Technical White Paper

Printer Security considerations

Important security aspects to consider when assessing print solutions

Table of contents

Non-secured printing and imaging devices is the status quo

IT is continually tasked with protecting confidential information, including employee identities and customer data, across multiple devices. This need to service a range of people with different work styles across the organization makes unanticipated IT security threats a constant challenge.

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. The security threats are real, however, and as printing and imaging devices become increasingly sophisticated, they offer greater opportunities for attackers to compromise the device or the entire network.

Five Key Areas of Printer Security

The purpose of this document is to provide you with not only a framework, but also very specific aspects of printing security that you should consider when purchasing, deploying, or using printers and print solutions. HP Printers that support the "Big 3" security features (HP Sure Start, White Listing, and Run-Time Intrusion Detection) launched in fall 2015 will meet all of the criteria in each of the sections (when paired with JetAdvantage Security Manger and ArcSight).[1] The FutureSmart devices that do not support HP Sure Start will meet all of the criteria except those listed in section #1 (Secure Boot Process). See device table below for security feature support details.

You should focus on five key areas of printer security:

1. Secure Boot Process
2. Firmware Code Integrity
3. Run-Time Intrusion Detection
4. Continuous Assurance of Security Policy Settings
5. Real-Time Threat Detection and Analytics

Secure Boot Process

The following items are aspects of a Secure Boot Process that HP recommends for maximum security:

- At startup, the device must validate the integrity of the BIOS.
- The device must "self-heal" an infected BIOS by replacing it with a hardware protected golden copy of the BIOS.
- The device must notify the administrator via standard event mechanisms, including SIEM systems, of any issues.
- The device must recover to a known good state after detecting an infected BIOS and replacing it with the golden copy.

Firmware Code Integrity

The following items are aspects of Firmware Code Integrity that HP recommends for maximum security:

- The device must validate the integrity of firmware code at load time and allow only known good firmware to execute.
- The device must notify the administrator via standard event mechanisms, including SIEM systems, of any issues.

Run-Time Intrusion Detection

The following items are aspects of Run-Time Intrusion Detection that HP recommends for maximum security:

- The device must provide continuous monitoring for in-memory malware injection attacks.
- The device must notify the administrator via standard event mechanisms, including SIEM systems, of any issues.
- The device must halt normal operation when an anomaly is detected and reboot to a known good condition.
- The intrusion detection algorithm must be randomly inserted into different places in the code image to prevent against its own detection.

The intrusion detection algorithm must execute frequently enough to detect malware injections before the malware can compromise the integrity of the device.

Continuous Assurance of Security Policy Settings

Continuous Assurance of Security Policy Settings is largely done through the use of a security compliance tool. The following items are aspects of a security compliance tool that HP recommends for maximum security:

- The security compliance tool must bring Printers/MFPs that are out of compliance into compliance, based on the Security Policy.
- The security compliance tool must have new or reset devices on the network announce themselves and immediately be brought into compliance.
- The security compliance tool must include an Intuitive Security Policy editor that guides the administrator through making appropriate policy settings by highlighting conflicting dependencies.
- The security compliance tool must manage and install certificates with an automated process across a fleet of Printers/MFPs.

Real-Time Threat Detection and Analytics

Real-Time Threat Detection and Analytics is largely done through the use of a Security Information Event Management (SIEM) system. The following items are aspects of a SIEM system that HP recommends for maximum security:

- The SIEM must retrieve critical security events from printers.
- The SIEM must allow the Security Analyst to customize reports and alerts from messages indicating real-time threats.
- The SIEM must integrate with other Networked IT assets (servers, routers, etc.) being monitored for real-time threat detection.
- The SIEM must transform Big Data into actionable security intelligence by using real-time correlation combined with powerful security analytics.
- The SIEM must spot abnormal user behavior and prevent threats to sensitive data.

Supported FutureSmart devices and feature availability

The following matrix shows how the new embedded security features will be supported across the HP Enterprise FutureSmart Fleet starting in late fall '15. All new FutureSmart devices introducing after fall '15 will support the 3 new embedded security features moving forward. (HP Sure Start, Whitelisting and Intrusion Detection). Due to device hardware limitations some features will not be supported on certain older platforms.

