Security and Manageability White Paper

HP Enterprise-Ready Android Devices

January 2015

Table of contents

Executive summary

One of the most popular mobile device operating system (OS) platforms, Android is equipped with a number of security measures to protect users from modern-day threats and exploits. Yet many security decisions are left up to individual hardware vendors, leaving Android devices open to critical gaps and weaknesses if security isn't fully prioritized.

HP Enterprise-Ready Android devices help IT personnel overcome these key challenges when deploying, securing, and managing Android devices in a business environment. The comprehensive HP Enterprise-Ready Android security approach extends from product design and manufacturing to updating devices in the field. HP reinforces device security by leveraging hardware, firmware, and cloud capabilities without fragmenting Android application programming interfaces (APIs) or breaking compatibility with Android applications and enterprise mobility management (EMM) solutions.

This white paper provides an overview of HP Enterprise-Ready Android security and manageability features that include:

- Hardware-reinforced root of trust, encryption, and boot-loader functions
- Secure key-store function that prevents unauthorized access to the cryptographic keys used by device encryption and apps
- Security hardening that minimizes damage from specific types of threats
- Anti-theft protection that allows IT personnel to locate, lock, and wipe a lost or stolen device
- Out-of-the-box manageability with HP Touchpoint Manager[1], giving organizations a single solution for managing their users, data, and Android devices

Audience

IT managers and system administrators seeking to understand the security and manageability features of HP Enterprise-Ready Android devices. This audience should already be familiar with the following topics:

- Mobile devices
- Mobile security
- Mobile device management
- Android operating system

Applicable products

Features covered in this document apply to the following 2015-16 products:

- HP Pro Slate 8 Tablet
- HP Pro Slate 12 Tablet

Disclaimers

Some details provided in this document may vary depending on the system-on-chip (SoC) semiconductor package used in a particular device model. Future Enterprise-Ready Android devices will featured in additional white papers or updates to this white paper.

[1] HP Touchpoint Manager supports Android, iOS, and Windows operating systems, and PCs, notebooks, tablets, and smartphones from various manufacturers. Not available in all countries. Subscription plan is required.
Visit hp.com/touchpoint for availability information, pricing, and system requirements.

Glossary of acronyms and terms

AD	Microsoft Active Directory
AES	Advanced Encryption System See http://csrc.nist.gov/publications/fips/fips197/fips-197.pdf
ARM	Advanced RISC Machines—refers to the microprocessor architecture used in HP Enterprise-Ready Android devices See http://www.arm.com/products/processors
BYOD	Bring your own device
CBC	Cipher-block chaining. See CBC-AES
CBC-AES	Cipher-block chaining—an AES mode of operation See http://csrc.nist.gov/publications/nistpubs/800-38a/sp800-38a.pdf
DDR-SDRAM	Double data rate synchronous dynamic random-access memory
DPM	Android Device Policy Manager See http://developer.android.com/reference/android/app/admin/DevicePolicyManager.html
EAS	Exchange ActiveSync—refers to the Microsoft protocol for synchronizing mail, contacts, calendar, and tasks between mobile clients and Microsoft Exchange servers
EMM	Enterprise mobility management—refers to the servers used to secure and manage mobile access to enterprise applications and data. Includes MDM, MAM, MCM, and more.
FIPS	Federal Information Processing Standard See http://www.nist.gov/itl/fipsinfo.cfm
HMAC	Hash message authentication code —a mechanism for message authentication using cryptographic hash functions. See http://tools.ietf.org/html/rfc2104
MAC	Message authentication code Also, see HMAC
MAM	Mobile application management
MCM	Mobile content management
MDM	Mobile device management
NIST	National Institute of Standards and Technology See http://nist.gov
OEM	Original equipment manufacturer—refers to device manufacturers
PBL	Primary Boot Loader—refers to the first code that runs when a processor powers up. This code initializes the primary processor and loads processor specific secondary boot loaders (SBL).
PKI	Public key infrastructure —supports the distribution of public encryption keys, enabling users and computers to exchange data securely and verify identities. See http://en.wikipedia.org/wiki/Public_key_infrastructure
ROM	Read-only memory
RSA	Refers to a public-key cryptosystem that is widely used to protect data exchanges between two computers See http://en.wikipedia.org/wiki/RSA_(cryptosystem)
SBL	Secondary Boot Loader—performs processor-specific initialization
SHA	Secure hash algorithms See http://csrc.nist.gov/groups/STM/cavp/documents/shs/sha256-384-512.pdf
SoC	System on chip—refers to a semiconductor package that includes the CPU, ROM, and other processors and components
TEE	Trusted execution environment—refers to the trusted environment created using ARM TrustZone to run trusted applications
TZ	TrustZone—refers to the ARM TrustZone technology
VPN	Virtual Private Network
AES-XTS	Cipher text stealing—an AES mode of operation See http://csrc.nist.gov/publications/nistpubs/800-38E/nist-sp-800-38E.pdf

