THE MOBILE SECURITY GAP

In a recent survey of more than 4,000 IT and IT Security professionals, 77 percent of respondents said that the use of mobile devices in the workplace is important to achieving their business objectives. But a nearly equal portion of survey-takers—76 percent—believe that these devices introduce a “serious” set of risks. At the same time, only 39 percent of organizations have security controls in place to mitigate risks.

That’s a great characterization of the mobile security gap faced by most organizations today. Mobile devices are essential to the business, but they pose major security risks that few organizations have begun to address.

THE IMPACT ON USABILITY

Organizations that have attempted to address the security vulnerabilities introduced by mobile devices have often done so at the expense of usability and user choice. VPN connections, container solutions and other security measures implemented to protect corporate networks, apps and data often introduce the need for multiple sign-ins and other barriers that make the user experience convoluted, awkward, and fraught with support issues.

Strict security and manageability requirements have also caused many organizations to block employee-owned devices from accessing corporate networks, apps and data. Employees who want to use mobile devices for work must use corporate-owned devices, which run only corporate email and applications. Unhappy employees wind up carrying both company-owned and personal devices, switching back and forth as the situation demands. It would be much simpler if the devices employees love could just be made secure and manageable for the workplace.
When it comes to devices users love, nothing beats the Android and Samsung combination. With more than 81% of the smartphone market share as of Q4 2013, Android is the world’s most popular smartphone platform, and Samsung sells more Android devices than anyone else.

With the introduction of KNOX, Samsung has delivered breakthrough technologies that bridge the mobile security gap, bringing enterprise-grade security and manageability to the world’s most popular devices.

**SAMSUNG KNOX OVERVIEW**

Samsung KNOX was designed from the ground up to address the needs and requirements of the enterprise. While retaining full compatibility with Android and the Google ecosystem, Samsung KNOX integrates fundamental enhancements to safeguard platform and application security and improve device manageability. All of these advantages make Samsung KNOX the perfect choice for both regulated and general enterprise environments.
PLATFORM SECURITY

Samsung KNOX addresses platform security with a comprehensive three-pronged strategy to secure the system: Customizable Secure Boot, ARM® TrustZone®-based Integrity Measurement Architecture (TIMA), and a kernel with built-in Security Enhancements for Android (SE for Android) access controls.

Customizable Secure Boot
Customizable Secure Boot forms the first line of defense against malicious attacks by ensuring that only verified and authorized software can run on Samsung KNOX devices.

TrustZone-based Integrity Measurement Architecture (TIMA)
TIMA provides continuous integrity monitoring of the device’s Linux kernel. When TIMA detects that the integrity of the kernel or the boot loader is violated, it takes a policy-driven action in response. One of these policy actions can disable the kernel and power down the device.

Security Enhancements for Android
Security Enhancements for Android isolates applications and data into different domains so that threats of tampering and bypassing of application security mechanisms are reduced while the amount of damage that can be caused by malicious or flawed applications is minimized.

APPLICATION SECURITY

In addition to securing the platform, Samsung KNOX addresses enterprise application and data security requirements. The Samsung KNOX container provides security for enterprise data by isolating enterprise applications and encrypting enterprise data both at-rest and in motion.

Samsung KNOX Container
Samsung KNOX Container is an isolated and secure environment within the mobile device, complete with its own home screen, launcher, applications, and widgets. Applications and data inside the container are separated from applications outside the container. This provides a powerful solution for the “data leakage problem” associated with the BYOD model.

Encrypted File System
Samsung KNOX container uses a separate encrypted file system completely isolated from applications outside the container. The data is encrypted using an Advanced Encryption Standard (AES) cipher algorithm with a 256-bit key (AES-256).

