SOTI®

ENTERPRISE MOBILITY MANAGEMENT

skywire

White Paper

Mobile Security

Addressing the Evolving Threat Landscape

Today’s Enterprise is a Mobile Enterprise 2

Addressing an Evolving Threat Landscape 2

Toward a Holistic Mobile Security Approach 2

Physical Security 4

Network Security 4

Device Security 6

Data Security 10

Regulatory Compliance 12

Healthcare (HIPAA) 12

Education (CIPA) 13

Retail (PCI-DSS) 13

Government (FIPS 140-2) 15

Emerging Mobility 15

Wearable Technology 15

Smart Peripherals 15

Connected Smart Devices 15

Bringing It All Together 16

Today's Enterprise is a Mobile Enterprise

Mobile computing continues to expand throughout organizations to increase efficiency, empower collaboration, speed workflow, and boost employee productivity. The expansion of enterprise mobility across many organizations is having a transformative effect to their business and fueling product and service differentiation.

Mobility is no longer a "must-have" in the employee toolkit; it is as ubiquitous as a desktop computer. Once relegated to line of business and management use, mobility use continues to expand throughout many organizations as business units discover novel applications to drive their businesses forward. In many aspects, the rise of mobile devices, from smartphones, tablets, to smart peripherals and smart connected devices, is the most significant change to business workflow since the invention of the personal computer. Mobility is 'computing', as mobile devices have evolved from what we referred to as 'smartphones' to a powerful computer in everyone's pocket, where the phone is just another app.

With this evolution toward a mobilized enterprise, CIOs and IT organizations must ensure corporate security policies can accommodate the expansive mobile ecosystem – from form factors, to capabilities, operating systems, applications and communications protocols. As mobile is intrinsically woven into the fabric of enterprise, mobile security is less about protecting data and devices and more about protecting intellectual property, brand value, and customer trust. IT is tasked with a continual assessment of the changing threat landscape to ensure users are aware of risks and policies are created to mitigate those risks. The purpose of this white paper is to consider a holistic approach to mobile security that includes enterprise mobility management (EMM), and discusses best practices for securing mobility without diminishing the potential for mobile utility.

> "As mobile is intrinsically woven into the fabric of enterprise, mobile security is less about protecting data and devices and more about protecting intellectual property, brand value, and customer trust."

Addressing an Evolving Threat Landscape

The mobile threat landscape continues to evolve as hardware becomes more powerful and new applications and device capabilities continue to add additional security risks. Malware and spyware are becoming increasingly sophisticated, targeting mobile users as mobile messaging and social applications grow in use faster than email. Mobile form factors continue to expand to include wearable technologies and other smart peripheral devices, extending the data footprint inside today's enterprise.

Wearable technologies designed for consumer use, like other mobile technologies, will eventually find their way into the enterprise, and IT departments need to be prepared for the security and management challenges that are imminent. Wearable devices use communications technologies that are inherently insecure at the protocol level and require strong application level protection to prevent interception.

Users have embraced mobile apps as a part of their day-to-day responsibilities, and enterprises need to be assured that these mobile apps are authentic, aren't leaking sensitive data, and don't compromise the operation of the larger enterprise software and service infrastructure. Mobile apps have become a growing malware delivery mechanism, and no operating system is currently immune to attack. Mobile app security remains a significant challenge to many organizations, as apps are rushed into production without the necessary security controls in place, often because of lack of technical expertise, budget, or priority.

As critical business workflows migrate to mobile, security of data-at-rest and data-in-motion becomes more difficult to safeguard. The use of strong encryption and authentication policies, secure networking, data loss protection and user education are not enough. There is an underlying need to understand how users interact with new technologies, and to design security frameworks and controls that respect the user experience and the user's 'preferred way to work'. When IT makes it easier to follow the rules than to break them, users will follow the right path. The need to balance security with usability is one of the greatest challenges faced by enterprise today. We use technology to work differently, so we need to think about security differently.

> **There is an underlying need to understand how users interact with new technologies, and to design security frameworks and controls that respect the user experience and the user's 'preferred way to work'. When IT makes it easier to follow the rules than to break them, users will follow the right path.**

Moving Toward a Holistic Mobile Security Approach

Organizations that have made the decision to move forward with a mobile strategy need a holistic security framework to mitigate risk – taking into account physical, network, device, and data (app and content level) protection. The best security frameworks use a layered approach, and mobile security is no different. A holistic approach to mobile security that includes best practices for physical security, network security, device security, and data security is required. Best practices for complying with regulatory standards and guidance for emerging technologies that include wearable devices and connected smart devices, commonly classified under the Internet of Things (IoT), are also crucial elements of moving towards an all encompassing security approach.