RFP Category		**Secure Boot Process**	**Firmware Code Integrity**	**Run-Time Intrusion Detection**	**Continuous Assurance of Security Policy Settings**	**Real-Time Threat Detection and Analytics**
Device Platform (includes all bundles and Managed options)	New Embedded Security Feature Availability	HP Sure Start	Whitelisting	Run-Time Intrusion Detection	HP JetAdvantage Security Manager	HP ArcSight Integration
HP LaserJet Enterprise MFP M527	Fall '15	✓	✓	✓	✓	✓
HP Color LaserJet Enterprise M577	Fall '15	✓	✓	✓	✓	✓
HP LaserJet Enterprise M506	Fall '15	✓	✓	✓	✓	✓
HP Color LaserJet Enterprise M552 and M553	Fall '15	✓	✓	✓	✓	✓
HP LaserJet Enterprise M604, M605, and M606	Fall '15	✓	✓	✓	✓	✓
HP LaserJet Enterprise 700 color MFP M775	Spring '16	⊘	✓	✓	✓	✓
HP LaserJet Enterprise 500 color MFP M575	Spring '16	⊘	✓	✓	✓	✓
HP LaserJet Enterprise 500 MFP M525	Spring '16	⊘	✓	✓	✓	✓
HP LaserJet Enterprise MFP M725	Spring '16	⊘	✓	✓	✓	✓
HP LaserJet Enterprise flow MFP M830	Spring '16	⊘	✓	✓	✓	✓
HP LaserJet Enterprise M806	Spring '16	⊘	✓	✓	✓	✓
HP Color LaserJet Enterprise M855	Spring '16	⊘	✓	✓	✓	✓
HP Color LaserJet Enterprise flow MFP M880	Spring '16	⊘	✓	✓	✓	✓
HP OfficeJet Enterprise Color MFP X585	Spring '16	⊘	✓	✓	✓	✓
HP OfficeJet Enterprise Color X555	Spring '16	⊘	✓	✓	✓	✓

RFP Category		Secure Boot Process	Firmware Code Integrity	Run-Time Intrusion Detection	Continuous Assurance of Security Policy Settings	Real-Time Threat Detection and Analytics
Device Platform (includes all bundles and Managed options)	New Embedded Security Feature Availability	HP Sure Start	Whitelisting	Run-Time Intrusion Detection	HP JetAdvantage Security Manager	HP ArcSight Integration
HP Color LaserJet Enterprise M651	Spring '16	⊘	✓	✓	✓	✓
HP Color LaserJet Enterprise MFP M680	Spring '16	⊘	✓	✓	✓	✓
HP LaserJet Enterprise MFP M630	Spring '16	⊘	✓	✓	✓	✓
HP LaserJet Enterprise 700 M712	Spring '16	⊘	✓	✓	✓	✓
HP Color LaserJet Enterprise M750	Spring '16	⊘	✓	✓	✓	✓
HP LaserJet Enterprise 600 M601, M602 and M603	Spring '16	⊘	✓	✓	✓	✓
HP LaserJet Enterprise color M551	Spring '16	⊘	✓	✓	✓	✓
HP LaserJet Enterprise M4555 MFP	Not Supported	⊘	⊘	⊘	✓	✓
HP Color LaserJet CM4540 MFP	Not Supported	⊘	⊘	⊘	✓	✓
HP LaserJet Enterprise CP5525	Not Supported	⊘	⊘	⊘	✓	✓
HP Digital Sender Flow 8500 fn1	Not Supported	⊘	⊘	⊘	✓	✓
HP Scanjet Enterprise 7000n	Not Supported	⊘	⊘	⊘	✓	⊘

[1] A FutureSmart service pack update may be required to activate security features.

Sign up for updates
hp.com/go/getupdated

Share with colleagues

Rate this document

4AA6-3571ENW, December 2015