Technical white paper

Embedded printer security considerations

Important security aspects to consider when assessing printers

Table of contents

Printing and imaging device security is often overlooked

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. As printing and imaging devices become increasingly sophisticated and interconnected with more mobile and endpoint devices, printers become a potential attack vector for hackers to compromise the device or the entire network.

Six key areas of printer security

The purpose of this document is to provide 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 FutureSmart printers that support the "Big 4" security features (HP Sure Start, whitelisting, run-time intrusion detection, and HP Connection Inspector) meet all the criteria in each of the sections (when paired with HP JetAdvantage Security Manager and a Security Information Event Management (SIEM) tool such as ArcSight, Splunk, SIEMonster, or McAfee).[1] FutureSmart devices that do not support HP Sure Start will meet all the criteria except those listed in "Secure boot process." See device table on pages 4-5 for security feature support details.

You should focus on six key areas of printer security:

1. Secure boot process
2. Firmware code integrity
3. Run-time intrusion detection
4. Network behavior anomaly detection
5. Continuous assurance of security policy settings
6. Real-time threat detection and analytics

Secure boot process

The following items are aspects of a secure boot process that HP recommends for optimal 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 of any issues via standard event mechanisms, including SIEM systems.
- 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 optimal 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 of any issues via standard event mechanisms, including SIEM systems.

Run-time intrusion detection

The following items are aspects of run-time intrusion detection that HP recommends for optimal security:

- The device must provide continuous monitoring for in-memory malware injection attacks.
- The device must notify the administrator of any issues via standard event mechanisms, including SIEM systems.
- 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.

Network behavior anomaly detection

The following items are aspects of network behavior anomaly detection that HP recommends for optimal security:

- The device must provide continuous monitoring for network behavior anomalies.
- The device must notify the administrator of any issues via standard event mechanisms, including SIEM systems.
- The device must halt normal operation when an anomaly is detected and reboot to a known good condition.

Continuous assurance of security policy settings

Continuous assurance of security policy settings is largely done using a security compliance tool. The following items are aspects of a security compliance tool that HP recommends for optimal 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 require new or reset devices on the network to announce themselves and immediately be brought into compliance.
- The security compliance tool must include a 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 using a SIEM system. The following items are aspects of a SIEM system that HP recommends for optimal 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 embedded security features are supported across the HP Enterprise FutureSmart fleet. All new FutureSmart devices introduced after fall '15 support the four embedded security features. (HP Sure Start, whitelisting, run-time intrusion detection, and HP Connection Inspector). With the investment protection that HP FutureSmart firmware provides, you can add some features to many existing HP Enterprise printer models. (Due to device hardware limitations, HP Sure Start is not supported on certain older platforms.)

RFP category	Continuous assurance of security policy settings HP Security Manager	Real-time threat detection and analytics Integration with SIEM tools	Firmware code integrity Whitelisting	Run-time intrusion detection Run-time intrusion detection	Network behavior anomaly detection HP Connection Inspector	Secure boot process HP Sure Start BIOS protection
MFP devices						
HP LaserJet Enterprise 500 MFP M525 series	✓	✓	✓	✓	✓	⊘
HP LaserJet Enterprise MFP M527 series	✓	✓	✓	✓	✓	✓
HP LaserJet Enterprise 500 color MFP M575 series	✓	✓	✓	✓	✓	⊘
HP Color LaserJet Enterprise MFP M577 series	✓	✓	✓	✓	✓	✓
HP LaserJet Enterprise MFP M630 series	✓	✓	✓	✓	✓	⊘
HP LaserJet Enterprise MFP M631, M632, M633 series	✓	✓	✓	✓	✓	✓
HP Color LaserJet Enterprise M652, M653 series	✓	✓	✓	✓	✓	✓
HP Color LaserJet Enterprise MFP M680 series	✓	✓	✓	✓	✓	⊘
HP Color LaserJet Enterprise Flow MFP M681-M682 series	✓	✓	✓	✓	✓	✓
HP LaserJet Managed MFP E62550-E62560-E62570 series	✓	✓	✓	✓	✓	✓
HP Color LaserJet Managed MFP E67550-E67560 series	✓	✓	✓	✓	✓	✓
HP LaserJet Enterprise MFP M725	✓	✓	✓	✓	✓	⊘
HP LaserJet Enterprise 700 color MFP M775 series	✓	✓	✓	✓	✓	⊘
HP LaserJet Enterprise Flow MFP M830z	✓	✓	✓	✓	✓	⊘
HP Color LaserJet Enterprise Flow MFP M880z	✓	✓	✓	✓	✓	⊘
HP PageWide Enterprise Color MFP M586 series	✓	✓	✓	✓	✓	✓
HP PageWide Enterprise Color MFP 780, 785 series	✓	✓	✓	✓	✓	✓
HP PageWide Managed Color MFP P77440dn	✓	✓	✓	✓	✓	✓
HP PageWide Managed Color MFP P77940-P77950-P77960 series	✓	✓	✓	✓	✓	✓
HP PageWide Managed Color MFP E77650-E77660 series	✓	✓	✓	✓	✓	✓
HP LaserJet Managed MFP E72520-E72540 series	✓	✓	✓	✓	✓	✓
HP Color LaserJet Managed MFP E77820-E77830 series	✓	✓	✓	✓	✓	✓
HP LaserJet Managed MFP E82540-E82560 series	✓	✓	✓	✓	✓	✓
HP Color LaserJet Managed MFP E87640-E87660 series	✓	✓	✓	✓	✓	✓

