SAMSUNG

White Paper:

Securing and Managing Wearables in the Enterprise

Streamline deployment and protect smartwatch data with Samsung Knox Configure

Introduction: Smartwatches in the Enterprise

As the wearable device market heats up, wrist-worn devices such as smartwatches are leading the pack. According to CCS Insight, forecasts for global sales of smart wearable devices will grow strongly over the next five years, with the global market reaching nearly $30 billion by 2023.[1]

While smartwatches for fitness and activity tracking are popular, consumer demand is only part of the equation. Enterprises are also seeing business value in wearable devices. In a report by Robert Half Technology, 81 percent of CIOs surveyed expect wearable devices like smartwatches to become common tools in the workplace.[2]

81%

of CIOs surveyed expect wearable devices like smartwatches to become common tools in the workplace.

Industries as varied as healthcare, finance, energy, transportation, public safety, retail and hospitality are deploying smartwatches for added business value, such as hands-free communication for maintenance workers, task management, as well as physical monitoring of field workers in dangerous or remote locations. Smartwatches are also being deployed in corporate wellness programs to track fitness and health activities to reduce the cost of insurance premiums.

Yet despite the convenience, productivity and other business value that wearables offer, IT leaders remain concerned about wearable device management and security. Compared with mobile device security and management offerings, which include mobility device management (MDM) and enterprise mobility management (EMM) solutions, wearable device security and management offerings remain limited — impacting the ability of smartwatches and other wearable devices to adequately protect against security vulnerabilities.

Industries as varied as healthcare, finance, energy, transportation, public safety, retail and hospitality are deploying smartwatches for added business value.

Samsung has been working to address these concerns and has developed the tools to make its Galaxy and Galaxy Active smartwatches customizable, easily manageable and highly secure for enterprise users. This white paper will look at how these tools address key wearable security and manageability challenges, as well as considerations for smartwatch deployments.

Wearable Device Security and Manageability Challenges

While most enterprises leverage MDM or EMM solutions to manage smartphones or tablets, first-generation wearables have lacked these same capabilities, including authentication or encryption protocols. One reason authentication may be lacking in wearable devices is the notion that wearables are more secure because, rather than being placed in a pocket or purse, they attach directly to an individual's body. However, even if the risk of loss or theft is lessened with a wearable device, it's not completely alleviated — leaving wearables without authentication protocols and vulnerable to a data breach. In fact, 61 percent of IT professionals surveyed by Ipswitch indicated that security breaches are a top concern for wearable technology.[3]

Lost or Stolen Devices

Without remote wiping capabilities to manage devices, there is heightened risk of confidential corporate data being lost or stolen. Statistics show that 31 percent of workers have lost data due to the misuse of a mobile device.[4] While the number may not be as high with wearable devices due to their being worn on the body, IT leaders can still extrapolate from the data that there is reason for concern when remote wiping capabilities are not in place.

61%

of IT professionals surveyed by Ipswitch indicated that security breaches are a top concern for wearable technology.

Smartwatch Malware

The threat of wearable malware is also growing. As more various applications are developed for smartwatches, there is a greater risk of security vulnerabilities on these devices. Data that may be vulnerable to malware includes real-time geolocation information, messages, emails, contacts and other proprietary business information.

Manageability

The manageability of a fleet of wearable devices is another top IT concern. With many businesses pursuing digital transformation on multiple fronts, the workload of IT staff keeps increasing. Thus, without the ability to bulk enroll and provision wearable devices, managing even a small fleet of devices can be time consuming and resource intensive for IT administrators. In the Ipswitch survey, 45 percent of IT professionals named additional work to support and manage wearables as a chief concern.[5]

In a CIO article, Gartner research director Angela McIntyre acknowledges these difficulties for IT leaders: "A challenge CIOs face with wearables is that the MDM device software is often not yet available from the solution providers," she said. "Many of these devices don't even have SDKs [software development kits] to enable security software."[6]

Key Security and Management Considerations for Smartwatches

While their form factor is different, smartwatches must be evaluated against the same essential security checklist as other enterprise mobile devices. They should be built on a **strong platform** that protects security keys and certificates, limits access and attests to the integrity of the operating system. They must provide IT administrators the ability to enforce **core MDM policies** to provide guardrails for end users. And, acknowledging the wide variety of business use cases for smartwatches, they must be able to be **custom configured** for efficient enterprise use. This white paper will discuss how each of these requirements is addressed through Samsung's Knox Platform for Wearables and Knox Configure solution.

