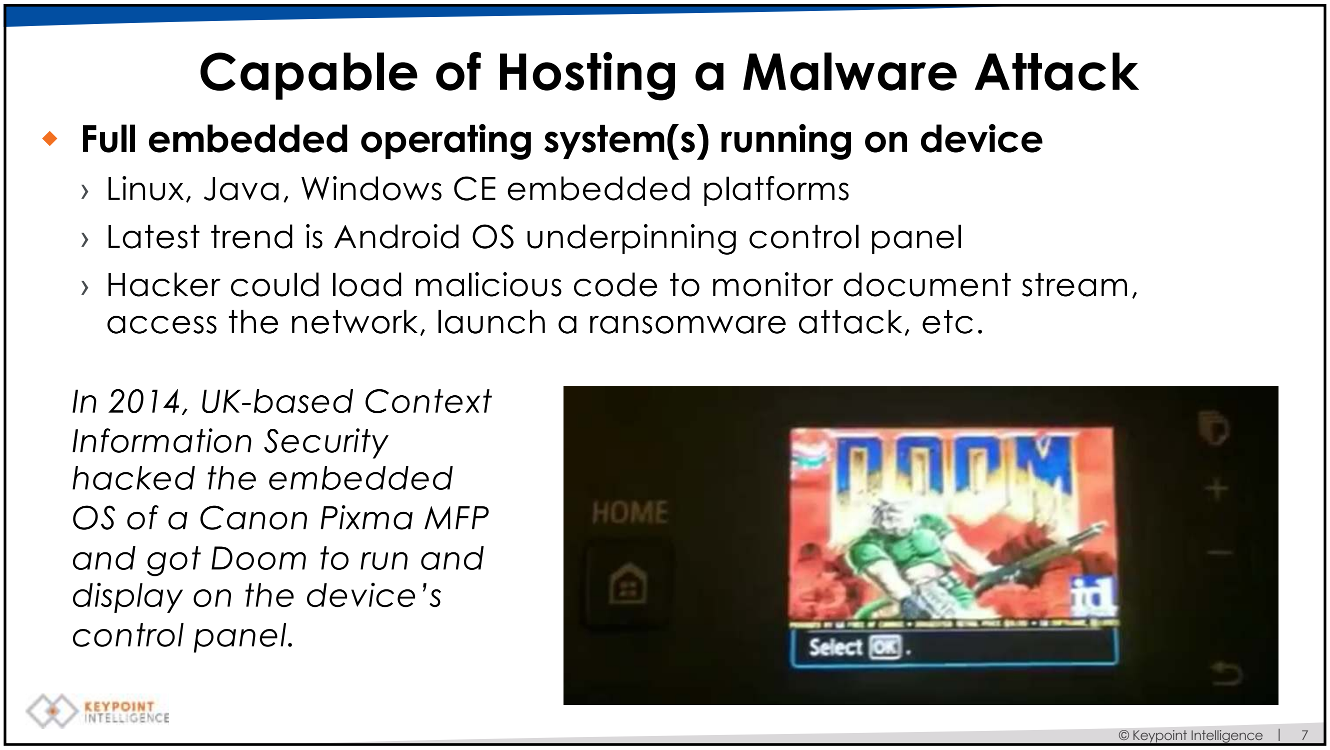
Send $300 worth of bitcoin to this address:
12t9YDPgwueZ9NyMgw519p7AA8isjr6SMw

Regulations Require Orgs to Protect Data

- **HIPAA** - requires health care organizations to protect private medical information
- **Gramm-Leach-Bliley Act** - requires financial institutions to implement the appropriate technical, physical and administrative safeguards to preserve the privacy of customer information
- **California SB 1386** - to protect consumers against identity theft resulting from their personal information being illegally obtained from corporate or government databases
- **Family Educational Rights and Privacy Act** - protects the privacy of student education records
- **Europe GDPR** – General Data Protection Regulation - regulation intended to strengthen and unify data protection for all individuals within the European Union
  - Several states in the US adopting similar regulations

Printer/MFP can be a Ticking Timebomb

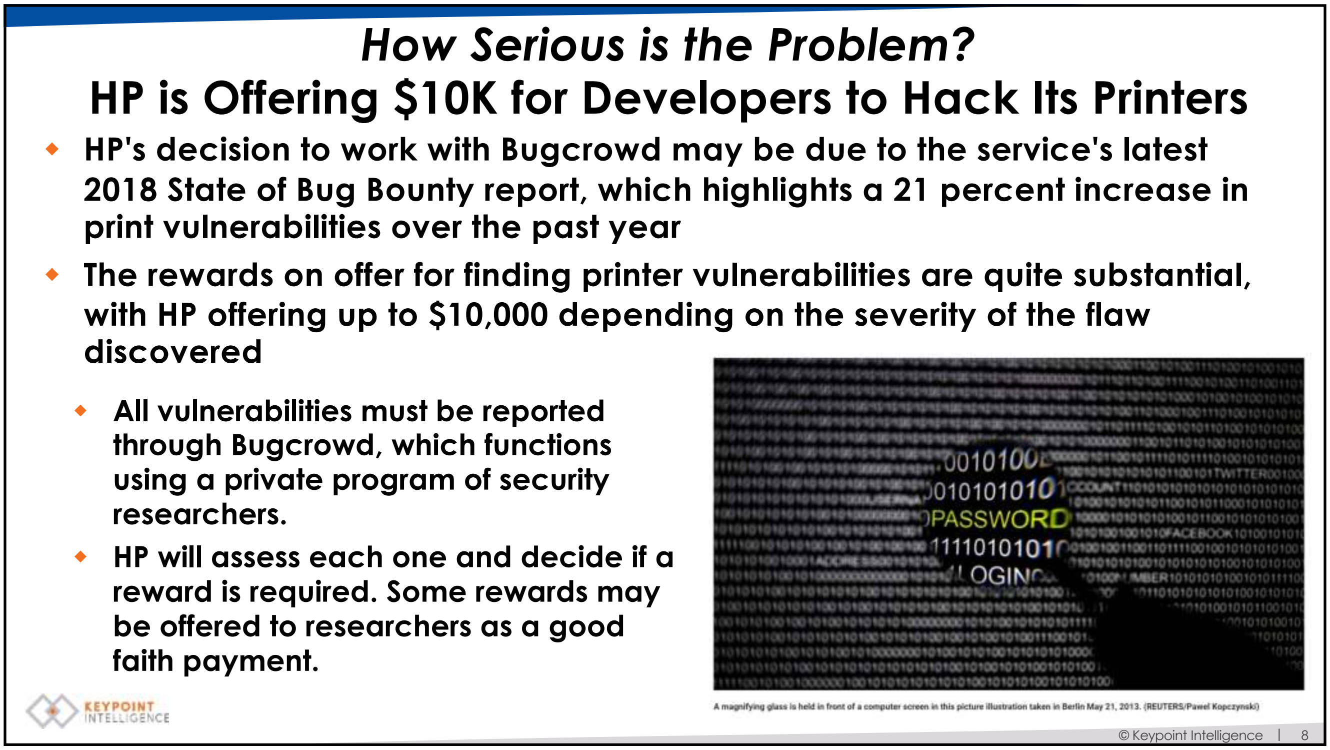
- **Conduit to the network**
  - Like a PC or server, an MFP is connected to both the Internet and the private network
  - Vulnerable threat to infiltrate the entire network
- **Easier target than PC or server**
  - Because MFPs typically are less secured than PCs/server, hackers see them as the weakest link and use this as an easy target into the network
- **Device-resident data at risk**
  - Hard drives contain stored documents and email addresses



Capable of Hosting a Malware Attack

- **Full embedded operating system(s) running on device**
  - › Linux, Java, Windows CE embedded platforms
  - › Latest trend is Android OS underpinning control panel
  - › Hacker could load malicious code to monitor document stream, access the network, launch a ransomware attack, etc.