Introduction

Securing Android

One of the most popular mobile device operating system (OS) platforms, Android™ is designed to protect users from modern-day threats and exploits. Its key security capabilities and benefits include:[2]

- Leveraging OS-level security measures built on the battle-hardened Linux® kernel
- Providing kernel-level security reinforced by security-enhanced (SE) Linux capabilities
- Minimizing damage from malware and misbehaving apps by isolating applications to sandboxes
- Securing applications from unauthorized changes and allowing applications to collaborate securely by using cryptographic signatures
- Protecting system resources by limiting application privileges to a minimum required level and securing inter-process communications
- Giving users visibility and control over what an app can do by employing a user-granted permission model
- Enabling additional, hardware-specific security features such as ARM eXecute-Never and hard ware-backed key stores

Because Android powers all types of devices—large and small, expensive and inexpensive—many decisions that affect device security are left up to the hardware vendor. Even though some security features are inherent in the Android OS itself, many of these features can be compromised if the hardware vendor does not do additional work to secure the system. In a typical scenario, the SoC vendor takes the source code from the Android Open Source Project and ports to the SoC. Some SoCs support hardware-level security features such as TrustZone, hardware root of trust, and tamper-proof hardware cryptographic modules; others may not support any of these. Device manufacturers perform critical functions such as enabling secure boot, integrating with TrustZone and the hardware cryptographic modules, signing the system images, securing the platform keys, performing ongoing security patching, and much more. The process may leave behind critical gaps and weaknesses. For example:

- When the secure boot is not implemented or is implemented incorrectly, an unsuspecting user's device software image can be altered to harvest user credentials and sensitive data.
- When the platform key is not well secured in the manufacturing process, it may end up in the hands of cyber criminals. With the platform key, a malware maker can gain root privileges and unrestricted access to user data, application credentials, and much more. This can result in leaks of critical private customer information, trade secrets, or other information—harming the company and its customers.
- When a software-based device encryption is used, a sophisticated attacker can dump the device RAM to retrieve the encryption key and decrypt the data.
- When a new security vulnerability is discovered, the device vendors have the responsibility to rapidly patch the device firmware and fix the vulnerability. Not many device vendors have the capability and the resources required to promptly patch. When not patched, devices serve as easy targets for exploitation of known weaknesses.

The HP approach

HP Enterprise-Ready Android devices are designed to address key pain points in deploying, securing, and managing Android devices for businesses. HP reinforces security by leveraging hardware, firmware, and cloud capabilities without fragmenting Android application programming interfaces (APIs) or breaking compatibility with Android applications and enterprise mobility management (EMM) solutions. This approach delivers enterprise-class security without creating dependency on a single vendor.

In addition, the HP Touchpoint Manager app provides a single, cloud-based solution for managing an organization's users, data, and Android devices—as well as devices running on Microsoft® Windows® or iOS platforms—from an easy-to-use dashboard. With HP Touchpoint Manager, IT personnel can access management, security, and user-support tools from virtually anywhere to solve issues in real time—improving IT effectiveness and employee productivity. IT managers and end users alike can use the agent-based wizard to easily enroll devices running on Microsoft® Windows®, Android™, and iOS platforms.

[2] For additional details on Android security, please see https://source.android.com/devices/tech/security.

Key pillars of secure HP Enterprise-Ready Android devices include:

Trusted hardware. The SoCs provide hardware-reinforced root of trust, encryption, and boot-loader functions that play a foundational role in securing the device. HP Enterprise-Ready Android devices are built on proven SoC platforms with robust security features from trusted vendors, including Qualcomm and Intel, that have established processes to secure the platforms from design through production. Further, for devices using ARM-based processors, HP Enterprise-Ready Android devices employ ARM TrustZone technology to provide a trusted execution environment (TEE) for implementing sensitive security functions such as securing the encryption keys and key-store keys.