Platform-Level Security

When evaluating wearable device solutions for enterprise deployment, it is critical to ensure that the devices are built on a trusted platform that provides protection from the hardware layer on up. Platform-level security is necessary to protect against both outside malicious actors and inside threats from employee negligence. Malware is a considerable threat to any mobile device, including smartwatches. To limit an application's ability to alter the device at the operating system level, the security platform should provide protection at boot, runtime and application layers.

Core Device Management

Without MDM capabilities, IT administrators are unable to effectively secure wearables deployed within the enterprise. While MDM controls for smartwatches may be less complex than those for smartphones and tablets, establishing a core set of policies is essential. Core capabilities of an MDM solution should include the ability to remotely wipe devices that are lost or stolen, lock the device to prevent unauthorized access, apply setting restrictions on connectivity, whitelisting/blocklisting applications and push firmware updates.

Advanced Configuration

As businesses look to use smart-watches to streamline business processes or perform specific functions, the need for custom configuration is growing. In some circumstances, enterprises will want to go beyond the core management capabilities listed above and fully customize or lock down wearables for a specific app. Advanced capabilities to customize wearable devices include the ability to preload apps, lock the device into a single app, or even remap the hardware keys.

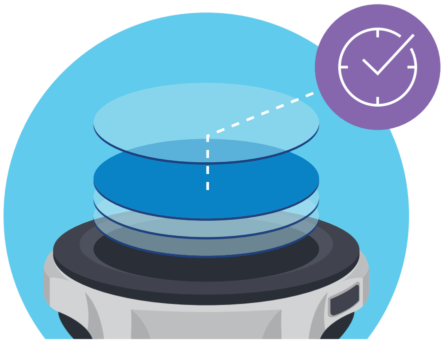
Samsung's Knox Platform for Tizen Wearables

Over the past several years, Samsung has invested considerable resources in building a full enterprise mobile security and management stack. The Samsung Knox platform, which was initially developed to secure Samsung Android-based smartphones and tablets, has received top ratings from industry analysts as well as security certifications from government agencies such as the U.S. Department of Defense.

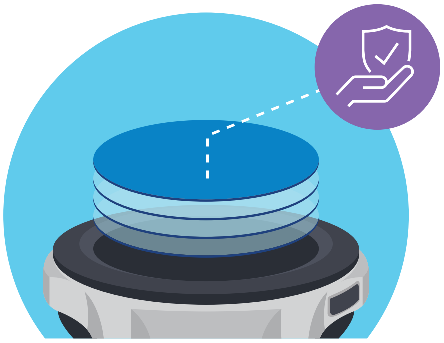
Since its initial development, Samsung has extended the core principles of the Knox platform to its Tizen-based smartwatches. This ensures that the Tizen devices have the same hardware-based, multilayered protection as other Samsung Galaxy devices. Core security features of the Knox Platform for Tizen wearables include:

TrustZone-Based Tizen Key Manager:
The Tizen Key Manager is based on TrustZone, which is a processor architecture that isolates sensitive computations and security certificates. The Key Manager provides functions to securely store keys, certificates and sensitive data related to users and their password-protected apps.

Secure Boot and Attestation:
Secure Boot is a security mechanism that prevents unauthorized boot loaders and kernels from being loaded during the startup process. Additionally, through attestation, IT admins are provided with device binary information if a device is not running the original factory binaries. This allows IT to determine whether the device has been tampered with or not.



Real-Time Kernel Protection (RKP) +
TrustZone-Based Integrity Measurement Architecture (TIMA):
Combined with TIMA, which provides security from the hardware level through to the OS and application, RKP prevents running unauthorized privileged code on the system and kernel data from being directly accessed by user processes. It also monitors some critical kernel data structures to verify that they are not exploited by attacks.



Security Enhancement for Tizen + Mandatory Access Controls:
This feature improves Tizen platform security and protects applications and data by strictly defining what each process is allowed to do and which data it can access.

Core Device Management Principles for Smartwatches

As previously discussed, MDM and EMM software is commonly used by enterprises to efficiently manage and secure a fleet of smartphones or tablets. Common features of smartphone and tablet MDM consoles include the ability to remotely wipe devices if they are lost or stolen, blocklist webpages, limit the applications which can be loaded onto a device and manage software updates. These remote capabilities, which can be applied across the fleet of devices, ensure consistent device security and management policies for the enterprise.

Smartwatches, however, have some notable differences when compared to smartphones and tablets. For instance, wearables can either be standalone devices that work independently over a cellular network without having to connect to a smartphone, or they may be designed to work in conjunction with a smartphone or tablet through Bluetooth tethering. Additionally, smartwatch applications are much more limited in function, and smartwatches are not typically used for traditional web browsing.

