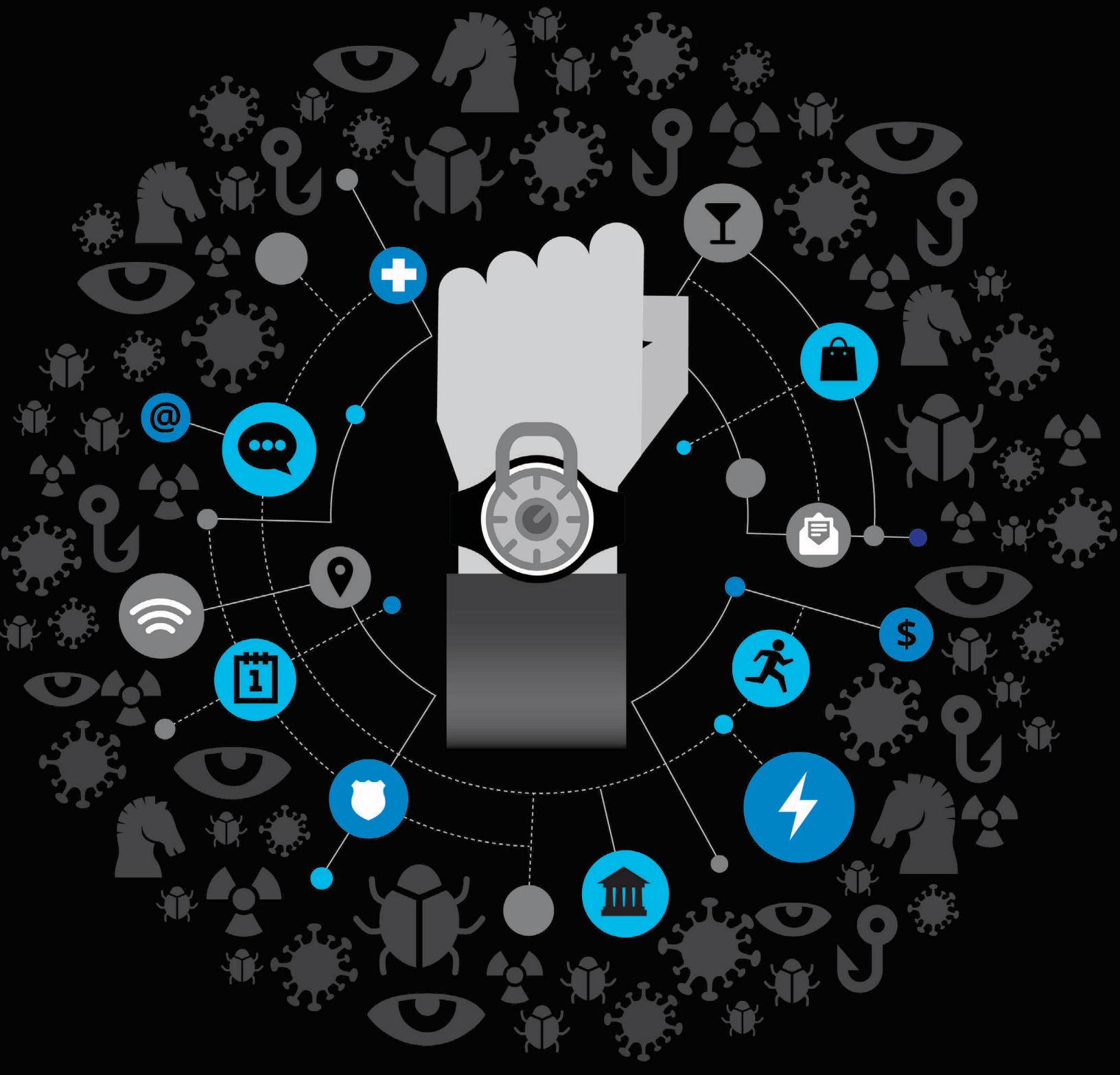
SAMSUNG

White Paper:

Securing and Managing Wearables in the Enterprise



As the wearable device market heats up, wrist-worn devices such as smartwatches lead the pack in device sales. Smartwatches were forecast to account for almost half of all wearable device shipments by early 2017 — more than 60 million units, according to CCS Insight.[1] CCS predicts that by 2020, the smart wearable market will be worth $34 billion, with smartwatches comprising approximately a quarter of device sales.[2]