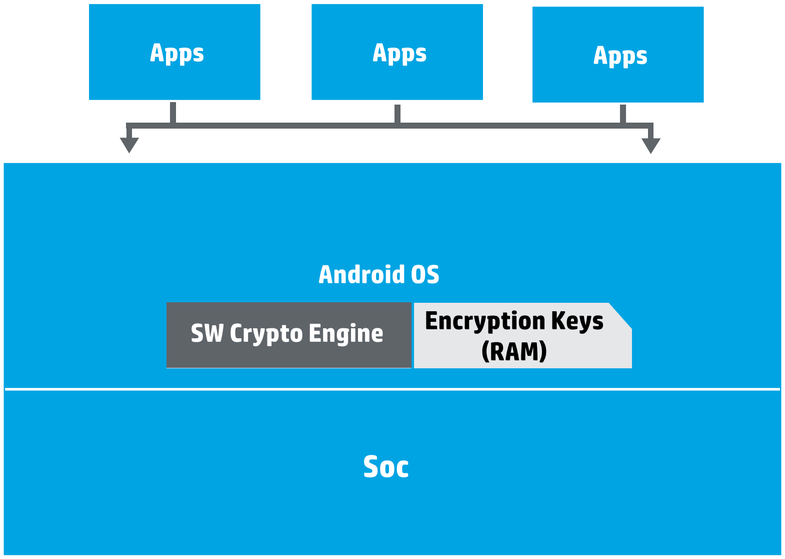
Trusted firmware. Only firmware images authorized by HP can run on Enterprise-Ready Android devices, protecting the user from harm arising from unauthorized or untrusted firmware.

Continuous hardening. In a continuously evolving threat landscape, products must also evolve to withstand new vulnerabilities and attacks. HP Enterprise-Ready Android devices undergo additional security hardening through a set of security-enhanced Android policies, and HP regularly fine-tunes these policies to counter the evolving threat landscape. HP takes a comprehensive approach to security in designing our products, such as the HP Pro Slate 8 and HP Pro Slate 12 tablets, securing the manufacturing process, and deploying security updates to devices in the field through over-the-air patching.

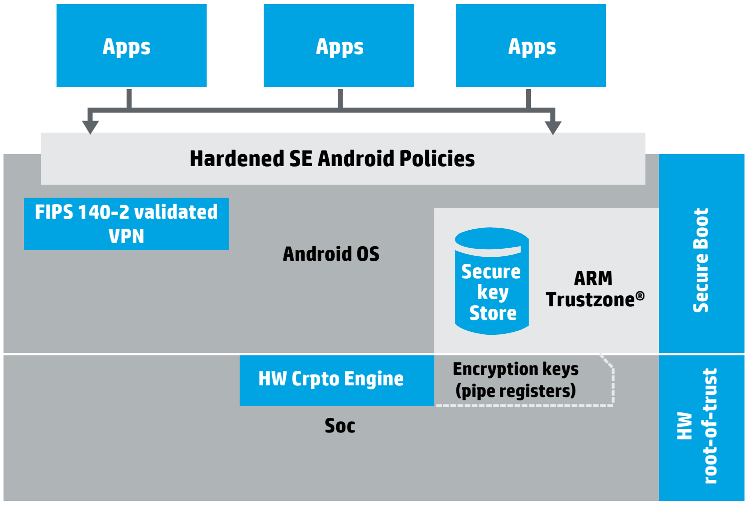
No API fragmentation. Because most businesses use devices from multiple vendors, vendor-specific APIs and security policies will only increase the complexity of securing and managing a device fleet. HP helps avoid such issues through a no-fragmentation approach that lets IT administrators use the same process to manage HP Enterprise-Ready Android devices and stock Android devices. HP Enterprise-Ready Android devices also work with most EMM solutions that support Android, allowing IT administrators to reuse existing EMM solutions. This is one of the many ways HP supports the complex, multi-OS environments that businesses must manage every day.

HP Enterprise-Ready Android features

HP Enterprise-Ready Android devices implement critical security features required to protect user data that go beyond the security features available on most commercially available Android devices geared toward consumers. The illustrations below help visualize the difference.