Physical Security

Portability of business devices is an essential part of enterprise computing for corporations to reap the benefits of the 'always-on' workforce, allowing workers to work anywhere/anytime. Despite the need to physically protect mobile devices, employees still lose millions of devices each year, with over 1 million smartphones lost or stolen in the United States alone in 2014, according to the Federal Communications Commission[1]. Mobile devices are attractive targets to thieves, not only for the resale value of the device, but increasingly also for the data that may be perceived as greater value.

As organizations extend mobile deployments across lines of business, it is imperative that IT incorporates physical security into their policies. Traditional policies on physical security are equally applicable to mobile devices. Unlike a laptop device that can be tethered to a desk, a smartphone or tablet is usually not physically secured in a corporate setting. Physical security rests squarely with employees, who should be reminded regularly of the risks of leaving mobile devices unattended while at work or in public spaces. The best preventative measure against lost or stolen devices is to ensure users keep the devices in their periphery at all times. As business workflows begin to migrate to wearable devices, this requirement may diminish in importance.

Changes to the physical access of a mobile device can pose a serious security concern. When a device is lost or stolen, physical access to a mobile device changes from an authorized user to an unauthorized user. Safeguards must be put in place to ensure that if a change in physical access occurs, IT administrators can take appropriate action. At a minimum, IT must be alerted to the change in physical possession in order to determine the course of action, which can range from restricting access to corporate networks and services to locking the device to a complete wipe of all data on the device. On employee-owned devices, containerization with OS level segregation is an appropriate solution for protecting sensitive corporate content that can be locked or wiped independently of the employee's personal space. Deploying strong authentication policies and an out-of-contact policy for mobile devices will mitigate the risk of data loss if devices end up in the wrong hands.

> “Each year, 1 million smartphones are lost or stolen in the United States.”

Network Security

VPN – Device Wide, Container Level and App Level

Encrypted communication between a mobile device and the enterprise network is a critical component of a trusted computing strategy for organizations scaling mobility across their enterprise. Virtual Private Networking (VPN) remains the preferred method of tunneling data over an insecure public network, but it is important to differentiate mobile VPN strategies to determine which level of protection is appropriate.

Device-Wide VPN

Device-wide VPN, when enabled, routes all device communication over a VPN to the enterprise network infrastructure. All outgoing communications from the device are routed over a single VPN connection. Device-wide VPN is most often used in corporate-liable and mission-critical line of business applications where security is paramount. While device-wide VPN is still effective at protecting communication between the mobile device and the enterprise, newer models are now available to limit VPN bandwidth to only enterprise applications. Device-wide VPNs offer a less than desirable user experience by requiring users to manually connect. It is also less secure than container level or app level VPNs in that they allow any app on the device to access protected corporate resources.

Container Level VPN

Container level VPN allows IT administrators to provision a VPN connection to all enterprise applications in the secure device container on the device. Applications that reside within the container will use the VPN connection to communicate with the enterprise infrastructure. Enterprise mobile platforms such as Samsung KNOX and Google Android™ for Work make use of secure OS level partitions and container level VPN on the device to protect enterprise data. For BYOD deployments, container level VPN prevents a user's personal apps from using corporate resources, protecting bandwidth and a user's privacy.

App Level VPN

With an app level or "per-app" VPN, individual mobile applications can be provisioned with a VPN connection back to the enterprise infrastructure, protecting data in transit. App level VPN reduces the risk of data loss by eliminating data exposure to specific apps. It also allows IT greater control and is less prone to configuration error as VPN settings are embedded directly into the mobile app.

App level VPN doesn't require user intervention and can be mandated remotely by IT administrators through their EMM software. Enterprise apps use a VPN connection upon launch, while personal apps are routed over the public Internet, which protects corporate network resources and saves bandwidth. App level VPN is also a best practice in BYOD scenarios to provide secure access to corporate applications on employee-owned devices without compromising privacy.

Wi-Fi Connectivity

Wi-Fi® is a ubiquitous and necessary connectivity feature on all mobile devices. Wi-Fi use is expected to grow exponentially throughout the next 3-5 years as the use of mobility and connected smart devices expands throughout the enterprise.

Unsecured Wi-Fi connectivity is a major security risk for enterprises. Insecure access points heighten the probability of eavesdropping, man in the middle attacks (MITM), denial of service exploits, and theft of sensitive corporate data. The use of free public Wi-Fi, personal hotspot connections, and other untrusted and potentially insecure networks are all risks that need to be addressed at the mobile security policy level.

Enterprise Mobility Management (EMM) solutions can mandate that managed mobile devices connect exclusively through known secure access points in the enterprise, eliminating the possibility of eavesdropping or tampering on the corporate network. Wi-Fi whitelisting and blacklisting allows IT administrators to have a high degree of control over the wireless networks that users are allowed to connect to. Advanced security policies including disabling the use of personal hotspots, enforcing a minimum level of security (e.g. WPA), and network agnostic URL filtering allow organizations to minimize risk from network intrusion.

