Technical white paper

HP JetAdvantage Apps

Security features of the app development ecosystem for HP MFPs

Table of contents

Executive summary

While network security is a priority for IT and leaders, many organisations neglect security of endpoints on the network, such as printers and MFPs. HP offers the most secure printers,[1] and that focus on security extends to the apps that run on HP printers. These apps are called HP JetAdvantage Apps, and are developed through the HP JetAdvantage Link for Device ecosystem.

This paper discusses the security features of the HP JetAdvantage Link for Device ecosystem in three areas of focus:

- Device ecosystem security
- App validation and verification
- App monitoring and revocation

The first intended audience for this document is app developers or resellers who need a deeper understanding of the security measures that protect HP JetAdvantage Apps and the print devices they run on. The second audience includes those making printer purchasing decisions who need to ensure their data, documents, and print devices are protected.

Glossary

Term	Description	Function
Active App Monitoring	Verifies whitelisting is current[2]	Active App Monitoring and Revocation
App Whitelist Revocation	Revokes whitelisting and prevents app launch	Active App Monitoring and Revocation
Ongoing Security Screening	Apps are continually re-screened to guard against newly discovered security threats	Active App Monitoring and Revocation
App Integrity Checking	Validates apps' digital signature and files during installation	App Validation and Verification
App Whitelisting	Only whitelisted apps can be installed on HP devices	App Validation and Verification
Security Screening and Signing	Apps are reviewed and signed by the HP Global Cyber Security team	App Validation and Verification
Connection Inspector	Detects suspicious network communications	Device Ecosystem Security
Downloaded Executable Protection	Blocks executable code from being downloaded after installation	Device Ecosystem Security
Firmware Whitelisting	Validates integrity of firmware system files	Device Ecosystem Security
Link Debug Bridge Auditing	Creates audit logs for the Link Debug Bridge (used for testing and debugging apps)	Device Ecosystem Security
Loopback Protection	Blocks loopback connections	Device Ecosystem Security
Ecosystem Enablement/Disablement	Sets ecosystem to **Disabled** as default	Device Ecosystem Security
Runtime Intrusion Detection	Validates firmware while printer is running	Device Ecosystem Security
Secure Boot	Scans for unexpected modifications when device is powered on	Device Ecosystem Security
Secure Kernel	Controls access to system resources	Device Ecosystem Security

HP JetAdvantage Link for Device ecosystem overview

The HP JetAdvantage Link for Device ecosystem allows independent developers to create apps for use in HP print devices. With more than 1.8M HP printers and MFPs[3] in service, it is the world's largest install base of office printing technology.[4] Embedding apps into a print device can offer organisations the ability to send scanned documents directly from the MFP to a cloud-based repository, integrate customer documentation into a digital recordkeeping system, process mobile payments through the MFP, and more.

The development ecosystem offers open, industry-standard APIs, robust forum support, as well as remote testing, deployment, and management of apps. Administration can be handled through the device, or through a cloud-based interface that includes app security validation.

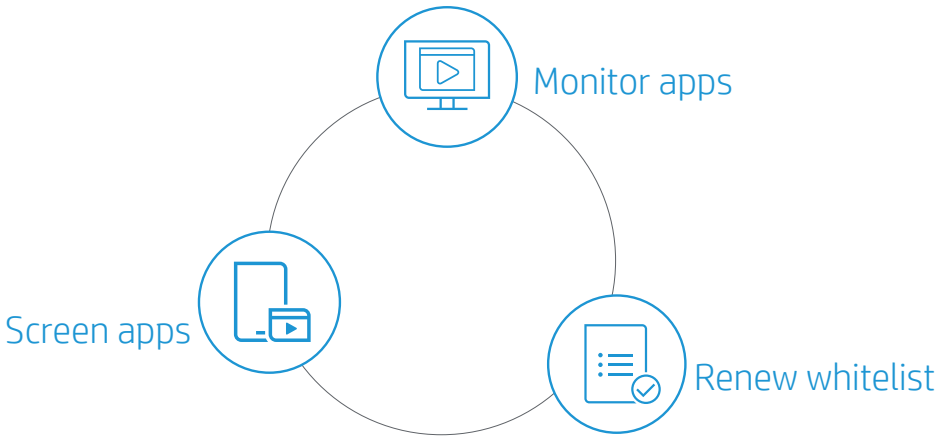
Apps must undergo HP's stringent validation and verification (VAV) process to provide that they are safe for use, before they can be offered in the app catalogue. Even after installation, apps can be actively monitored, and problems remediated.[5] The open app library makes it easy for organisations to find and deploy their chosen apps.