A Stock Android Implementation



HP Enterprise-Ready Android Secure Implementation

HP Enterprise-Ready Android security features deliver the following benefits:

ARM TrustZone® provides a trusted environment to counter hardware and software exploits.

Secure boot guarantees that only authorized Android images run on the devices.

Secure key-store prevents unauthorized access to the cryptographic keys used by device encryption and applications.

Hardware accelerated device encryption reinforces security, reduces wait times, and conserves power.

FIPS 140-2 validated VPN serves regulated industries such as finance and healthcare, along with U.S. government agencies that require validated encryption for virtual private network (VPN) stacks.

Security hardening minimizes damage from specific types of threats such as privilege escalation attacks.

Microsoft Exchange ActiveSync support works with existing Microsoft Exchange environments to enable mobile access to email, contacts, and calendar.

Over-the-air upgradability helps ensure that the devices remain up to date in terms of security patches such as fixes for the Heartbleed vulnerability, new features such as Android Work, and new releases such as Android Lollipop.

Anti-theft protection with HP Touchpoint Manager helps prevent sensitive data and documents from being compromised by allowing IT personnel to locate, lock, and wipe a lost or stolen device.

EMM compatibility enables standardized management using third-party MDM solutions.

Out-of-the-box manageability with HP Touchpoint Manager allows businesses to secure and manage Enterprise-Ready Android devices without any additional infrastructure, major investments, or extra IT resources.

Security

ARM TrustZone®

Provides a secure environment to mitigate risks from hardware and software exploits

At their core, HP Enterprise-Ready Android devices use proven ARM TrustZone (TZ) technology that provides a secure, hardware-separated environment, a separate memory space, and a TEE. The TEE runs security functions to minimize OS and firmware vulnerabilities as well as risks from malware and misbehaving apps running on the OS.

HP Enterprise-Ready Android devices leverage TrustZone to secure the boot process, data-at-rest encryption keys, and application keys stored in the Android KeyStore. The following sections provide more details.

Example scenario

An employee tries to install a custom image on the mobile device, which could introduce unknown vulnerabilities.

HP Enterprise-Ready Android devices use the secure boot feature to prevent users and hackers from loading unauthorized OS images to gain access to corporate data and networks.

Secure boot

Establishes a trusted platform for Android applications by preventing unauthorized code in the boot process

HP Enterprise-Ready Android devices support secure boot sequence to provide a trusted platform for Android applications. The sequence uses cryptographic methods to authenticate the software by verifying that HP signed the software image. This process prevents injection of malicious and unauthorized code during the boot process.

Secure boot starts from a hardware root of trust that consists of a set of one-time-programmable hardware fuses—non-volatile memory that can be written only once—and Primary Boot Loaders (PBL). One of the hardware fuses contains an HP public key that authenticates the software. Writing this key in the factory prevents subsequent tampering that could, for example, allow unauthorized firmware images to run and compromise user data. The PBL code resides in a read-only-memory (ROM) area inside the SoC, which ensures that the PBL code remains unmodified. This combination is immutable and serves as the root of trust to provide a trusted foundation from where boot sequence is initiated. Each step in the boot sequence loads and authenticates the code used in the subsequent step before executing this code, thus establishing a chain of trust to authenticate all the code that runs from the start of boot to the start of apps.

Upon power-up, the PBL loads, runs, and authenticates the Secondary Boot Loader (SBL) code. The first mutable code that runs in the boot process, SBL initializes the DDR-SDRAM and then loads and authenticates the TrustZone software. Executing TrustZone code before the rest of the mutable code helps protect the integrity of the secure TrustZone environment. The TrustZone code sets up a secure environment in which to securely store cryptographic keys, using ongoing verification, and perform monitoring.

SBL subsequently loads and authenticates the code that initializes the rest of the SoC and application processors. Where available, SBL also loads and authenticates modem firmware prior to execution. The process culminates in loading and authenticating the Android kernel. TrustZone software verifies the code that initializes and operates the peripherals.

