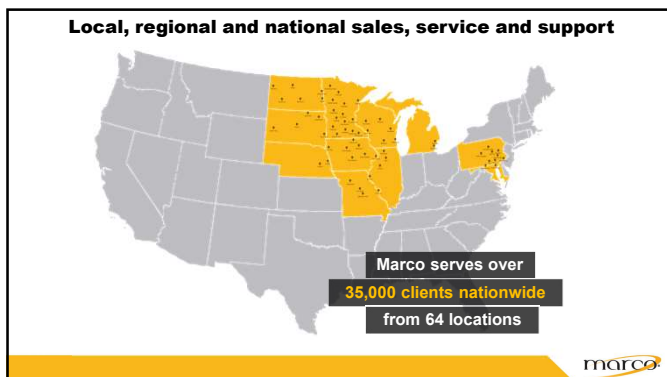




1



2

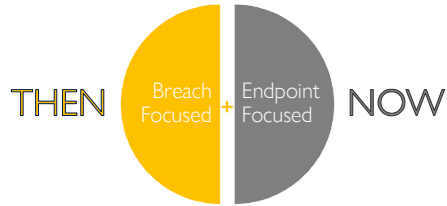


3



4

## State of Print Security



5

## Breach Focused

Controlling the transmission, storage, and processing of data

Secure data at rest, and in transit

- Print Data Flows
- Scan Data Flows

Breach Focused Controls:

**Hard Drives**  
Encryption

**Output Tray**  
Secure Printing

**Data Loss Prevention**  
Non-repudiation

6

## Endpoint Focused

Printers as fully fledged network endpoints

Printers are endpoints that:

- ... are network connected
- ... process sensitive data
- ... have credentials
- ... require patching
- ... stick around past EOL

7

## Endpoint Focused Framework

Default Configs

**Configuration**  
Device Hardening

**Firmware**  
Patch Management

**Hardware**  
Lifecycle Management (EOL)

Scarily Updated



Featureless

Long Lived

8

## Attacks at Every Skill Level

### Average Skill

**PRIVILEGE  
ESCALATION**

### Low Skill

**UNAUTHORIZED  
ACCESS**

9

## Print Security is Complicated

<b>DATA AND INFORMATION SECURITY</b> <ul style="list-style-type: none"> <li>Data Overwrite</li> <li>Manual Data Overwrite</li> <li>Custom and DOD 3200.22-01</li> <li>End-of-Lease Data Erase</li> <li>Power-Up Data Overwrite</li> <li>Up to 16 Times Data Overwrite</li> <li>256-Bit AES Data Encryption</li> <li>Data Backup/Disaster Recovery</li> </ul>	<b>ACCESS CONTROL SECURITY</b> <ul style="list-style-type: none"> <li>User Authentication (Local/LDAP/Active Directory)</li> <li>Group Authentication</li> <li>Page Limit Control</li> <li>Password Protected Access to Device Home Page (Administrator and User)</li> <li>User Authority Setting</li> <li>Single Sign-On (Kerberos and OAuth Token)</li> <li>USB Card Reader Support</li> <li>ID Card User Authentication</li> <li>Scan-to-Home and Scan-to-Me</li> </ul>	<b>PRINT SECURITY</b> <ul style="list-style-type: none"> <li>User Authentication</li> <li>TLS Encryption</li> <li>Secure Panel Release with a PIN Number</li> <li>Serverless Print Release</li> <li>Sharp CSA Applications</li> </ul>
<b>FAX SECURITY</b> <ul style="list-style-type: none"> <li>Segregated Fax Line</li> <li>Prevention of Junk Fax</li> <li>Confidential Fax</li> </ul>	<b>NETWORK SECURITY</b> <ul style="list-style-type: none"> <li>TLS Encryption (2048 bit Key supported)</li> <li>Security Policy Management</li> <li>SNMPv3</li> <li>SNMP Community Name Support</li> <li>Kerberos</li> <li>IPv6 and IPv4</li> <li>Device Certificates</li> <li>IP Address Filtering</li> <li>MAC Address Filtering</li> <li>Port Control</li> <li>IEEE 802.1X™ Authentication</li> </ul>	<b>AUDIT TRAIL SECURITY</b> <ul style="list-style-type: none"> <li>Job Log and Usage Tracking</li> <li>Reporting and Data Export</li> <li>Administrator System Audit Logs</li> <li>Program Partner Applications</li> <li>SRDM Security Policy Management</li> </ul>
	<b>EMAIL SECURITY</b> <ul style="list-style-type: none"> <li>User Authentication</li> <li>S/MIME</li> <li>Send Only to Logged in User's Email Address</li> <li>Send Item Logged in User (Email Connect)</li> <li>Store Sent Email on Send Item Folder</li> <li>Apply Exchange Email Rules to Send to Email</li> <li>Single-Sign-On (SSO) (Kerberos and OAuth token)</li> </ul>	<b>DOCUMENT SECURITY</b> <ul style="list-style-type: none"> <li>Secure Print Release with a PIN Number</li> <li>Encrypted PDF (AES 256 bit Encryption)</li> <li>Encrypted PDF Lockout</li> <li>Tracking Information Print</li> <li>Hidden Pattern Print and Detection</li> </ul>
		<b>MOBILE AND WIFI SECURITY</b> <p>Control mobile printing and scanning by eliminating unauthorized access to corporate assets.</p> <ul style="list-style-type: none"> <li>User Authentication</li> <li>Print Retention</li> <li>PIN Number Printing</li> <li>Access Point WiFi Mode</li> </ul>