RFP category	Continuous assurance of security policy settings HP Security Manager	Real-time threat detection and analytics Integration with SIEM tools	Firmware code integrity Whitelisting	Run-time intrusion detection Run-time intrusion detection	Network behavior anomaly detection HP Connection Inspector	Secure boot process HP Sure Start BIOS protection
Single function devices						
HP LaserJet Enterprise M506 series	✓	✓	✓	✓	✓	✓
HP LaserJet Enterprise 500 Color Printer M551 series	✓	✓	✓	✓	✓	⊘
HP Color LaserJet Enterprise 500 M552dn	✓	✓	✓	✓	✓	✓
HP Color LaserJet Enterprise M553 series	✓	✓	✓	✓	✓	✓
HP LaserJet Enterprise 600 Printer M601, M602, M603 series	✓	✓	✓	✓	✓	⊘
HP LaserJet Enterprise M604, M605, M606 series	✓	✓	✓	✓	✓	✓
HP LaserJet Enterprise M607, M608, M609 series	✓	✓	✓	✓	✓	✓
HP Color LaserJet Enterprise M651 series	✓	✓	✓	✓	✓	⊘
HP LaserJet Managed E60055-E60065-E60075 series	✓	✓	✓	✓	✓	✓
HP Color LaserJet Managed E65050-E65060 series	✓	✓	✓	✓	✓	✓
HP LaserJet Enterprise 700 Printer M712 series	✓	✓	✓	✓	✓	⊘
HP Color LaserJet Enterprise M750 Printer series	✓	✓	✓	✓	✓	⊘
HP LaserJet Enterprise M806 Printer series	✓	✓	✓	✓	✓	⊘
HP Color LaserJet Enterprise M855 series	✓	✓	✓	✓	✓	⊘
HP OfficeJet Enterprise Color X555 series	✓	✓	✓	✓	✓	⊘
HP PageWide Enterprise Color 556 series	✓	✓	✓	✓	✓	✓
HP PageWide Enterprise Color 765dn	✓	✓	✓	✓	✓	✓
HP PageWide Managed Color P75250dn	✓	✓	✓	✓	✓	✓
HP PageWide Managed Color E75160dn	✓	✓	✓	✓	✓	✓
HP Officejet Enterprise Color X585 series	✓	✓	✓	✓	✓	⊘
Scanner devices						
HP Digital Sender Flow 8500 fn2	✓	✓	✓	✓	✓	✓
HP ScanJet Enterprise Flow N9120 fn2	✓	✓	✓	✓	✓	✓

Learn more

hp.com/printersthatprotect

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

Sign up for updates

hp.com/go/getupdated

Share with colleagues

4AA6-3571ENW, March 2018, Rev. 1