Knox Configure for Wearables

Samsung's Knox Configure for Wearables addresses all of the core device management requirements and use cases, eliminating the need for a separate MDM to manage smartwatches. The device management features of Knox Configure for Wearables include:

- **Device lock:**
Provides the ability to enforce the use of authentication PIN, or to activate screen lock remotely to protect against unauthorized access.

- **Remote wipe:**
Prevents data leaks by remotely triggering a factory reset in the event that a device is lost or stolen.

- **Connectivity restrictions:**
Manages and restricts device settings for Wi-Fi, Bluetooth, GPS, near-field communication (NFC) and flight mode to save battery drain and to avoid the possibility of connecting to unsecured networks.

- **Application block/whitelisting:**
Permits end users to install and use only a limited set of applications on the device. Internet browser applications can be blocked, eliminating the need for web-filtering.

- **APN Management:**
Securely push custom/private APNs to the device during configuration for devices that need to be placed on an MVNO band or managed network.

- **Device feature restrictions:**
Restricts the use of roaming, tethering, factory reset, SD card, USB storage, camera, microphone and more.

- **Firmware update management:**
Disables firmware updates and security patches from being pushed to devices over both cellular and Wi-Fi.

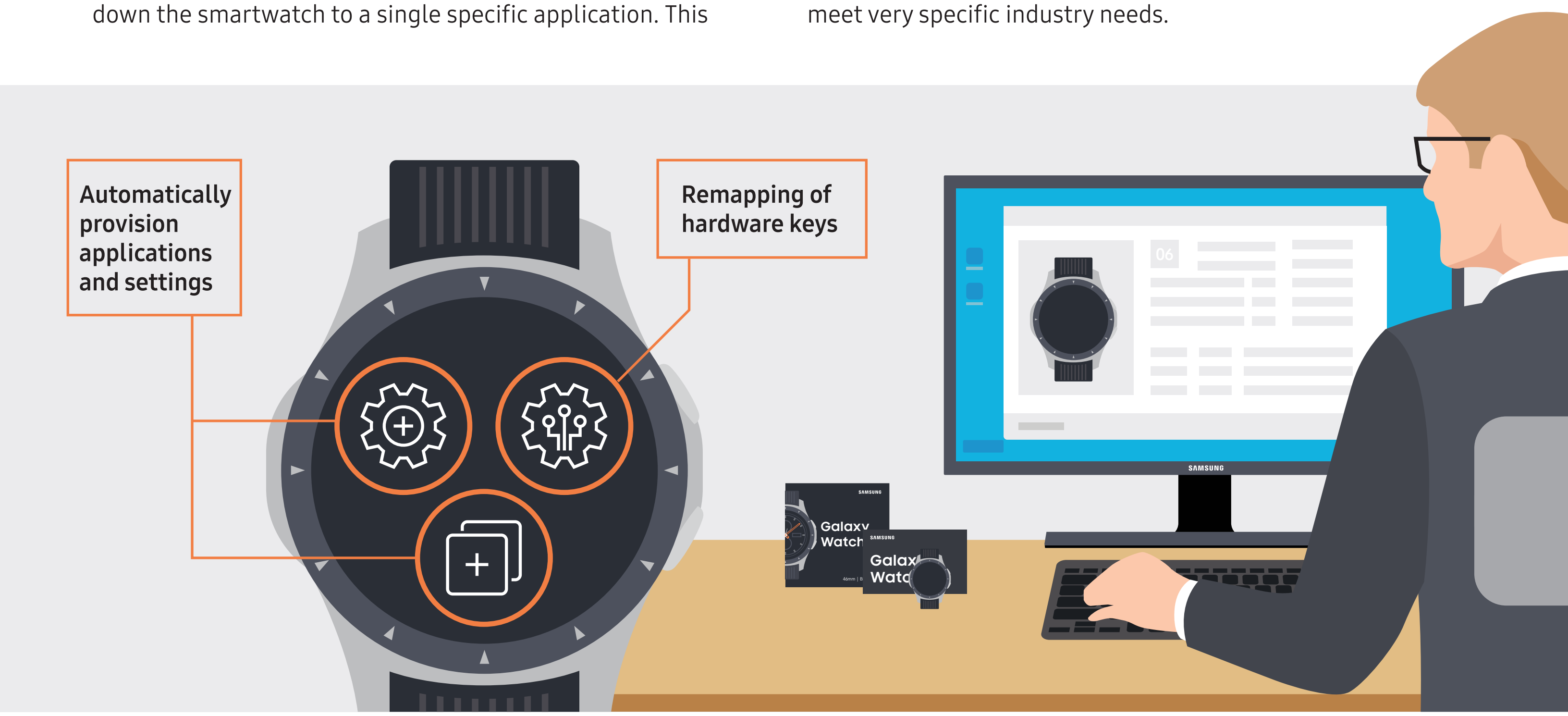
Advanced Configuration of Smartwatches for Business Use