10

## Hacking Printers is Not

[hacking-printers.net](http://hacking-printers.net)

This is the **Hacking Printers Wiki**, an open approach to share knowledge on printer (in)security.

### Attacks

- Denial of service:
  - Transmission channel
  - Document processing
  - Physical damage
- Privilege escalation:
  - Factory defaults
  - Accounting bypass
  - Fax and Scanner
- Print job access:
  - Print job retention
  - Print job manipulation
- Information disclosure:
  - Memory access
  - File system access
  - Credential disclosure
- Code execution:
  - Buffer overflows
  - Firmware updates
  - Software packages

### TLS/DR

Check out the Printer Security Testing Cheat Sheet

### Tools

- PRET, Pweds, PPT, BEEP

### Fundamentals

- Printer languages
- PCL, PCL, PostScript
- Network protocols
- LPD, IPP, Raw, SMB

### Attack Carriers

- USB drive or cable
- Port 9100 printing
- Cross-site printing

### Countermeasures

- Vendors, Admins, Users

### Bibliography

- Literature on printer security

### References

- Printer language references

11

## Advanced Controls

Organization Specific Innovative Controls

### Advanced Breach & Endpoint Controls

- OCR Breach Monitoring (detect/respond)
- SIEM Integration (detect/respond)
- Secure Faxing Solutions (protect)
- Workflow Automation (risk reduction)

12

## Industry Updates

How is the industry responding

Manufacturers and resellers are responding:

- Hardware Improvements
- Professional Services
- Configuration Management Solutions

13

## Solution Architecting

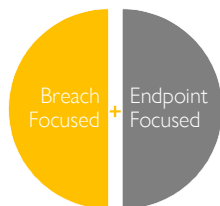
Solutioning Realities:

- No Silver Bullets
- No Single Software
- Not Always Single Manufacturer

Every environment is unique

14

## Control Planning

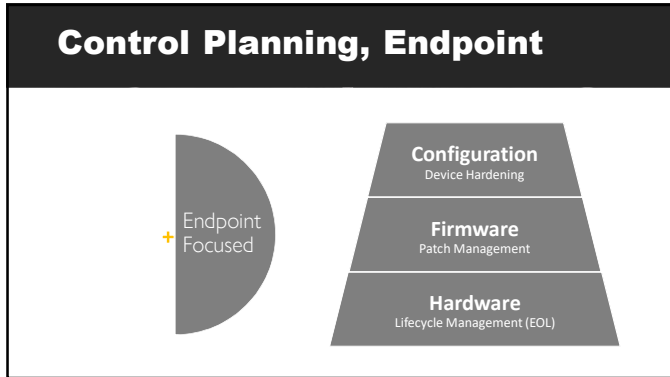


15

## Control Planning, Breach



16



17



18



19