HP Enterprise-Ready Android devices use PKI key pairs to verify the software. As explained above, the public key is fused into the device at the factory in a one-time-programmable fuse. The private key is used for signing the software image that is loaded into the devices. The private key is secured within HP facilities, and access is limited to select authorized HP personnel. The verification mechanism does not require the public keys to be secret, allowing HP to program them in the factory without compromising the integrity of the secure boot process.

HP Enterprise-Ready Android secure boot implementation uses 2048-bit exponent 65537 public RSA keys for certificate and image signatures. The SHA256 algorithm is used to sign the PKI certificates, while the code itself is signed using a proprietary algorithm.

Example scenario

Cyber criminals attempt to extract the encryption key by side-loading malware and dumping the device memory.

Although this attack would work on a stock Android device, HP Enterprise-Ready Android devices use an ARM TrustZone-based key management system to secure the keys. Because the keys are not stored in the RAM, dumping the device memory does not reveal the encryption key.

Example scenarios

Cyber criminals steal an executive's tablet to extract highly sensitive corporate information.

Through HP Touchpoint Manager or a compatible EMM solution, IT personnel enforce a policy that requires device encryption as a prerequisite to protect confidential data. This policy helps minimize risk by preventing unencrypted devices from accessing corporate email, contact, and calendar data. Any user data extracted from encrypted devices is useless to the cyber criminals.

Cyber criminals attempt to guess the user password to decrypt the data.

HP Enterprise-Ready Android devices use hardware-based encryption that wipes the data automatically after 32 failed attempts. This behavior is hard-coded and tamper-resistant.

Secure key store

Ensures integrity of cryptographic capabilities by protecting the keys in the TrustZone

Android provides a keymaster component as a service to the applications. This component implements key generation, signing, and verification. Android services and applications use these functions to protect data through encryption and to verify the integrity of the data through signatures. When the integrity of the key management function or the keys themselves is compromised, so is data security.

To prevent such compromises, HP Enterprise-Ready Android devices implement a hardware-backed keymaster environment in which key generation, storage, signature, and verification are performed. Stored keys are accessible to trusted applications running inside TrustZone, and the keys never leave the TrustZone. This approach prevents any malware on the Android side from accessing the keys.

Further, HP Enterprise-Ready Android devices protect the integrity of key management functions by implementing them with the TrustZone environment. Standard keymaster APIs then expose these functions to Android.

Hardware-accelerated device encryption

Provides enhanced security for data at rest through tamper-proof, power-efficient, hardware-based encryption

Android provides a device encryption mechanism to protect user data stored in the device. By default, this mechanism uses a crypto engine implemented in the software and employs AES-CBC-ESSIV: SHA-256 algorithms with 128-bit keys.

Stock Android devices implement software-based encryption to minimize costs related to additional hardware modules and hardware-specific integration efforts. This approach has several disadvantages. First, the encryption key can be compromised, as it is stored in the RAM area. Second, software-based encryption slows down the system, as computation-intensive crypto operations are performed in the software rather than the hardware. Third, this approach consumes excessive power.

HP Enterprise-Ready Android devices employ hardware-based crypto-engines for encryption/decryption and a hardware-based mechanism for storing and retrieving encryption keys. Together, these features offer better security, speed, and power efficiencies. HP Enterprise-Ready Android devices employ AES-XTS-plain64: SHA-256 algorithms with 256-bit keys for file system encryption. A hardware random number generator creates a key, which is encrypted using a hash derived from the user-provided password. The encrypted key is stored inside a key store. This data is further encrypted by a TrustZone component using an AES-256 CBC algorithm and verified using HMAC-SHA-256, providing another layer of security. The encrypted key store data is secured using a versioned and replay-protected, secure storage mechanism to prevent tampering.

Further, HP Enterprise-Ready Android devices allow enterprises to enforce security policies that require users to turn on the device encryption using a compatible EMM solution.

FIPS 140-2 validated VPN

Complies with requirements for U.S. government, defense, and regulated industries such as healthcare and finance

HP Enterprise-Ready Android devices implement FIPS 140-2 validated 256-bit encryption for Virtual Private Network (VPN) connectivity. This feature ensures secure connectivity to corporate networks and employs SSL and IPsec VPN standards. In addition, it supports secure authentication with corporate directories including Microsoft Active Directory (AD).

This VPN implementation is certified by the VPN consortium (VPNC) for interoperability with leading VPN gateway appliances and vendors.