Advanced device configuration capabilities can further improve both the security and business functionality of wearables used within the enterprise for a particular application. Similar to "gold master" images that are developed to configure desktop and laptop PCs for an enterprise workforce, Knox Configure allows the creation of granular smartwatch profiles that can be pushed out across a user group.

Here's a look at how enterprises can take advantage of these advanced configuration capabilities to enhance not only security, but also the business utility of the smartwatches:

- **Automatically provision applications and settings:** Allows IT to automatically provision, enroll and configure smartwatches during initial setup and after factory reset. Provisioning and configuration can be done based on roles, allowing IT to assign different custom profiles to each user group.
- **Remove preloaded applications:** To streamline the user experience, preloaded applications that are not needed can be disabled or removed.
- **Dedicated application mode:** Through the use of the "kiosk" mode, enterprises can lock down the smartwatch to a single specific application. This prevents users from accessing the settings menu, and system notifications can be hidden.
- **Remapping of hardware keys:** Hardware keys, such as a long or double press of the physical "back" and "home" buttons, can be remapped to perform a specific key function within an application, allowing the business to provide a specialized user experience.
- **Add Wi-Fi profiles with advanced security options:** Preconfigure the Wi-Fi networks that the smartwatch can connect to. End users won't need to worry about putting in Wi-Fi passwords, and it can eliminate security concerns of employees connecting to unsecured Wi-Fi networks.

There is such a wide range of potential uses for smartwatches in the enterprise, so the ability to custom configure devices is critical. For example, a public safety agency may wish to configure its smartwatches to access only one, key dispatch application, enabling officers in the field to receive urgent alerts. To support improved officer safety, the agency may also want to remap hardware buttons to trigger an immediate request for backup upon double press. Knox Configure allows this level of advanced customization to meet very specific industry needs.


Automatically provision applications and settings
Remapping of hardware keys
SAMSUNG
Galaxy Watch

Conclusion: Security, Manageability and Business Value

Wearable devices can deliver high business value, but that value can only be tapped into when IT leaders feel confident that managing them won't overburden resources or impact the security of corporate data. As smartwatches continue to expand in the enterprise market, security risks will only heighten, making it all the more important to deploy solutions today that can protect against future vulnerabilities.

Organizations that do not think through security and manageability when executing a smartwatch deployment risk suffering a security breach or struggling to deal with scalability issues as wearable use across the organization grows.

Samsung's Knox Platform for Tizen Wearables provides an enterprise-grade security foundation, mirroring the hardware-based, multilayered approach implemented on Samsung's Android tablets and smartphones. Integrating closely with this platform, the Knox Configure for Wearables service allows enterprises to implement core mobile device management policies and custom configure devices to match their business needs.

Samsung offers a range of smartwatches for enterprise deployments, including the Galaxy Watch and Galaxy Watch Active, which feature standalone 4G connectivity, advanced sensors, military-grade durability and all-day battery life.

Learn more about Samsung's smartwatch portfolio: samsung.com/b2bwearables

Learn more about Samsung Knox Configure: samsung.com/knox

Footnotes

1. "Optimistic Outlook for Wearables," CCS Insights, March 2019, https://www.ccsinsight.com/press/company-news/optimistic-outlook-for-wearables/.
2. "Tech Leaders See Wearables Working in the Workplace," Robert Half Technology. PR Newswire. April 22, 2015.
3. "IT Pros Worried About Wearable Technology in the Workplace," Ipswitch. September, 2015.
4. "Securing #GenMobile: Is Your Business Running the Risks?" Aruba Networks, 2015.
5. "IT Pros Worried About Wearable Technology in the Workplace," Ipswitch. September, 2015.
6. "Wearable Devices Offer Promise (and Potential for Peril) for the Enterprise," Al Sacco. CIO Jan. 22, 2014.

Learn more: samsung.com/b2bwearables | insights.samsung.com | 1-866-SAM4BIZ

Follow us: youtube.com/samsungbizusa | @SamsungBizUSA

SAMSUNG