The development ecosystem itself is also protected by strong security features to guard the devices and any network communications that involve apps.

Security features and processes

Security is managed across three aspects: Active App Monitoring and Revocation, App VAV, and Device ecosystem security. These security measures support HP's mission of offering the world's most secure printers.[1] Along with app-specific security measures, HP JetAdvantage Apps are also protected by HP Sure Start, which responds to any potential compromise of the BIOS by restarting with a safe "golden copy" of its BIOS.

Active App Monitoring and Revocation[5]



Active App Monitoring

Devices must remain connected to HP's cloud-based security web services, which monitors app installations and renews every installed app's whitelisted status on the device regularly. If the whitelisted status of an installed app has not been renewed for more than 14 days, the device will display a clearable warning (This app will be disabled in X days.) each time that the app is launched, but the app will be allowed to launch. If the whitelisted status of an installed app has not been renewed for more than 30 days, the device will display an error (This app has been disabled.) each time the app is launched, and the app will not be allowed to launch. These warnings and errors can be avoided by keeping the device constantly connected to HP's cloud-based security web services.

App Whitelist Revocation

In extreme cases, an app may be removed from the whitelist at HP's sole discretion. When an app is removed from the whitelist, HP security web services will automatically revoke the app's whitelisted status on all connected devices. Once revoked, the device will display an error each time an app attempts to launch and the app will not be allowed to launch. Its revoked whitelist status will also be displayed in the App Gallery. If a device has been disconnected from HP security web services, the warning/error sequence will ultimately result in the app being disabled within 30 days or less.

Ongoing Security Screening

Because new security vulnerabilities are discovered as time passes, HP's Global Cyber Security team is constantly updating its test suite to screen for those new vulnerabilities. As the test suite changes, all HP JetAdvantage Apps are re-screened. If a major threat is discovered in a whitelisted app, the app developer will be notified, and is expected to publish a fixed version in a reasonable amount of time. In extreme cases, an app may be removed from the whitelist at HP's sole discretion.

App Validation and Verification

App Integrity Checking

The device validates the digital signature and the integrity of app files during the installation, except when loaded through the Link Debug Bridge (LDB) for testing on a device set to developer mode. In this setting the device cannot have any live whitelisted apps installed.

App Whitelisting

All apps that pass VAV are added to a cloud-based whitelist. All tools that support app installation (including HP App Manager and HP App Gallery) must utilise the HP JetAdvantage Management (JAM) cloud APIs to install apps.

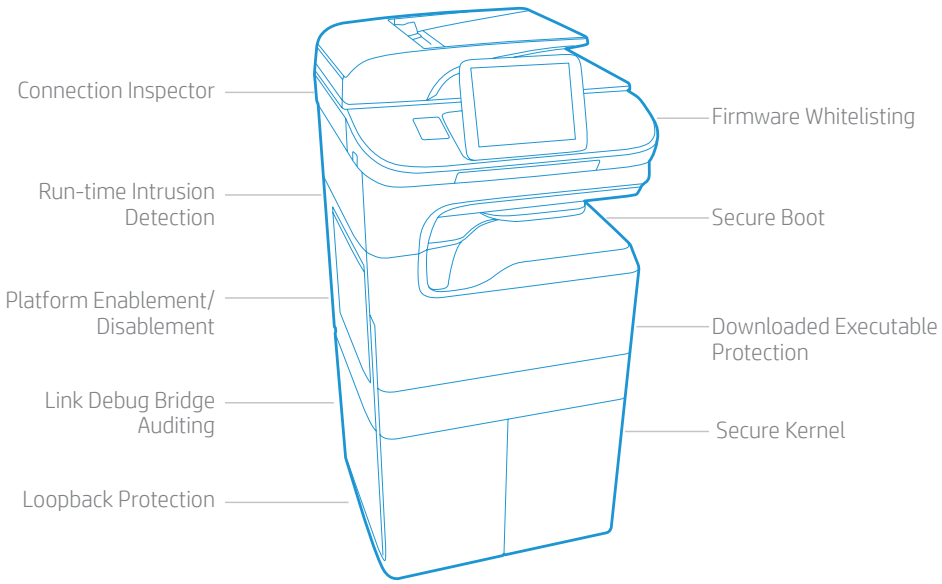
Every app's whitelisted status is verified before allowing installation onto an HP device, except when loaded through the LDB for testing.