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.[3]

81% of CIOs surveyed expect wearable devices like smartwatches to become common tools in the workplace.[3]

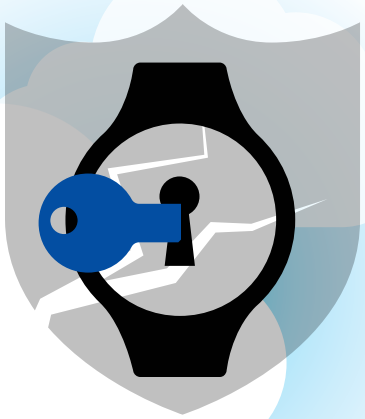
Industries as varied as healthcare, finance, energy, transportation, public safety, retail and hospitality are deploying smartwatches for added business value, such as hands-free communication for maintenance workers, GPS and barcode tracking for faster product location in warehouses and physical monitoring 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 wearables offer, IT leaders remain concerned about wearable device management and security. Compared with mobile device security and management offerings, which include MDM (mobility device management) and EMM (enterprise mobility management) solutions, wearable device security and management offerings remain limited or non-existent — impacting the ability of smartwatches and other wearable devices to adequately protect against security vulnerabilities.

With the recent introduction of the SDK for Samsung's Gear S3, IT leaders now have access to a smartwatch that takes their security and manageability concerns seriously. Not only is the smartwatch's hardware secure, but enterprise customers can leverage a comprehensive EMM solution to address additional security and manageability requirements. This paper takes a deeper dive into what Samsung SDS' EMM for wearables offers and how IT leaders can take advantage of the solution to effectively incorporate Gear S3 smartwatches into their corporate device portfolio.

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

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, wearables attach directly to an individual's body. However, even if the risk of loss or theft is less with a wearable device, it's not completely alleviated — leaving wearables without authentication protocols vulnerable to a data breach. In fact, 61 percent of IT professionals surveyed by Ipswitch indicated that security breaches are their top concern for wearable technology.[4]

> Cisco predicts that 600 million wearable devices will be online globally by 2020.[5]

Additionally, with Cisco predicting that 600 million wearable devices will be online globally by 2020,[5] there is a high level of security concern around the data wearable devices collect — which typically resides in the cloud in an unencrypted state. In a recent Cloud Security Alliance survey, 73 percent of IT respondents said concerns about the security of data in the cloud was an issue.[6]

Manageability of a fleet of wearable devices is another IT concern, and one that has so far not been well addressed by wearable manufacturers. Without the ability to bulk upload applications or provision wearable devices, managing a fleet of devices can be time-consuming and resource-intensive for IT administrators. For instance, in 2015, the Mitre database, which maintains the database on common vulnerabilities and exposures (CVE), assigned over 6,000 new CVEs.[7] Not surprisingly, nearly half of all IT staff surveyed said they struggle to keep up with or are overwhelmed by the volume of patches released.[8] With many offices using increasingly complex technology, the workload of IT staff keeps increasing. In the Ipswitch survey, 45 percent of IT professionals named additional work to support and manage wearables as their chief concern.[9]

Further, 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.[10] 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.

In a CIO article, Gartner research director Angela McIntyre acknowledges these difficulties for IT leaders: "A challenge CIOs face with wearables," she said, "is that the MDM device software is often not yet available from the solution providers. Many of these devices don't even have SDKs to enable security software."[11]

> **61%** of IT professionals surveyed by Ipswitch indicated that security breaches are their top concern for wearable technology.[4]

Better Management of Security Threats

Forrester predicts that in 2017 more than 500,000 IoT devices will suffer a compromise.[12] Smartwatches and other smart wearables will be vulnerable, making it imperative for enterprises deploying wearables to have a way to secure the devices and protect corporate data. While there are numerous levels of security that must be addressed in any smart device, focusing on security at the hardware level is critical. Yet, most wearable devices lack even basic hardware security features that would prohibit devices from being rooted or prevent malicious attacks against the operating system.