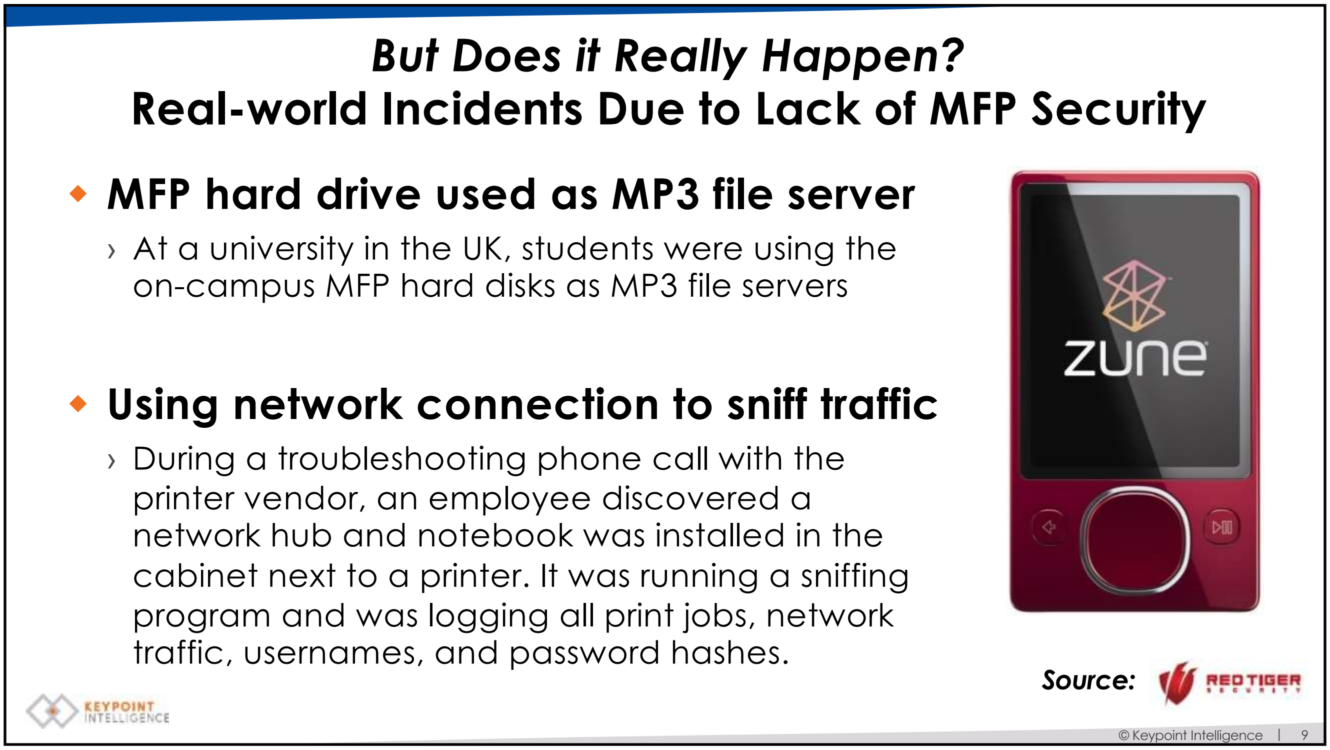
In 2014, UK-based Context Information Security hacked the embedded OS of a Canon Pixma MFP and got Doom to run and display on the device's control panel.



How Serious is the Problem?
HP is Offering $10K for Developers to Hack Its Printers

- **HP's decision to work with Bugcrowd may be due to the service's latest 2018 State of Bug Bounty report, which highlights a 21 percent increase in print vulnerabilities over the past year**
- **The rewards on offer for finding printer vulnerabilities are quite substantial, with HP offering up to $10,000 depending on the severity of the flaw discovered**
  - **All vulnerabilities must be reported through Bugcrowd, which functions using a private program of security researchers.**
  - **HP will assess each one and decide if a reward is required. Some rewards may be offered to researchers as a good faith payment.**

A magnifying glass is held in front of a computer screen in this picture illustration taken in Berlin May 21, 2013. (REUTERS/Pawel Kopczynski)

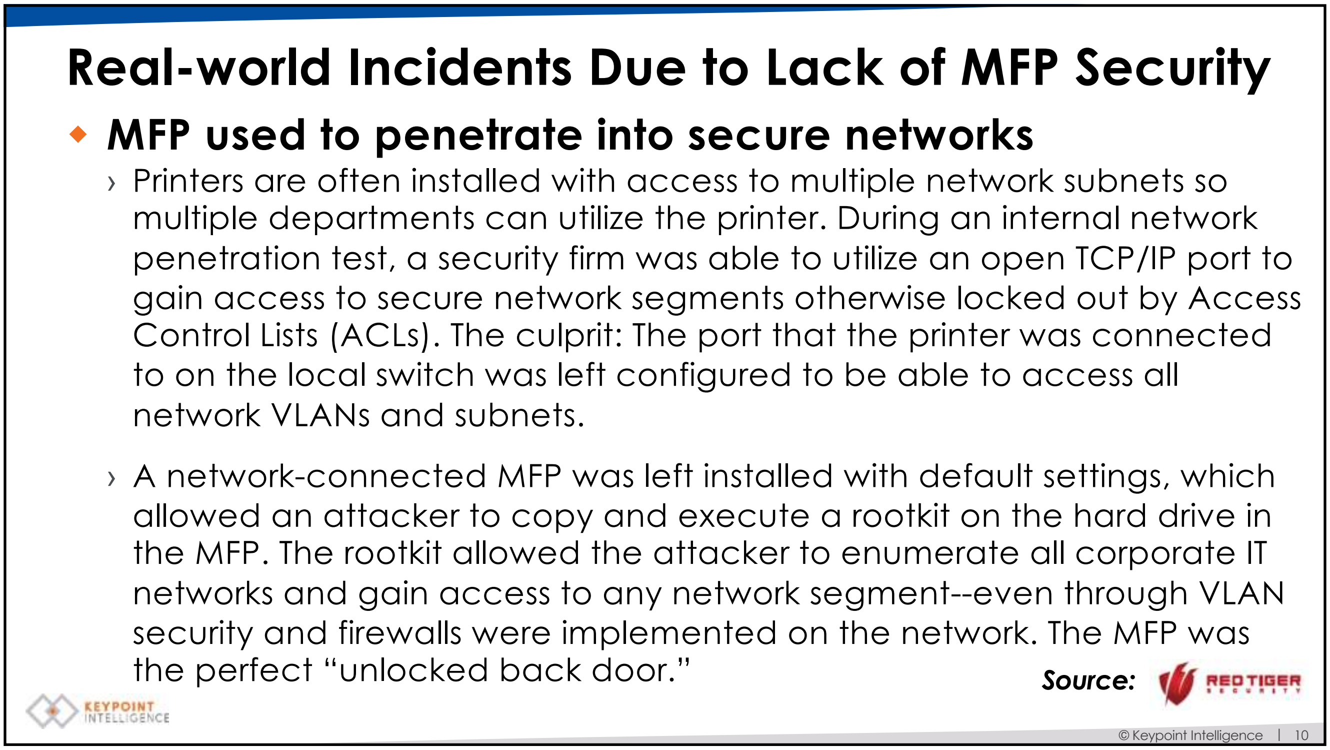


But Does it Really Happen?
Real-world Incidents Due to Lack of MFP Security

- **MFP hard drive used as MP3 file server**
  - At a university in the UK, students were using the on-campus MFP hard disks as MP3 file servers
- **Using network connection to sniff traffic**
  - During a troubleshooting phone call with the printer vendor, an employee discovered a network hub and notebook was installed in the cabinet next to a printer. It was running a sniffing program and was logging all print jobs, network traffic, usernames, and password hashes.