Example scenario

A competitor gets hold of a company sales vice president's tablet and tries to gain ongoing access to confidential information.

The competitor installs malware to snoop information from the device and report back to a stealth server on an ongoing basis. The malware requires system-level privileges to gain unrestricted access, and the tablet is rooted to gain such privileges.

On HP Enterprise-Ready Android devices, hardened SE Android policies protect the data by limiting this type of privilege escalation attack.

Security hardening

Mitigates app-level exploits through hardened SE Android policies and security configurations

Security Enhanced (SE) Android, based on SE Linux, enables rule-based access control to protect Android's system resources, services, and application data. HP Enterprise-Ready Android devices come with a set of hardened SE Android policies that:

- Protect application data by reinforcing application sandboxes to prevent access from misbehaving apps and malware
- Prevent unauthorized access to system services, storage, and sensors by preventing privilege escalation attacks, such as rooting attacks, that gain unrestricted access to and control of the device

HP verifies hardened policies against many known attacks and continues to fine-tune its SE Android policies to provide greater protection.

Manageability

ARM TrustZone® EMM compatibility

Ensures compatibility with incumbent EMM solutions through standards and compatibility testing

Mobile device management (MDM) solutions allow businesses to secure devices and data by remotely provisioning security policies and performing remote lock and wipe operations on lost or stolen devices.

Through its support for Android standard Device Administration (also known as Device Policy Manager or DPM APIs), HP Enterprise-Ready Android devices are compatible with most MDM solutions that support Android. In addition, businesses without an EMM solution can subscribe to HP Touchpoint Manager.

HP Enterprise-Ready Android secure boot implementation uses 2048-bit exponent 65537 public RSA keys for certificate and image signatures. The SHA256 algorithm is used to sign the PKI certificates, while the code itself is signed using a proprietary algorithm.

Out-of-the-box manageability with HP Touchpoint Manager

Provides an instantly deployable and simplified EMM solution to manage PCs and mobile devices

Many small businesses lack IT personnel who understand the nuances in properly deploying, securing or managing mobile devices. These businesses require a tool that simplifies these tasks.

The cloud-based HP Touchpoint Manager service allows businesses to secure and manage HP Enterprise-Ready Android devices, PCs, and other mobile devices from a single, easy-to-use dashboard. This solution is available on a subscription basis and requires no additional IT infrastructure.

Example scenario

A business owner is concerned that employees are not doing enough to protect the company data.

Through HP Touchpoint Manager or a compatible EMM solution, the business owner sets up a policy to require a password and device encryption. The owner may also enforce rules to prevent simple and obvious passwords. Together, these mechanisms protect confidential data.

Example scenarios

A sales professional leaves the tablet at her hotel after a weekend getaway.

The IT support center (or the user, through a self-service portal) issues a remote lock command using HP Touchpoint Manager or another compatible EMM solution. This command locks the device screen until the device is recovered.

A company executive loses his tablet containing confidential data.

The IT support center or user issues a remote wipe command using HP Touchpoint Manager or another compatible EMM solution[3]—removing any user data stored in the device to help prevent confidential data loss.

Microsoft Exchange ActiveSync (EAS) features and policies

Enable secure mobile access to enterprise email, and calendar while leveraging existing IT infrastructure and Microsoft Exchange

HP Enterprise-Ready Android devices work with Microsoft Exchange Server 2003 SP2 and later versions to synchronize email, contacts, and calendar. This support is available through native mail, contact, and calendar client applications included in the Android KitKat release.

To better protect Exchange data, Enterprise-Ready Android devices enable IT administrators to remotely enforce EAS policies such as encryption and password policies. Supported policies include:

- Requiring a PIN or a password to protect the devices from unauthorized personnel
- Requiring a minimum complexity for the password (length, alphabetic or alphanumeric characters, special characters, etc.)
- Controlling the screen lock time
- Requiring device encryption
- Disabling camera

These are available through the native device administration capabilities supported in the KitKat release. The features and policies supported vary based on the Microsoft Exchange server version. See "Appendix A: Microsoft Exchange features and policies."

Remotely administering and enforcing EAS policies requires a compatible EMM or MDM solution.