Virtual Private Network
Samsung KNOX container offers an on-demand FIPS-certified VPN client called per-app VPN. Per-app VPN provides enterprise IT administrators with the ability to configure, provision, and manage the use of VPN on a per-application basis. Samsung KNOX container VPN offers support for strong IPSec VPN encryption for most sensitive government agencies, including support for Suite B cryptography.
SAMSUNG KNOX & CORPORATE LIABLE DEVICES

The extensive security features of Samsung KNOX enable corporate IT departments to protect enterprise networks, apps and data while accommodating the personal use of corporate-owned devices. KNOX Customizable Secure Boot, TrustZone®-based Integrity Measurement Architecture (TIMA), and built-in Security Enhancements for Android (SE for Android) provide malware protection that effectively extends from the hardware up. With hardware-based integrity measurements and built-in security enhancements, Samsung KNOX technologies effectively detect malicious or flawed software, and prevent it from compromising the device, data or applications.

Samsung KNOX Container isolates applications and data and enables a powerful solution for the “data leakage” problems associated with many Android applications. KNOX advanced encryption allows users and enterprise IT administrators to encrypt data on the entire device with a FIPS 140-2 certified Advanced Encryption Standard (AES) cipher algorithm with a 256-bit key (AES-256) and offers the levels of security required by government and regulated industries such as healthcare and finance.

Samsung KNOX comprehensive support for an enterprise virtual private network (VPN) enables businesses to offer their employees an optimized, secure path to the enterprise intranet from their BYOD or corporate-issued device.

SAMSUNG KNOX & BYOD

Samsung KNOX offers all the same protections to IT departments looking to implement and manage BYOD strategies. For employees, KNOX Container technology keeps personal apps and data private and separate from corporate apps and data. IT departments can remotely disable, lock or wipe only the corporate information on the device without compromising individuals’ personal data and applications.

For users, Samsung KNOX offers a seamless and intuitive dual-persona platform that enables effortless switching from personal to business modes. Samsung KNOX Container provides the user reassurance that their personal applications and data are safe and separate from their work environment.

MOBILE DEVICE MANAGEMENT

Mobile Device Management (MDM) helps enterprises to monitor, control, secure and administer mobile devices used by employees. Several vendors provide MDM solutions with a broad range of capabilities and features. Samsung KNOX works with all leading MDM solutions by providing a wide variety of policies for security, enterprise integration, asset tracking, remote control, and more.

The advanced security and management features of Samsung KNOX make it the ideal Android platform for enterprise deployment.
Samsung KNOX builds upon Samsung’s industry-leading SAFE® MDM capabilities by providing additional policies for security, enterprise integration, and enterprise applications such as asset tracking, remote control, and so on. With more than 400 SAFE policies and 73 KNOX policies, Samsung KNOX is unequalled as a platform for enterprise deployment.

<table>
<thead>
<tr>
<th>ENTERPRISES NEED</th>
<th>MANAGEMENT POLICIES</th>
</tr>
</thead>
<tbody>
<tr>
<td>CONFIGURATION</td>
<td>Wi-Fi</td>
</tr>
<tr>
<td></td>
<td>Bluetooth</td>
</tr>
<tr>
<td></td>
<td>Kiosk Mode</td>
</tr>
<tr>
<td></td>
<td>Roaming</td>
</tr>
<tr>
<td></td>
<td>VPN</td>
</tr>
<tr>
<td></td>
<td>Geo Fencing</td>
</tr>
<tr>
<td></td>
<td>Call Logs</td>
</tr>
<tr>
<td></td>
<td>Email Forwarding</td>
</tr>
<tr>
<td>CONTROL &amp; LIMITS</td>
<td>Security</td>
</tr>
<tr>
<td></td>
<td>Password</td>
</tr>
<tr>
<td></td>
<td>Applications Rights</td>
</tr>
<tr>
<td></td>
<td>Phone Restrictions</td>
</tr>
<tr>
<td>ENTERPRISE</td>
<td>Exchange Account</td>
</tr>
<tr>
<td>INTEGRATION</td>
<td>CAC</td>
</tr>
<tr>
<td></td>
<td>Message Logs</td>
</tr>
<tr>
<td></td>
<td>Device Inventory</td>
</tr>
<tr>
<td>MONITORING</td>
<td>Email Accounts</td>
</tr>
<tr>
<td></td>
<td>Browser</td>
</tr>
<tr>
<td></td>
<td>APN Settings</td>
</tr>
<tr>
<td>PREVENT DATA LEAK</td>
<td>Container Management</td>
</tr>
<tr>
<td></td>
<td>Integrity Management</td>
</tr>
<tr>
<td>SRG-SPECIFIC POLICIES</td>
<td>Email Forwarding</td>
</tr>
<tr>
<td></td>
<td>Container Management</td>
</tr>
<tr>
<td></td>
<td>Integrity Management</td>
</tr>
<tr>
<td>LEGEND</td>
<td>SAFE Policy</td>
</tr>
<tr>
<td></td>
<td>KNOX Policy</td>
</tr>
</tbody>
</table>