Source: REDTIGER SECURITY

© Keypoint Intelligence | 9

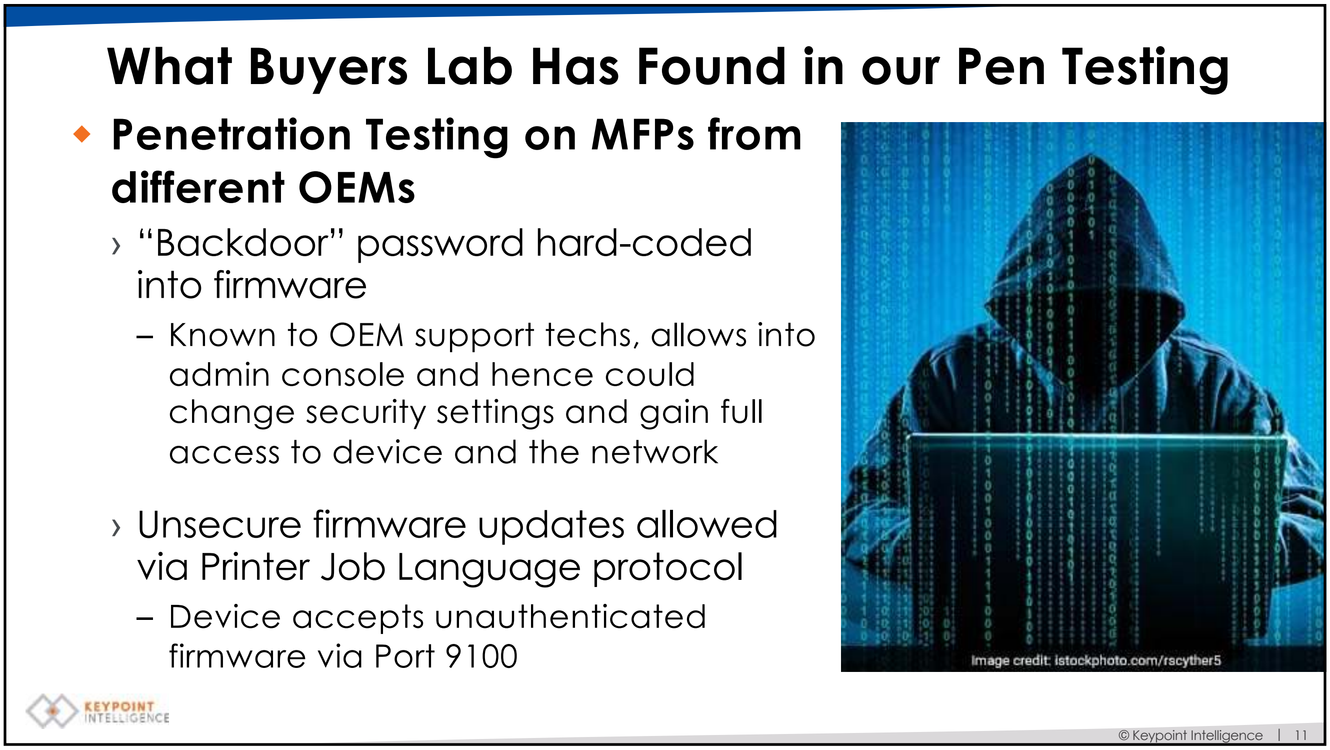


Real-world Incidents Due to Lack of MFP Security

- **MFP used to penetrate into secure networks**
  - Printers are often installed with access to multiple network subnets so multiple departments can utilize the printer. During an internal network penetration test, a security firm was able to utilize an open TCP/IP port to gain access to secure network segments otherwise locked out by Access Control Lists (ACLs). The culprit: The port that the printer was connected to on the local switch was left configured to be able to access all network VLANs and subnets.
  - A network-connected MFP was left installed with default settings, which allowed an attacker to copy and execute a rootkit on the hard drive in the MFP. The rootkit allowed the attacker to enumerate all corporate IT networks and gain access to any network segment--even through VLAN security and firewalls were implemented on the network. The MFP was the perfect “unlocked back door.”

Source: REDTIGER SECURITY

© Keypoint Intelligence | 10

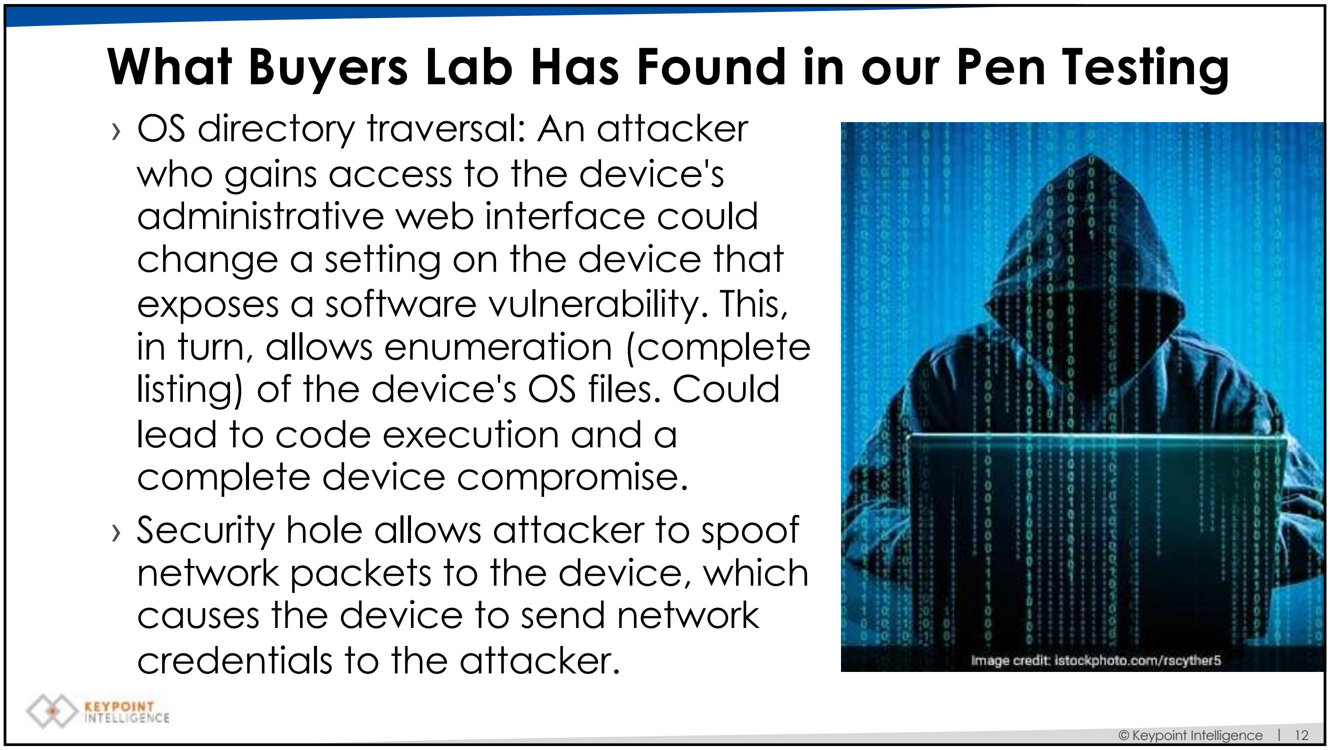


What Buyers Lab Has Found in our Pen Testing

- **Penetration Testing on MFPs from different OEMs**
  - “Backdoor” password hard-coded into firmware
    - Known to OEM support techs, allows into admin console and hence could change security settings and gain full access to device and the network
  - Unsecure firmware updates allowed via Printer Job Language protocol
    - Device accepts unauthenticated firmware via Port 9100

Image credit: istockphoto.com/rscyther5

© Keypoint Intelligence | 11

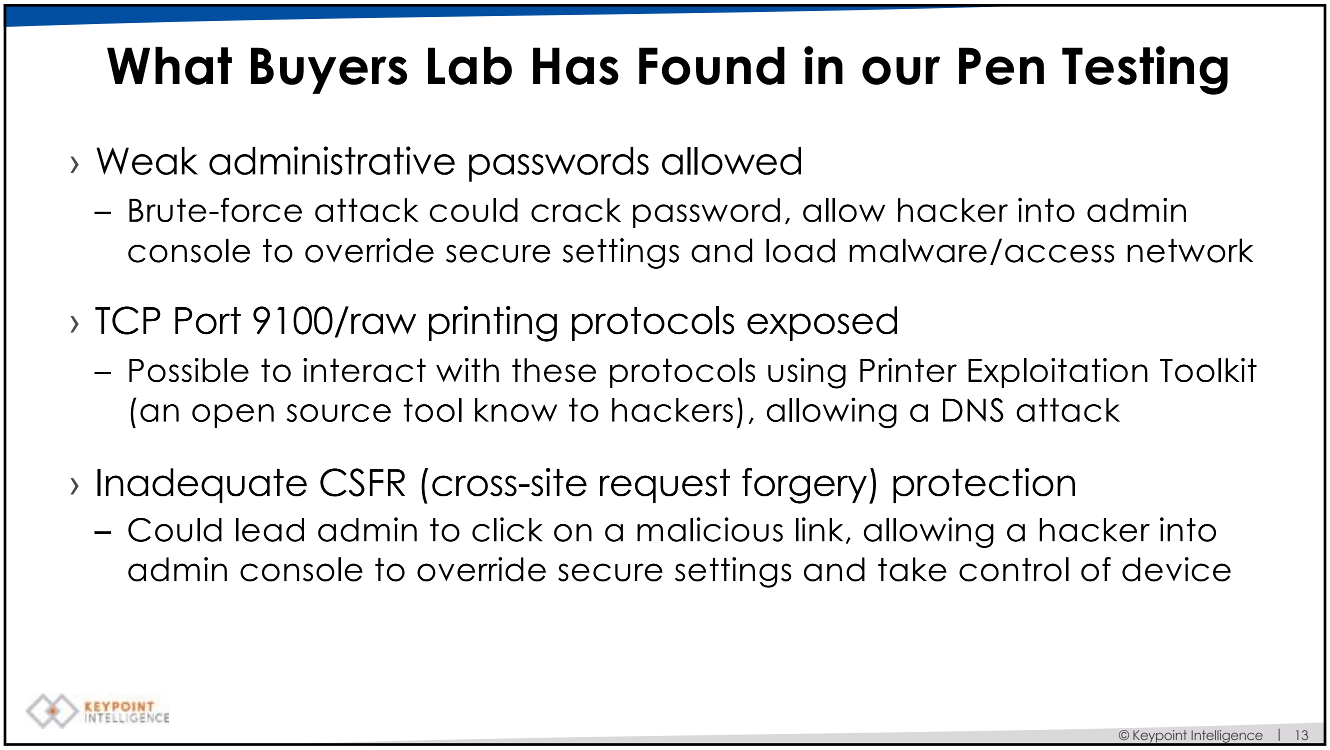


What Buyers Lab Has Found in our Pen Testing

- OS directory traversal: An attacker who gains access to the device's administrative web interface could change a setting on the device that exposes a software vulnerability. This, in turn, allows enumeration (complete listing) of the device's OS files. Could lead to code execution and a complete device compromise.
- Security hole allows attacker to spoof network packets to the device, which causes the device to send network credentials to the attacker.