> **"Wi-Fi use is expected to grow exponentially throughout the next 3-5 years as the use of mobility and connected smart devices expands throughout the enterprise"**

Short Range Wireless Protocols (Bluetooth and NFC)

Bluetooth and Near Field Communication (NFC) are short-range communications protocols that are included on nearly every modern mobile device. Bluetooth is a convenient method for transferring files from device to device, and is widely used by mobile users to pair their device to other mobile devices, peripherals, and increasingly, wearable technologies like smart watches and fitness trackers. NFC is most widely used for mobile payments and to facilitate a data transfer session with another device. As the proliferation of mobile devices and smart connected technologies continues to grow within the enterprise, Bluetooth and NFC use is expected to grow significantly to support the growth of mobile computing and autonomous computing.

Bluetooth hacking (aka Bluesnarfing, Bluejacking) is a method of gaining access to a mobile device via its Bluetooth connection. A malicious third-party can use the mobile device's Bluetooth connection to gain access and potentially steal data, learn the IMEI of the device to redirect voice calls as well as perform other activities on the device. Mobile devices are, by default, configured in 'discoverable' mode, making it easy for devices to be discovered and paired with other devices. Like any other wireless networking technology, it can be used to gain access to devices and data at rest.

The NFC protocol can only be secured at the application level by implementing measures like credential authentication. Despite NFC being proximity driven, it is not immune from attack. Hackers can compromise NFC tags to gain access to an unsuspecting user's device to implant malware or steal user data. Users who leave NFC capabilities on by default on their mobile device are at risk from proximity attacks from any number of sources; from compromised tags on public transit and payment terminals to 'planted' tags disguised in high-traffic areas.

The original specification for NFC tags fell short of protecting the integrity of tag data. The NFC Forum, a non-profit industry association promoting NFC short-range wireless interaction, is in the process of updating their technical specification for Signature Record Type Definition (RTD) to provide increased security of NFC messaging used for communications between NFC-equipped mobile devices and tags. With the expansion of NFC tag applications across industries such as retail and healthcare, the integrity of tag data becomes a critical priority. The new RTD 2.0 standard is designed to ensure tag data is authentic.

EMM security policies can be configured to govern the use of Bluetooth and NFC capabilities on mobile devices. To prevent unauthorized access, administrators can restrict voice and data transfer over Bluetooth, control pairing with mobile devices and desktop computers as well as enforce parameters around Bluetooth discovery mode on the device. For example, Bluetooth voice and data transfer can be restricted for devices containing sensitive information, and pairing can be limited. The National Institute for Standards and Technology (NIST) Guide to Bluetooth Security has been widely recognized as the de-facto resource for best practices in securing Bluetooth devices.

Device Security

Device Kernel Authenticity

On certain mobile operating systems such as Android, verifying the integrity and authenticity of the device kernel is the appropriate defense against the installation of a compromised Android kernel that allows a sophisticated user to root the device and gain privileged access to device resources.

For highly regulated organizations considering using Android devices, verification of the authenticity of the device kernel is a critical security requirement. This will ensure the integrity of managed devices and prevent users from attempting to install custom firmware on the device.

An EMM solution should include support for device attestation to verify device kernel authenticity and flag any managed device that does not pass an attestation challenge. Based on the challenge, the device will return a 'verdict' indicating whether the device has been compromised. Policy controls can be automated to perform specific actions if a compromised device is detected – from rescinding access to the secure corporate network to wiping data in a container.

OS Privilege Escalation

Jailbreaking (on iOS) and rooting (on Android) are two methods by which users gain low-level access and permissions to the mobile operating system. Jailbreaking and rooting are both forms of privilege escalation allowing the user to gain access to the root file system on the device. Privilege escalation occurs when a loophole or design flaw in an operating system is exploited to gain a privileged level of access to the operating system's resources – including core file system – that is normally not available to the user.

Jailbreaking an iOS device allows users to download and install applications that may not adhere to Apple's comprehensive application development standards for optimization and hardware resource use. This can have an adverse impact on corporate-liable devices ranging from hardware instability and performance issues to 'bricking' the device. Jailbreaking also allows users to unlock their device from carrier restrictions, enabling them to use their device on other carrier networks.

Rooting allows users to gain privileged access (aka 'root' access) to the subsystems on their Android device, including the core file system. Through the process of rooting, users can remove restrictions imposed on the Android device by carriers and hardware manufacturers. This can allow the user to alter or replace native Android system applications, run unsanctioned applications on the device, and perform a myriad of operations that were never intended to be exposed to the typical Android user including the manipulation of system files and hardware capabilities on the device. Unlike jailbreaking on an iOS device, rooting allows the user to completely remove the Android OS on the device and replace it with a version of the OS that may not have been optimized for use by either the wireless operator or the device manufacturer.