Specific MDM enhancements include:
- Policies to comply with the US DoD Mobile OS Security Requirements Guide (MOS SRG)
- Support for Samsung KNOX Container
- Support for management via ActiveDirectory/Group Policy Manager
- VPN and Wi-Fi Provisioning
- Idle screen and lock screen configuration

**SECURE MOBILE APP DEVELOPMENT**

Samsung KNOX offers real advantages to mobile app developers. The security features integrated into the KNOX platform enable existing Android eco-system applications to automatically gain enterprise-grade security, when deployed within the KNOX Container, for data storage and transmission without any new application development. Samsung KNOX also relieves application developers from the burden of developing individual enterprise features like FIPS-compliant VPN, on-device encryption (ODE), and enterprise Single Sign On (SSO). Leveraging the KNOX foundation for app security can shorten development cycles and reduce the costs of building secure mobile applications—a big plus both for app developers and enterprise IT organizations.
CONCLUSION

For enterprises that have wanted to move to Android because of its openness, flexibility and user appeal, but were holding back because of security concerns, Samsung KNOX provides an exciting, secure, enterprise-friendly solution. There are some big benefits:

- Samsung KNOX platform and app security enhancements effectively address the leading security concerns that have dogged Android—making it possible for the first time for IT organizations to welcome Android into the enterprise without worry.
- The popularity of Samsung and Android means IT organizations can finally let employees use the devices they want while still getting the security and manageability they need.
- Another major advantage of the KNOX is that it enables enterprises to adopt secure Android devices that can cost considerably less than alternative solutions—a major cost savings for corporate-liable environments.
- Samsung KNOX reduces the lifetime costs of enterprise mobility by ensuring the security and integrity of the mobile environment and by making devices easier to manage.
- Finally, the security advances built into the KNOX platform are easily leveraged by mobile apps. This reduces the cost and complexity of mobile app development, and makes it easier for developers and IT organizations to quickly roll out, update and support enterprise applications.

The benefits of Samsung devices and the Android platform are brought to life by KNOX in enterprise environments, making it possible for the first time to combine security, manageability, user experience and cost effectiveness in one incredibly attractive package. Whether your mobile strategy is to support corporate-liable devices, BYOD or both, Samsung KNOX merits careful evaluation.

DMI & SAMSUNG

Digital Management, Inc. (DMI), a world-leading provider of mobile enterprise solutions and services, has formed a strategic alliance with Samsung to implement and manage Samsung security solutions and platforms, including Samsung Knox™, for enterprise and government customers. Through this collaboration, the companies will equip enterprises with a complete portfolio of services that address the secure deployment and management of Samsung Mobile smartphones and tablets, including:

- Enterprise Mobility/Security Assessment
- Mobile Device Management (MDM) Solution Implementation/Migration
- Device Migration Services
- Mobility Solution Management
- End User Help Desk
- Staging/Kitting/Device Configuration/Device Provisioning Services
DMI MANAGED MOBILITY SERVICES

DMI offers the most comprehensive set of Mobile Enterprise Solutions in the world—everything from Mobile Strategy and Managed Mobility Services to Mobile Application Solutions and Integrated Big Data Analytics. We provide Managed Mobility Services for more than 500,000 devices all over the world. We keep hundreds of thousands of users connected and productive with 24 x 7 mobile helpdesk support. And we keep mobile environments up-to-date, secure, and running at peak performance for hundreds of enterprise clients.