Anti-theft features

Allow businesses to deter device theft and protect data

Tablets and smartphones are vulnerable to theft and loss. To address this problem, HP Enterprise-Ready Android devices support the following features:

- Sound Alarm
- Lock Device
- Remote Wipe
- Send Message

These features require HP Touchpoint Manager or a compatible third-party EMM or MDM solution[3] from which anti-theft commands are issued.

[3] Third-Party EMM or MDM solution sold separately

Example scenario

An unsuspecting employee downloads malware that is posing as a legitimate app.

The antivirus agent preinstalled on the HP Enterprise-Ready Android device scans the app before installation and alerts the user that it is malware.

Example scenario

Hackers launch a new vulnerability—similar to the much-publicized OpenSSL "Heartbleed" bug—to steal confidential data from affected devices.

HP Enterprise-Ready Android devices are patched promptly over the air, reducing the window of opportunity for potential hacks and minimizing the damage.

Antivirus protection

To help prevent users from installing malware applications, HP Enterprise-Ready Android devices come preloaded with a market-leading antivirus application that provides essential protection against suspected malware. For enhanced protection, customers can upgrade to a premium version.

Security patching through over-the-air firmware delivery

When new vulnerabilities are discovered, all affected systems must be promptly patched. An unpatched system serves as an easy and attractive target to hackers.

HP Enterprise-Ready Android devices are protected through prompt over-the-air delivery of firmware patches for critical vulnerabilities for a period of two years. HP takes into account the severity of a vulnerability, allowing for rapid responses to critical situations.

HP works with Google™ and the SoC vendors to prioritize, develop, and deploy patches. Devices are configured to check the over-the-air server at regular intervals. The server checks for available updates, based on the device model and firmware version, and downloads them to the device. To avoid interrupting user activities or causing other inconveniences, the server applies updates only after the user consents. Consistent with security best practices to protect users from attacks that take advantage of known vulnerabilities, devices cannot be rolled back to prior versions.

In addition to security patches, HP Enterprise-Ready Android devices also support over-the-air updates for the device firmware— allowing the device to keep up with new features and releases introduced as part of the Android roadmap.

Conclusion

The enhanced security, manageability, and support capabilities of HP Enterprise-Ready Android devices are designed to resolve key challenges that IT personnel face when deploying Android devices in a business environment.

HP provides a solid foundation of trusted hardware and firmware, combined with additional security hardening through SE Android policies that undergo regular fine-tuning to safeguard devices against evolving threats. This comprehensive security approach extends from product design and manufacturing to updating devices in the field.

Plus, HP takes a no-fragmentation approach that allows IT administrators to manage HP Enterprise-Ready Android devices and stock Android devices in the same way, and to use existing EMM solutions.

Learn more about HP Enterprise-Ready Android devices at hp.com/go/android-tablets.

Appendix A: Microsoft Exchange features and policies

This section lists features and policies supported in the Enterprise-Ready Android devices when working with various Exchange versions. Note that the features and policies listed for each version are incremental to prior versions.

Exchange ActiveSync 2.5 - Exchange Server 2003 SP2

Features

- Direct push
- Email sync
- Calendar sync
- Contacts sync
- Remote wipe
- Sync multiple folders
- GAL lookup
- SSL encrypted transmission

Exchange ActiveSync 12.0 - Exchange Server 2007

Features

- User-started remote wipe (server side)
- HTML email
- Server search
- Follow-up flags
- Auto discover
- Bandwidth reduction

Policies

- Allow attachment download (client side)
- Maximum attachment size
- Allow simple password
- Password expiration (days)
- Enforce password history

Exchange ActiveSync 12.1 - Exchange Server 2007 SP1

Features

- No additional features

Policies

- Disable camera
- Device encryption
- Minimum number of complex characters for passwords
- Include past email items (days)
- Include past calendar items (days)
- Require manual sync while roaming

Exchange ActiveSync 14.0 - Exchange Server 2010

Features

- Reply state

Policies

- No additional policies

Exchange ActiveSync 14.1 - Exchange Server 2010 SP1

Features

- No additional features

Policies

- Require password
- Require alphanumeric password
- Require encryption on the device
- Allow simple password
- Number of failed attempts allowed (before the device is wiped)
- Minimum password length
- Time without user input before password must be re-entered (idle timeout after which screen is locked)

Sign up for updates
hp.com/go/getupdated

Share with colleagues

Rate this document

4AA5-6428ENW, January 2015