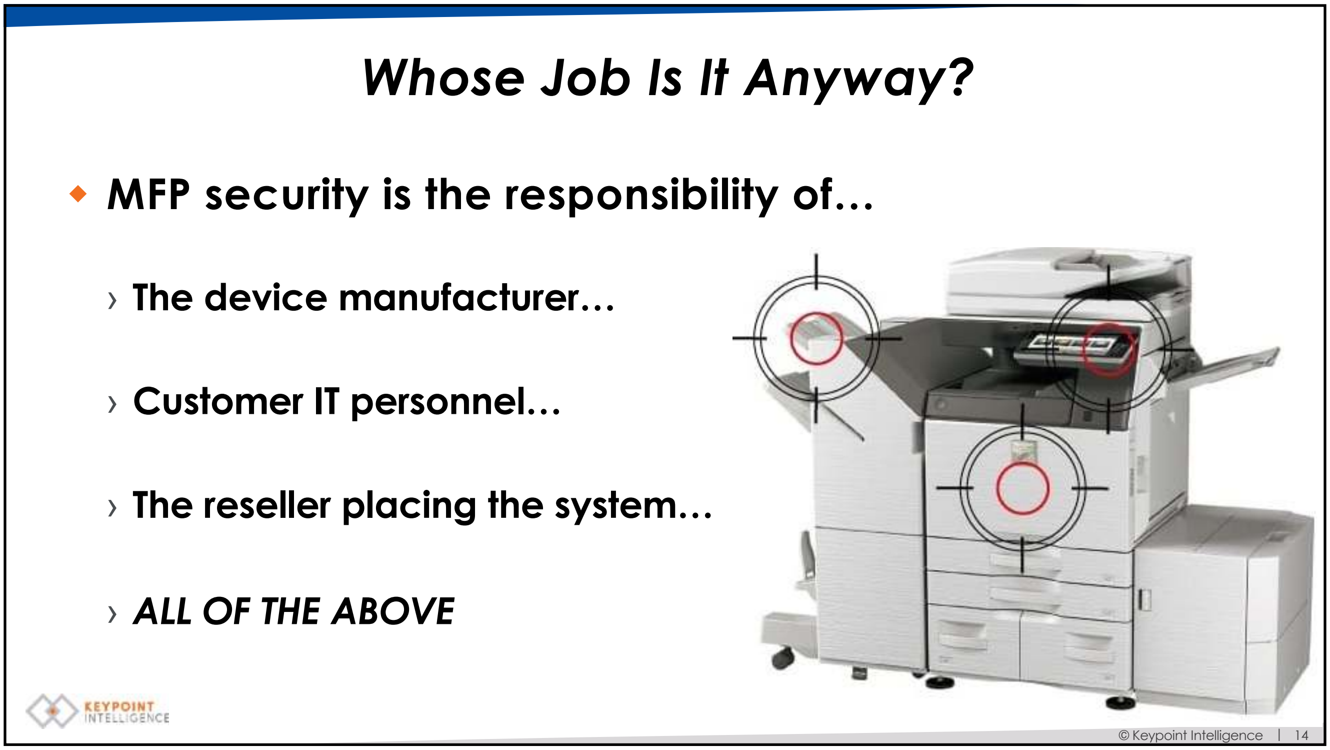
Image credit: istockphoto.com/rscyther5

© Keypoint Intelligence | 12



What Buyers Lab Has Found in our Pen Testing

- Weak administrative passwords allowed
  - Brute-force attack could crack password, allow hacker into admin console to override secure settings and load malware/access network
- TCP Port 9100/raw printing protocols exposed
  - Possible to interact with these protocols using Printer Exploitation Toolkit (an open source tool know to hackers), allowing a DNS attack
- Inadequate CSFR (cross-site request forgery) protection
  - Could lead admin to click on a malicious link, allowing a hacker into admin console to override secure settings and take control of device



Whose Job Is It Anyway?

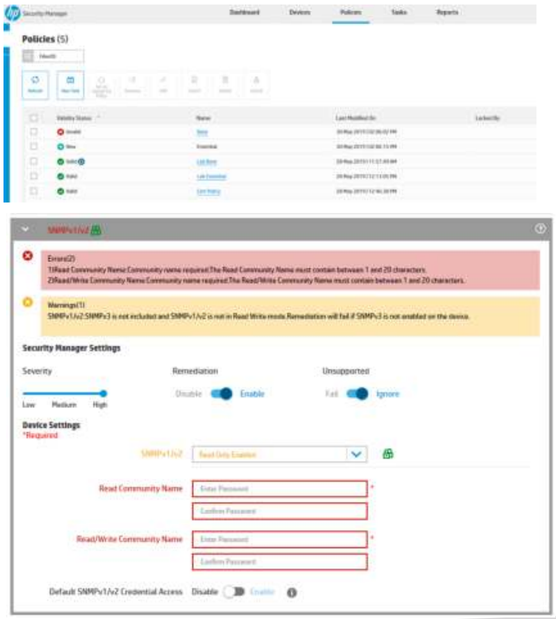
- **MFP security is the responsibility of…**
  - **The device manufacturer…**
  - **Customer IT personnel…**
  - **The reseller placing the system…**
  - ***ALL OF THE ABOVE***

OEMs Are Improving MFP Security…

- **Tight control over development environment**
  - Only approved vendors have access to SDK to develop for the embedded OS
- **Whitelisting capabilities**
  - No way to keep a “blacklist” of known malware current with evolving threats
  - Whitelist ensure that only known/approved apps will run
  - Require all apps loaded on MFP to be digitally signed
- **BIOS/firmware integrity checking**
  - At bootup (and after other events), BIOS/firmware/memory spaces checked against factory state to see if changed
- **SIEM system integration**
  - Feed device event info to enterprise Security Information Event Management solutions, which collect and analyze machine data from across an organization's IT environment to provide organizations with real-time indicators of potential security violations.

OEMs Are Improving MFP Security…

- **Device resiliency features**
  - NIST 800-193 guidelines for IoT devices: Ability to “self heal” and return firmware to a “clean” state after a breach
- **Policy creation/checking/enforcement**
  - Admin tools to create template for desired security settings (aka a “policy”), assign to devices, and remotely apply configurations to target devices
  - Monitor devices for changes to the policy
  - Alert IT personnel of out of compliance devices
  - Ideally, automatically bring the device back into compliance with the desired policy settings



Policies (5)

Validity Status	Name	Last Modified On	Locked By
Invalid	[illegible]	[illegible]	
New	Essential	[illegible]	
Valid	[illegible]	[illegible]	
Valid	[illegible]	[illegible]	
Valid	[illegible]	[illegible]	

SNMPv1/v2

Errors(2)
1)Read Community Name:Community name required.The Read Community Name must contain between 1 and 20 characters.
2)Read/Write Community Name:Community name required.The Read/Write Community Name must contain between 1 and 20 characters.

Warnings(1)
SNMPv1/v2:SNMPv3 is not included and SNMPv1/v2 is not in Read Write mode.Remediation will fail if SNMPv3 is not enabled on the device.