DMI is also Samsung’s Enterprise Service Partner in the US, and a Certified Samsung Knox solution provider. No one offers a more comprehensive mobile business solution than DMI.

MANAGED MOBILITY SERVICES OVERVIEW:

24 x 7 Mobility Solution Management Services
Continuous monitoring, management, and troubleshooting for your mobility management systems, including:

- Policies, settings, LDAP and SCEP integration, certificate management, and more
- Application management and control policies
- Troubleshooting and log file analysis. System upgrades. Reporting. (Supported vendors include MobileIron, AirWatch, Good Technology, and BlackBerry)

Provisioning and Deployment Services

- Fully secured and provisioned devices are always on hand to keep users productive
- Comprehensive tracking to make sure you’re always in control
- Full lifecycle provisioning ensures robust security from beginning to end

24 x 7 Mobility System Administration
Daily management of users and devices in your MDM system, including:

- Add/remove users and application of appropriate settings and policies
- Register/retire smartphones
- Theft/loss protection, including remote wipe, lock, and password resets

24 x 7 IT and End User Support

- Support via phone and email by certified Mobility Solutions Engineers
- Guaranteed Service Level Agreements ensure outstanding customer service and satisfaction
- Single point of contact for all mobility issues—device support, system administration, app support, and even carrier issues
- Feature and function support for corporate email, and PIM, calling, web browsing, security, synchronization, and selected application support
ABOUT DMI

DMI IS THE WORLD’S LEADING PROVIDER OF ENTERPRISE MOBILITY SERVICES AND SOLUTIONS.

We build enterprise class mobile solutions that generate results for the world’s top brands and businesses. Our mobile solutions combine the award-winning user experience design that has made us one of the top creators of consumer apps, with the deep middleware and engineering expertise that we’ve used to build and manage enterprise applications for the most demanding IT departments in the world. DMI mobility solutions improve business processes, tap new revenue streams, build customer loyalty, and increase employee productivity. And we offer a full range of Managed Services to securely set up, configure, and manage your mobile devices.

THE PROOF

- We’ve built more than 400 mobile apps—in the past 12 months alone—for more than 150 leading organizations like Disney, Coca-Cola, Toyota, Vodafone, P&G, The National Guard, and Universal Studios.

- We offer brilliant creative and user experience: Our mobile app development group was named the Best Branded App Developer at the 2012 Mobile Entertainment Awards.

- We have 500,000 devices under management for 100+ clients, including many Fortune 500 companies—like BP, Johnson & Johnson, Sears, The Associated Press, Allergan, and more. At BP, we’re deploying 1,000 managed mobile devices each day.

- We provide 24 x 7 x 365 mobile service support for more than 500,000 users. DMI is the one call our customers need to make to resolve any issue—devices, apps, infrastructure, even carriers.

- We offer a full range of security options that include Federal-grade hardware-based security, two-factor authentication, secure container, and sophisticated encryption solutions.

- With our expertise and economies of scale, we can provide mobility management at a higher service level and on average 20% lower cost than most companies can do on their own.

- Pervasive excellence is our commitment to quality service. DMI is one of only a handful of companies that is CMMI L3 appraised for both application development and services, as well as ISO 9001:2008, ISO 27001:2005, and ISO 20000-1:2011 certified. Our average D&B Open Ratings performance score from our clients is 94/100.