To avoid such vulnerabilities, the Gear S3 is built securely from the ground up, starting with the Knox security platform — the same hardware and application layer of security as other Samsung smartphones and tablets. Built-in security features for Knox on Samsung's Tizen-based smartwatches include:

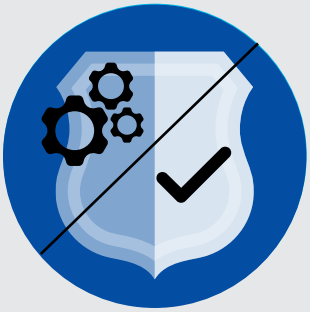
Forrester predicts that in 2017 more than 500,000 IoT devices will suffer a compromise.[12]

Hardware Root of Trust

A set of security mechanisms built into device hardware that flag any time the device's default controls have been altered. These include Secure Boot Key and Device Root Key, which perform authentication and encryption operations associated with the device.

Secure Boot

Secure Boot prevents unauthorized bootloaders and kernels from being loaded onto the device. This means that your device has not been tampered with and the Knox container can be loaded.



Trusted Boot

Trusted Boot ensures that the bootloader and OS kernel are the originals from the factory. This is done by recording the original device measurements and consistently checking the device at the start up to make sure these measurements haven't changed.

EMM for Wearables

A secure hardware layer is critical, but as IT leaders know, it's not the end of the story — vulnerability lies at every level, including the application layer.

EMM providers understand these threats and are working to build solutions; however, varying operating systems for smartwatches and smartphones, as well as lack of API standardization, are making it difficult for vendors to create an effective application that runs solely on the wearable device. A secondary solution has been to pair a smartphone with a wearable device. While this is a step in the right direction, such a solution still leaves wearable hardware vulnerable and limits the security and manageability their solutions can provide. Manageability is almost as big of an issue for IT administrators as security. Without the ability to manage and provision devices in bulk and through remote access, scaling wearables in an enterprise setting is difficult.

In addition to having the Knox platform integrated into the Gear devices, Samsung has built a Tizen SDK kit for its Gear S3 smartwatches. The SDK provides more than 300 APIs, many of which help enable security and manageability on the device.

However, to make it easier to manage and secure Gear smartwatches in the enterprise, Samsung SDS recently released an EMM for wearables. For IT leaders, the EMM provides critical security and manageability features that make scaling wearables at the enterprise-level more feasible.

The Samsung SDS EMM for wearables offers three categories of value: managing apps, managing the wearable device and securing the wearable device. Here's a deep dive into the features of each:

1. Managing Apps

By deploying the SDS EMM on Gear smartwatches, IT administrators gain the ability to secure and manage applications on the device. Key features include:

Remote app management: Includes the ability to install, update and uninstall apps; start and stop apps; set up user accounts for email applications; and wipe app data.

App user control: Allows IT to whitelist and blacklist apps and have complete control over what apps users can put on the device to help limit malware threats.

App removal: Permits organizations to remove preloaded apps and create customized, purpose-built devices that run only the applications necessary for the job function.

Having remote app management capabilities streamlines application management for IT, while other application features enhance control and allow enterprises to deploy wearables customized for specific use cases. Further, having the ability to track app stats allows IT to make informed decisions on what applications may drive down battery life or in other ways reduce the overall usability and productivity of the wearable.

The EMM provides critical security and manageability features that make scaling wearables at the enterprise-level more feasible.

Six out of ten workers said they were happy to let others regularly use their work devices.[13]

2. Managing Wearable Devices

Samsung SDS' EMM solution also provides manageability features at the device level that allow IT administrators better control of the device and how employees use it. For instance, IT can set up access point names (APNs) to control the Wi-Fi access points employees can connect to with their devices, limiting the risk of unsecured connections. Additionally, IT can configure browser settings or get device information such as available memory and last check-in.

If devices are being deployed for a specific use case, such as scanning barcodes for product locations in a warehouse, IT can maintain further control and increase the productivity value of the devices by restricting certain features that are not necessary, such as blocking incoming and outgoing calls or texts. In work environments where it is required for compliance or will improve business intelligence, such as in a customer service-oriented use case, IT can enable statistic tracking and GPS location. Finally, GPS, NFC and other wearable device features can be controlled remotely, giving IT the ability to track the devices and/or employees.