Security Manager Settings

Severity: Low — Medium — High

Remediation: Disable ● Enable

Unsupported: Fail ● Ignore

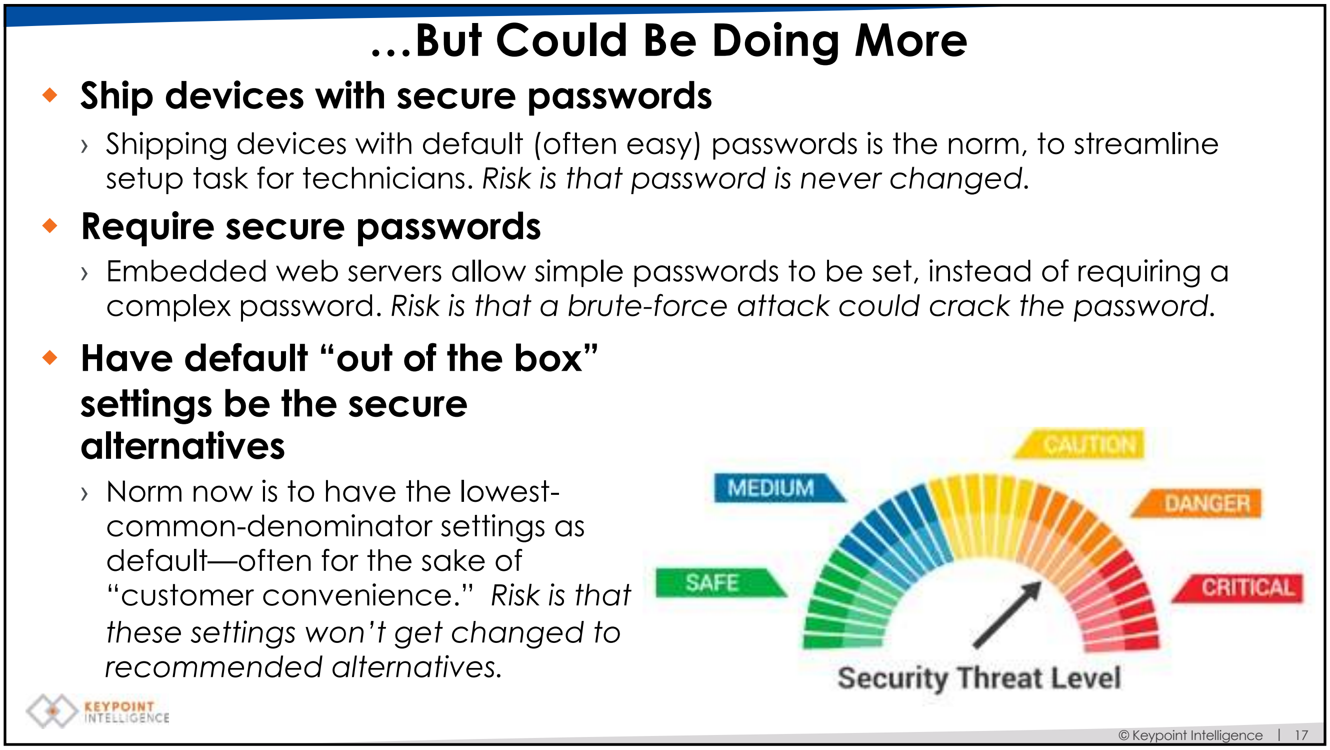
Device Settings
*Required

SNMPv1/v2: Read Only Enabled

Read Community Name: Enter Password * / Confirm Password

Read/Write Community Name: Enter Password * / Confirm Password

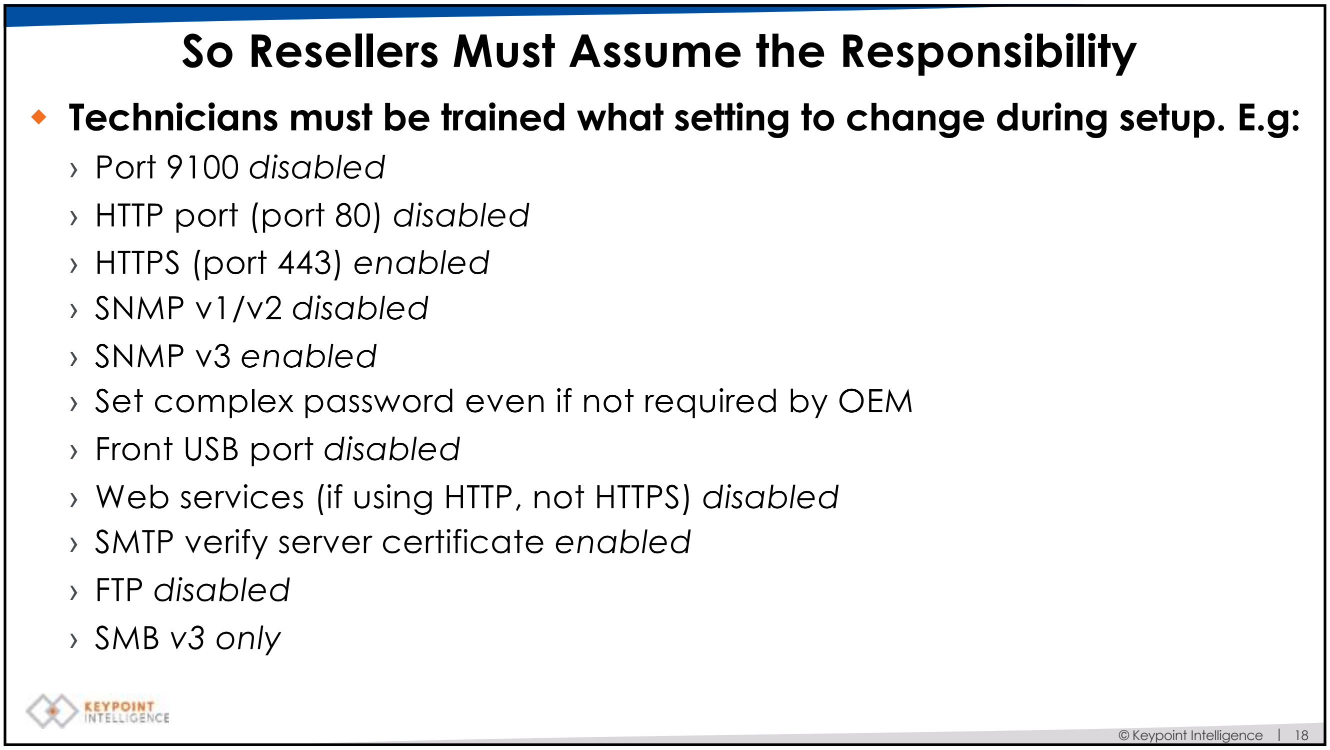
Default SNMPv1/v2 Credential Access: Disable ○ Enable



…But Could Be Doing More

- **Ship devices with secure passwords**
  - Shipping devices with default (often easy) passwords is the norm, to streamline setup task for technicians. *Risk is that password is never changed.*
- **Require secure passwords**
  - Embedded web servers allow simple passwords to be set, instead of requiring a complex password. *Risk is that a brute-force attack could crack the password.*
- **Have default "out of the box" settings be the secure alternatives**
  - Norm now is to have the lowest-common-denominator settings as default—often for the sake of "customer convenience." *Risk is that these settings won't get changed to recommended alternatives.*

© Keypoint Intelligence | 17



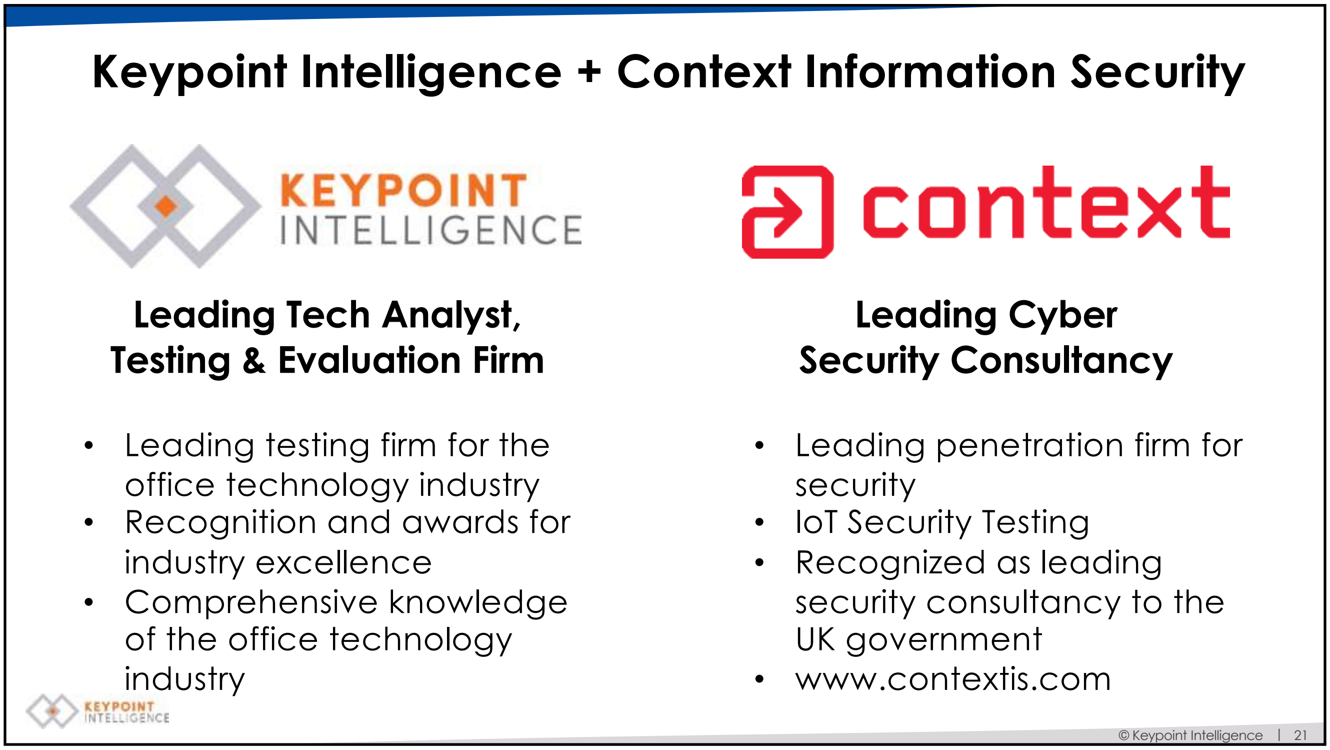
So Resellers Must Assume the Responsibility