Security Screening and Signing

All apps are screened by HP's in-house Global Cyber Security team for known security vulnerabilities. Only apps that have passed these VAV tests, and have subsequently been signed by HP using an SHA-256 HP digital signature, will be offered for installation onto HP devices, except when loaded through the LDB for testing. The VAV security review includes, but is not limited to:

- Threat surface analysis, including new features and products
- Static and dynamic code scanning tools, such as Fortify, WebInspect, and/or Coverity
- Penetration testing by industry-leading vulnerability assessment scanners, such as Qualys and/or Nessus by Tenable
- Adherence to Open Web Application Security Project (OWASP) secure coding practices
- Amazon Web Services (AWS) servers located in the U.S., the U.K., and Germany

Device ecosystem security



Connection Inspector

Unique HP technology is used to inspect outgoing network connections to stop malware from "calling home" to malicious servers, stealing data, and compromising the network. (Enterprise printers only). Network activity is monitored for suspicious activity. Unfamiliar or distrusted requests are halted, and a warning is sent to IT administrators.

Downloaded Executable Protection

Link for Device apps are not allowed to download executable code after installation.

Firmware Whitelisting

Firmware whitelisting validates the integrity of firmware system files (including the Link for Device system files) during the load process using an SHA-256 hash signed with HP's digital signature. If validation fails, the device reboots and holds at the pre-boot menu to prevent a potential malware exploitation from executing.

Link Debug Bridge Auditing

The LDB facility allows app developers to install, test, and debug their unverified app code on HP devices. It can only be enabled by registered app developers with device administrator authority. The developer's identity is verified with the HP cloud-based security web services. LDB audit logs include the device serial number, model number, and firmware version.

When LDB is enabled, a warning is displayed in the Message Centre on the device's front panel, alerting users to this potential security issue. HP JetAdvantage Security Manager[6] can also detect devices where LDB is enabled, and alert customers to this potential security issue.

When LDB is disabled, all installed apps are automatically removed.

Loopback Protection

HP JetAdvantage Apps are not able to bypass network security by making network requests over loopback connections.

Ecosystem Enablement/Disablement

The Link for Device ecosystem is disabled by default and can only be enabled by an authorised device administrator.

Run-time Intrusion Detection

Run-time intrusion detection detects potential malware intrusions in system memory by running in the background to validate the memory space, then rebooting the device if a possible intrusion is detected. If the Auto-recover feature is disabled, or a possible intrusion occurs twice within 30 minutes, the device reboots and holds at the pre-boot menu to prevent a potential malware exploitation from executing. The device will attempt to wait until in-process print jobs have been cancelled, before rebooting.

Secure Boot

Each time the device is powered on, the Link for Device kernel is scanned for unexpected modifications. In addition, the root and system mass storage partitions are verified using device-mapper-verity (dm-verity). The boot sequence will be stopped if any unexpected modifications are found.

Secure Kernel

The Link for Device ecosystem uses the most secure kernel available.

Learn more

For more information, contact your HP representative or reseller.

For information about compatibility, refer to the HP JetAdvantage Apps Compatibility Matrix.

[1] HP's most advanced embedded security features are available on HP Enterprise-class devices with FutureSmart firmware 4.5 or above and is based on HP review of 2018 published embedded security features of competitive in-class printers. Only HP offers a combination of security features for integrity checking down to the BIOS with self-healing capabilities. For a list of compatible products, visit: hp.com/go/PrintersThatProtect. For more information, visit: hp.com/go/printersecurityclaims.

[2] Devices must remain connected to HP's cloud-based security web services to use this feature.

[3] Expected number of compatible HP devices by end of 2019 based on internal HP projections.

[4] Based upon HP internal analysis of units shipped and still active.

[5] Currently only available for HP JetAdvantage Link for Device apps.

[6] HP JetAdvantage Security Manager must be purchased separately. To learn more, please visit hp.com/go/securitymanager.

4AA7-4239EEW, April 2019