13% of data breaches are caused by company insiders.[14]

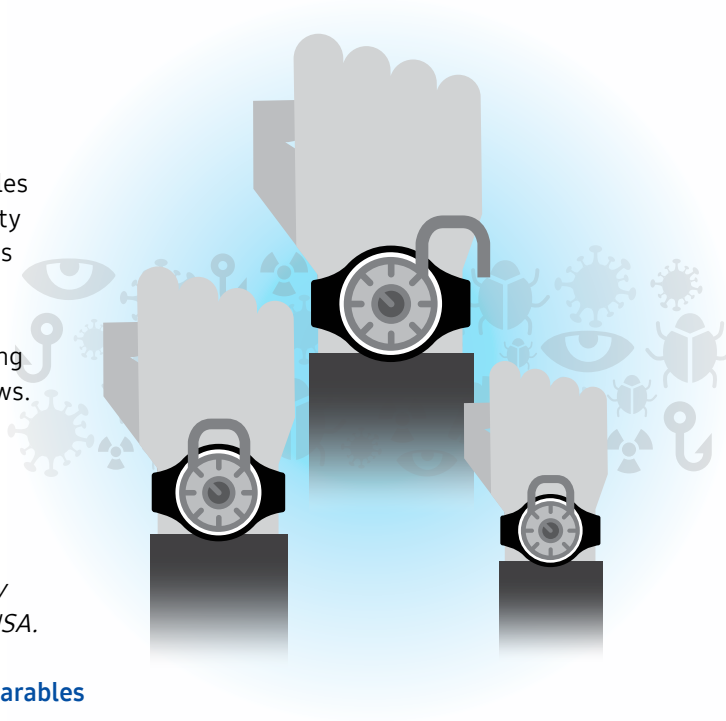
3. Securing Wearables

On the security side, the SDS EMM for wearables offers several features that enhance its secure Knox platform and enable IT to better protect corporate data. The Samsung SDS EMM solution can:

- Set up password requirements for unlocking devices to ensure strong authentication requirements that better secure the devices if lost or stolen.
- Encrypt data to better secure data that is stored in the cloud.
- Disable device features to increase security in specific environments — IT can disable device features such as Bluetooth, Wi-Fi, NFC and GPS.

By tapping into these management and security features, IT can address one of the biggest threats to any device's security — the human element. Unfortunately, employees do not always take security seriously. In a recent survey from Aruba Networks, six out of ten workers said they were happy to let others regularly use their work devices.[13] Meanwhile, a Bitglass report found that 13 percent of data breaches are caused by company insiders.[14] Strong authentication, encryption, firewalls and disabling cameras or microphones in confidential environments all help limit the risk of data breaches when devices are lost or stolen or when employees may have malicious intentions.

Conclusion



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 wearables continue to expand into both the consumer and enterprise markets, security risks will only heighten, making it all the more imperative to deploy devices today that can limit an organization's vulnerability tomorrow. Those organizations that forgo the security and manageability aspects an EMM solution provides on wearables risk suffering a security breach or struggling to deal with scalability issues as wearable use across the organization grows.

Gear S3 smartwatches provide users with a high-quality user experience and offer IT leaders the ability to achieve security and manageability requirements for devices while driving higher business value for the organization.

Samsung SDS' EMM solution is certified by the Common Criteria laid out by the National Information Assurance Partnership (NIAP), managed by the NSA.

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

Click here to learn more about the Samsung SDS EMM

Footnotes:

1 "Wearables Momentum Continues," CCS Insights. Feb. 17, 2016.

2 Ibid.

3 "Tech Leaders See Wearables Working in the Workplace," Robert Half Technology. PR Newswire. April 22, 2015.

4 "IT Pros Worried About Wearable Technology in the Workplace," Ipswitch. September, 2015.

5 "IoT Technology Makes Security and Privacy Top Challenges for Wearables," Kenneth Corbin. CIO. March 8, 2016.

6 "Cloud Adoption Practices and Priorities Survey Report," Cloud Services Alliance. January 2015.

7 "Combating Patch Fatigue," Tripwire. 2016.

8 Ibid.

9 "IT Pros Worried About Wearable Technology in the Workplace," Ipswitch. September 2015.

10 "Securing #GenMobile: Is Your Business Running the Risks?" Aruba Networks. 2015.

11 "Wearable Devices Offer Promise (and Potential Peril) for the Enterprise," Al Sacco. CIO. Jan. 22, 2014.

12 "Data Breaches Through Wearables Put Target Squarely on IoT in 2017," Ryan Francis. CSO. Jan. 3, 2017.

13 "Securing #GenMobile: Is Your Business Running the Risks?" Aruba Networks. 2015.

14 "Financial Services Breach Report." Bitglass. 2016.

WHP_WEARABLES_MANAGEMENT_MAY17SW