- **Technicians must be trained what setting to change during setup. E.g:**
  - Port 9100 *disabled*
  - HTTP port (port 80) *disabled*
  - HTTPS (port 443) *enabled*
  - SNMP v1/v2 *disabled*
  - SNMP v3 *enabled*
  - Set complex password even if not required by OEM
  - Front USB port *disabled*
  - Web services (if using HTTP, not HTTPS) *disabled*
  - SMTP verify server certificate *enabled*
  - FTP *disabled*
  - SMB v3 *only*

© Keypoint Intelligence | 18

Keypoint Intelligence MFP Security Testing 2019

“Keypoint Intelligence will be the defacto standard for Security Testing & Recognition for the Office Equipment Industry & the Smart Workplace…”



Keypoint Intelligence + Context Information Security

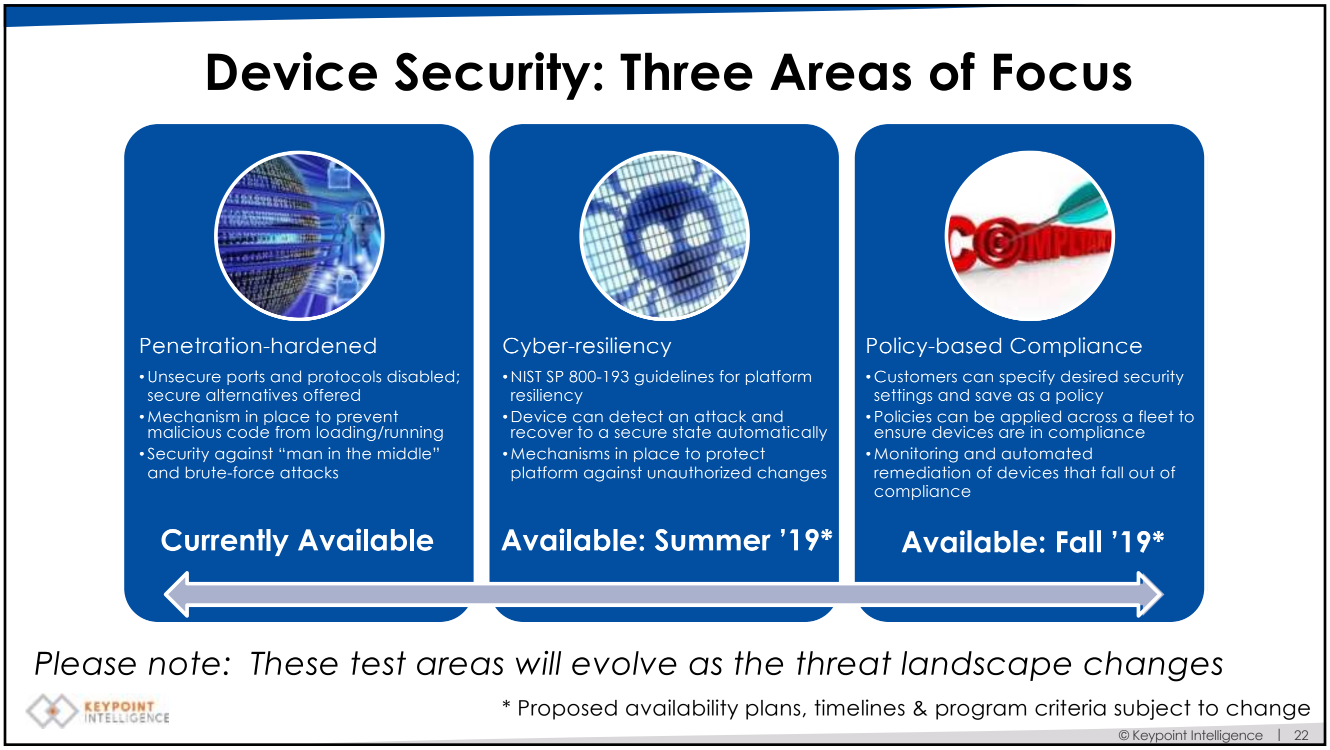
Leading Tech Analyst, Testing & Evaluation Firm

- Leading testing firm for the office technology industry
- Recognition and awards for industry excellence
- Comprehensive knowledge of the office technology industry

Leading Cyber Security Consultancy

- Leading penetration firm for security
- IoT Security Testing
- Recognized as leading security consultancy to the UK government
- www.contextis.com

© Keypoint Intelligence | 21



Device Security: Three Areas of Focus

Penetration-hardened

- Unsecure ports and protocols disabled; secure alternatives offered
- Mechanism in place to prevent malicious code from loading/running
- Security against "man in the middle" and brute-force attacks

Currently Available

Cyber-resiliency

- NIST SP 800-193 guidelines for platform resiliency
- Device can detect an attack and recover to a secure state automatically
- Mechanisms in place to protect platform against unauthorized changes

Available: Summer '19*

Policy-based Compliance

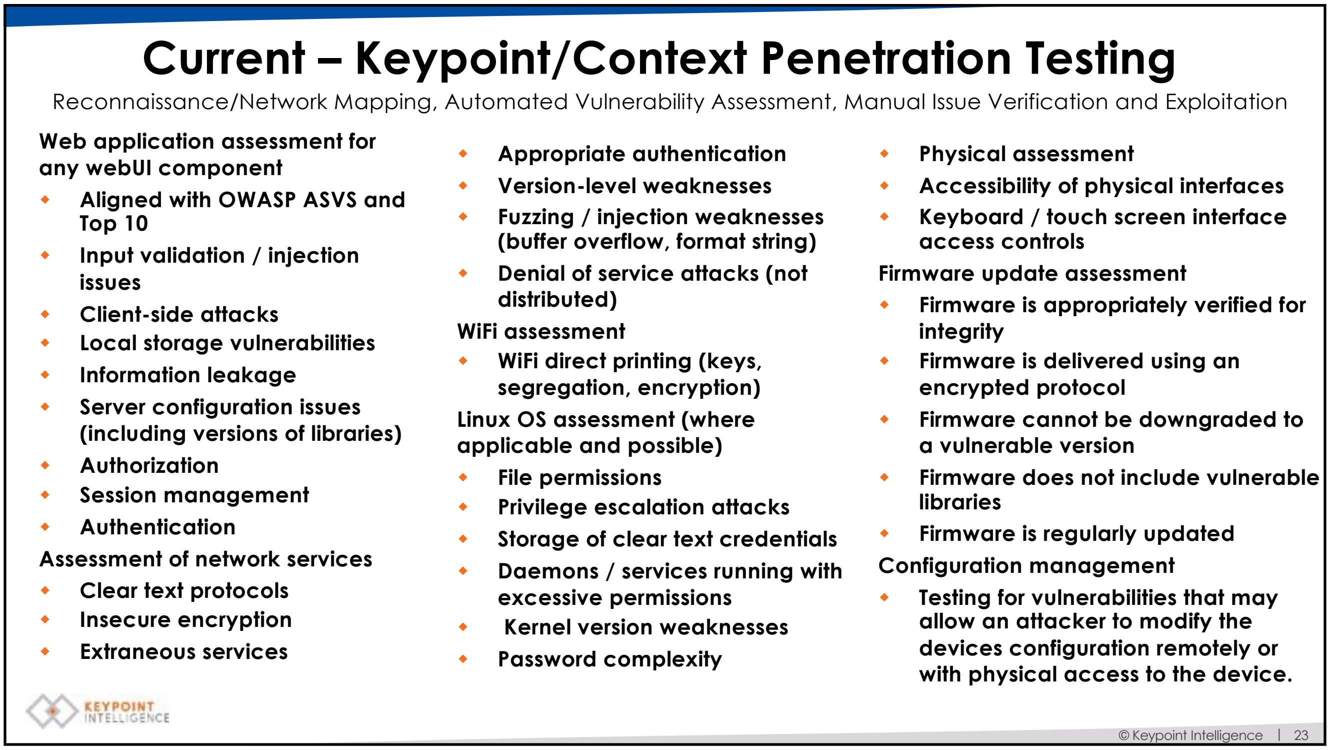
- Customers can specify desired security settings and save as a policy
- Policies can be applied across a fleet to ensure devices are in compliance
- Monitoring and automated remediation of devices that fall out of compliance

Available: Fall '19*

Please note: These test areas will evolve as the threat landscape changes

* Proposed availability plans, timelines & program criteria subject to change

© Keypoint Intelligence | 22



Current – Keypoint/Context Penetration Testing

Reconnaissance/Network Mapping, Automated Vulnerability Assessment, Manual Issue Verification and Exploitation

Web application assessment for any webUI component

- Aligned with OWASP ASVS and Top 10
- Input validation / injection issues
- Client-side attacks
- Local storage vulnerabilities
- Information leakage
- Server configuration issues (including versions of libraries)
- Authorization
- Session management
- Authentication

Assessment of network services

- Clear text protocols
- Insecure encryption
- Extraneous services
- Appropriate authentication
- Version-level weaknesses
- Fuzzing / injection weaknesses (buffer overflow, format string)
- Denial of service attacks (not distributed)

WiFi assessment

- WiFi direct printing (keys, segregation, encryption)

Linux OS assessment (where applicable and possible)

- File permissions
- Privilege escalation attacks
- Storage of clear text credentials
- Daemons / services running with excessive permissions
- Kernel version weaknesses
- Password complexity
- Physical assessment
- Accessibility of physical interfaces
- Keyboard / touch screen interface access controls

Firmware update assessment

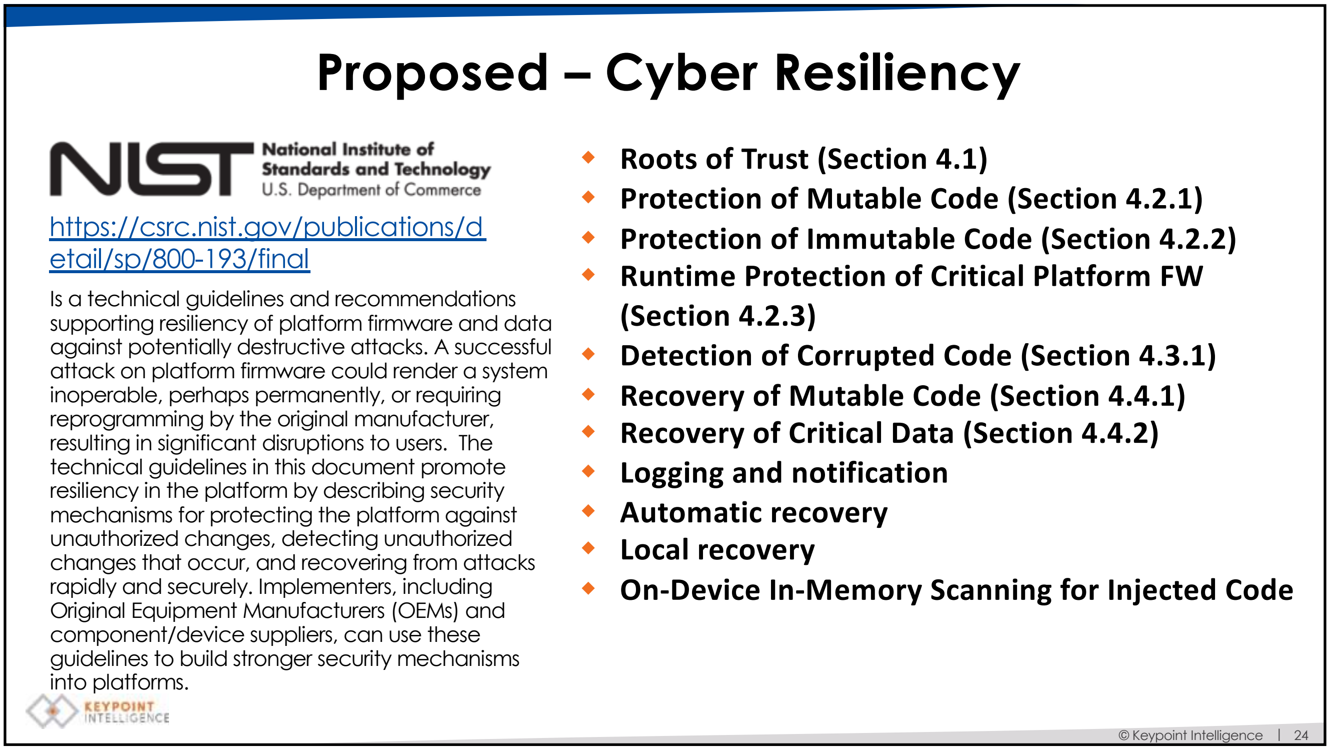
- Firmware is appropriately verified for integrity
- Firmware is delivered using an encrypted protocol
- Firmware cannot be downgraded to a vulnerable version
- Firmware does not include vulnerable libraries
- Firmware is regularly updated

Configuration management

- Testing for vulnerabilities that may allow an attacker to modify the devices configuration remotely or with physical access to the device.

KEYPOINT INTELLIGENCE

© Keypoint Intelligence | 23



Proposed – Cyber Resiliency

NIST National Institute of Standards and Technology U.S. Department of Commerce

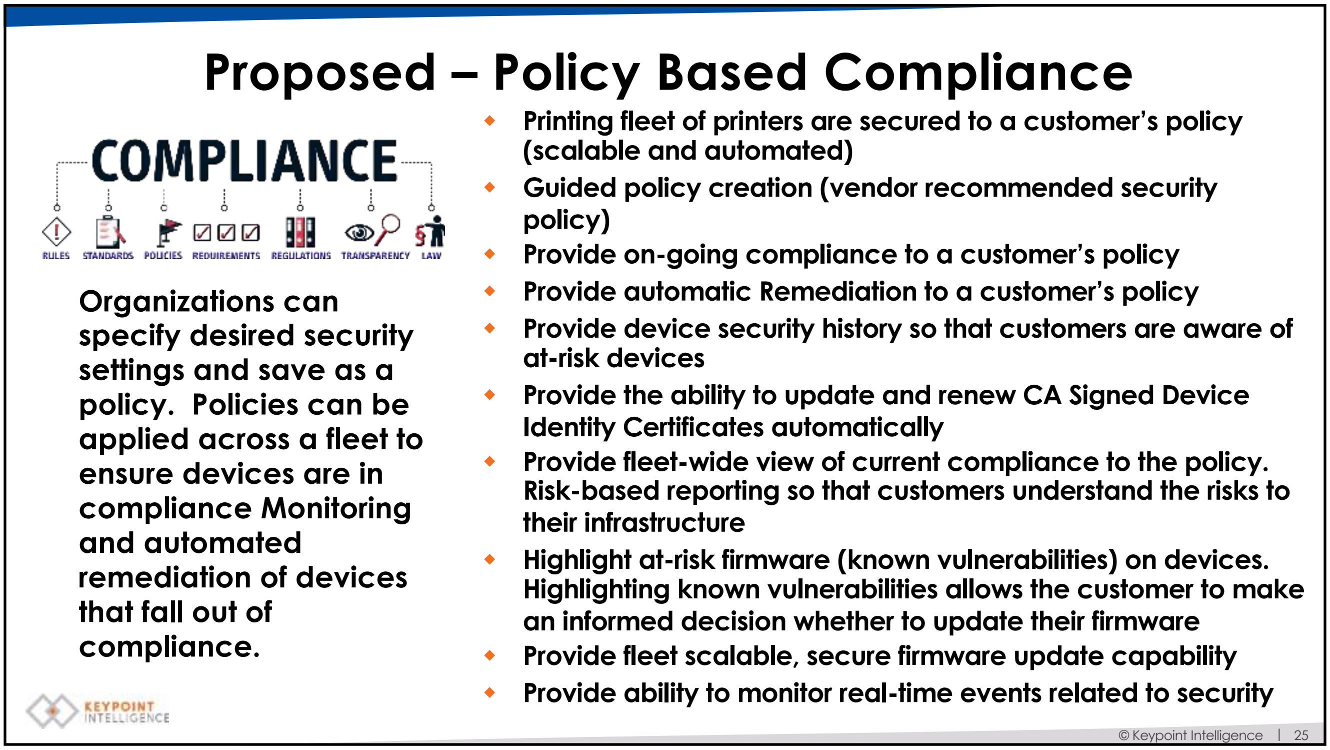
https://csrc.nist.gov/publications/detail/sp/800-193/final

Is a technical guidelines and recommendations supporting resiliency of platform firmware and data against potentially destructive attacks. A successful attack on platform firmware could render a system inoperable, perhaps permanently, or requiring reprogramming by the original manufacturer, resulting in significant disruptions to users. The technical guidelines in this document promote resiliency in the platform by describing security mechanisms for protecting the platform against unauthorized changes, detecting unauthorized changes that occur, and recovering from attacks rapidly and securely. Implementers, including Original Equipment Manufacturers (OEMs) and component/device suppliers, can use these guidelines to build stronger security mechanisms into platforms.

- Roots of Trust (Section 4.1)
- Protection of Mutable Code (Section 4.2.1)
- Protection of Immutable Code (Section 4.2.2)
- Runtime Protection of Critical Platform FW (Section 4.2.3)
- Detection of Corrupted Code (Section 4.3.1)
- Recovery of Mutable Code (Section 4.4.1)
- Recovery of Critical Data (Section 4.4.2)
- Logging and notification
- Automatic recovery
- Local recovery
- On-Device In-Memory Scanning for Injected Code

KEYPOINT INTELLIGENCE

© Keypoint Intelligence | 24



Proposed – Policy Based Compliance

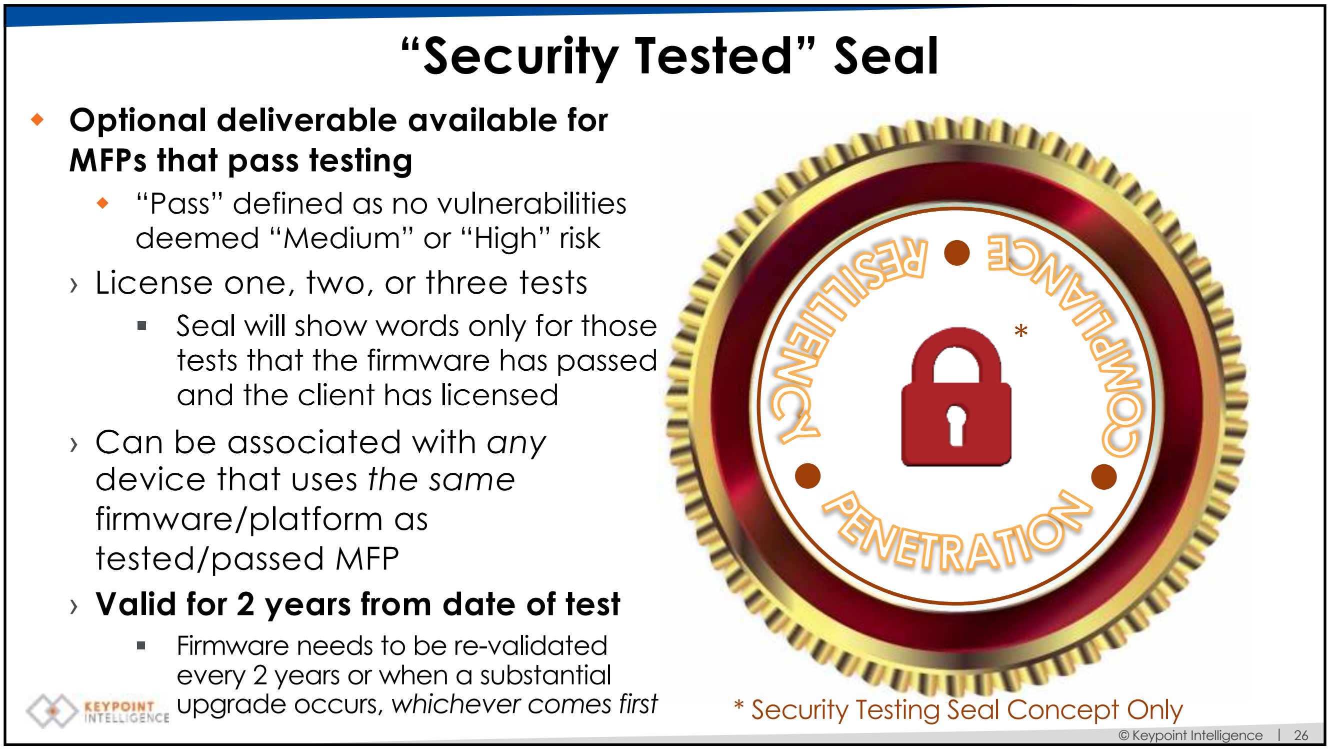
COMPLIANCE
RULES
STANDARDS
POLICIES
REQUIREMENTS
REGULATIONS
TRANSPARENCY
LAW

Organizations can specify desired security settings and save as a policy. Policies can be applied across a fleet to ensure devices are in compliance Monitoring and automated remediation of devices that fall out of compliance.

- Printing fleet of printers are secured to a customer's policy (scalable and automated)
- Guided policy creation (vendor recommended security policy)
- Provide on-going compliance to a customer's policy
- Provide automatic Remediation to a customer's policy
- Provide device security history so that customers are aware of at-risk devices
- Provide the ability to update and renew CA Signed Device Identity Certificates automatically
- Provide fleet-wide view of current compliance to the policy. Risk-based reporting so that customers understand the risks to their infrastructure
- Highlight at-risk firmware (known vulnerabilities) on devices. Highlighting known vulnerabilities allows the customer to make an informed decision whether to update their firmware
- Provide fleet scalable, secure firmware update capability
- Provide ability to monitor real-time events related to security

KEYPOINT INTELLIGENCE

© Keypoint Intelligence | 25



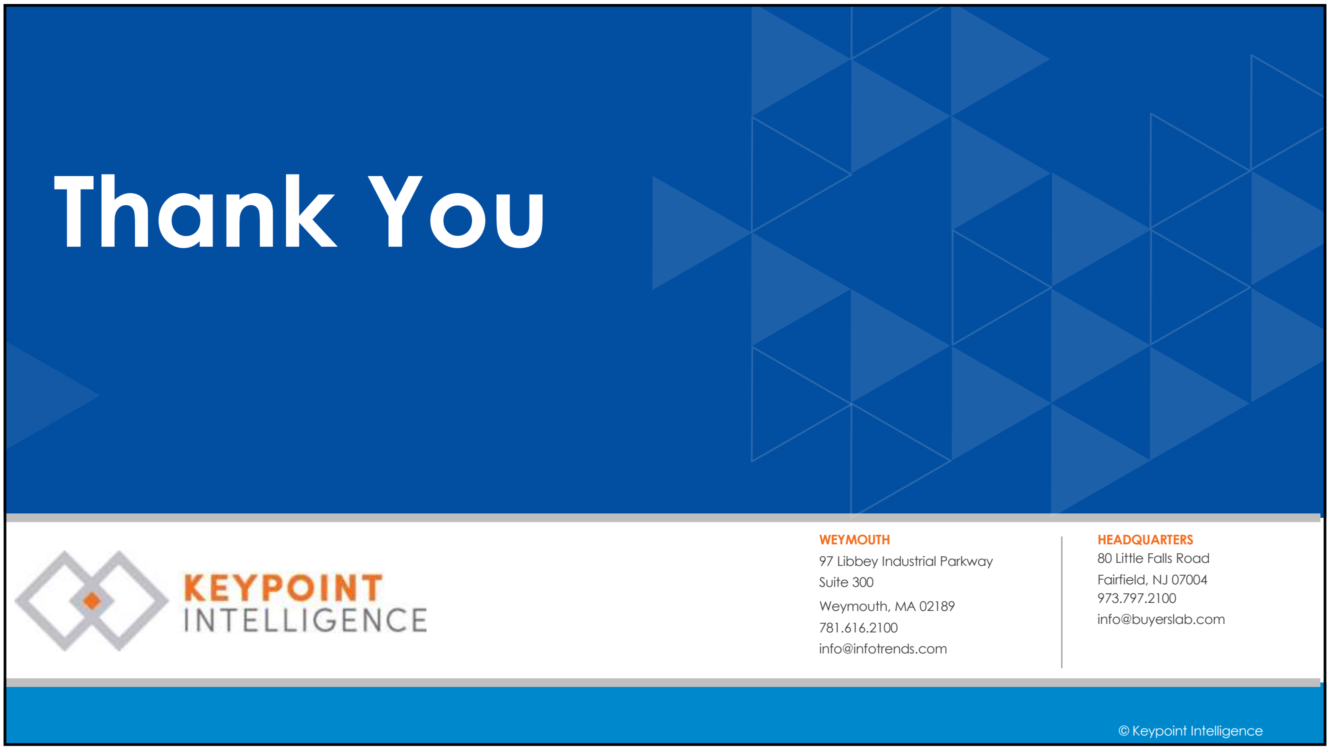
"Security Tested" Seal

- **Optional deliverable available for MFPs that pass testing**
  - "Pass" defined as no vulnerabilities deemed "Medium" or "High" risk
- › License one, two, or three tests
  - ▪ Seal will show words only for those tests that the firmware has passed and the client has licensed
- › Can be associated with *any* device that uses *the same* firmware/platform as tested/passed MFP
- › **Valid for 2 years from date of test**
  - ▪ Firmware needs to be re-validated every 2 years or when a substantial upgrade occurs, *whichever comes first*

* Security Testing Seal Concept Only

KEYPOINT INTELLIGENCE

© Keypoint Intelligence | 26



Thank You

KEYPOINT INTELLIGENCE

WEYMOUTH
97 Libbey Industrial Parkway
Suite 300
Weymouth, MA 02189
781.616.2100
info@infotrends.com

HEADQUARTERS
80 Little Falls Road
Fairfield, NJ 07004
973.797.2100
info@buyerslab.com

© Keypoint Intelligence