Both jailbreaking and rooting can compromise the stability and integrity of the mobile operating system. This can have an adverse impact on core device operation including battery life, cellular communication, and user interface responsiveness.

It is critical to continually scan for jailbroken/rooted devices and have automated policies in place to mitigate the risk. Once a jailbroken or rooted device is detected in the system, IT administrators can take appropriate action to limit the device's exposure to protected corporate resources including email servers, document management systems, and corporate file shares.

User Authentication

Mobile Certificate Management

Certificates are a critical element in establishing trusted enterprise mobile computing. Certificates offer a greater level of protection than passwords, which are subject to brute force attacks, social engineering, and employee misuse. Certificates are used to authenticate mobile devices and ensure that only authorized users have access to company resources including email, applications, content, and secure VPN connectivity.

EMM solutions help IT administrators manage the deployment, renewal, and revocation of mobile certificates on managed devices. Certificates are deployed silently to the end-user during device enrollment, and can be issued per device, group, or corporate-wide. Certificate renewal can also be automated to reduce administration overhead and enforce a consistent level of security. For example, flexible certificate templates allow IT administrators the ability to deploy certificates dynamically to users or devices.

EMM simplifies certificate management from leading cloud-based and on-premise Certificate Authorities including Microsoft Active Directory Certificate Services (ADCS), Entrust, and Simple Certificate Enrollment Protocol (SCEP). SCEP simplifies the deployment of certificates by standardizing the certificate request process, allowing organizations to deploy security certificates at scale.

Passcode and PIN Authentication

Users often choose non-complex passwords or PINs to restrict access to their mobile devices, opting for convenience at the expense of security. Popular passcodes include birthdays, anniversaries, or numeric patterns like 0000 or 1234. While convenient to the user, simple passwords are easily determined by someone in possession of the device, increasing the risk that sensitive data can be accessed by a third-party in the event that a device is lost or stolen.

Non-complex passwords make it easier for a malicious third-party to correctly guess the password on the mobile device and gain access to sensitive information that is stored at rest. Hackers can employ brute force hacking devices, available online for a few hundred dollars, to successfully gain access to password protected mobile devices in hours. In a recent example, a device with a 4-digit passcode could be guessed in a maximum of 4.5 days, assuming the brute force device needed to go through all 10,000 combinations. In comparison, a 7-digit password would take considerably longer to brute force, up to 12 years to potentially go through all 10 million combinations[2].

It is critical to enforce authentication security policies to ensure the composition of device passcodes. Mobile device passcodes must align with corporate standards for device authentication, including the quality and length of the passcode, the use of complex characters, granular password aging and re-use policies, screen lock durations, as well as failed password policies.

> “A device with a 4-digit passcode could be guessed in a maximum of 4.5 days.
>
> In comparison, a 7-digit password would take considerably longer to brute force, up to 12 years.”

Third Party App Stores

Third-party app stores contain collections of applications and games that are downloadable directly to a user's mobile device, independent of the officially supported app stores from Apple and Google. Third-party app stores exist for all mobile platforms, but are most popular with Android users. iOS devices must be jailbroken to allow installation of third-party applications. Android devices don't have this restriction because of a less restrictive security architecture that allows users to install Android applications from untrusted sources.

Unlike the Apple App Store or Google Play, third-party app stores do not guarantee the safety or integrity of applications that are offered, forcing the user to download 'at their own risk'. The onus is on the user to determine whether an application is safe to download and use. Malicious apps are often packaged as legitimate apps, and are indistinguishable from the legitimate app. The implications of using third-party apps can be severe. Hackers can disguise spyware and malware as legitimate apps to gain access to data on the device, compromising the privacy and security of both the user and the organization.

When evaluating EMM, it's critical to look for solutions that provide full application lifecycle management to mitigate the end-user's exposure to untrusted applications. Through an enterprise app catalog or managed container, IT administrators can provide employees with a curated set of secure enterprise applications for download. Application policy controls including whitelisting and blacklisting give IT administrators the tools to govern which applications to permit and restrict on devices, groups, or enterprise-wide.

Application Sideloading

Sideloading is the act of transferring files between two local devices over a physical connection. On the Android OS, sideloading involves the installation of an application in APK format on an Android device from a location other than Google Play. Applications can be side loaded using a variety of methods, the most popular of which include direct USB connection between a computer and a mobile device, over a Bluetooth connection, or by using removal storage media such as an SD card.

In order to allow sideloading, users have to configure their device to download and install applications from unknown services through the security settings on the device. Sideloading circumvents the native application store on the device by allowing a user to install the Android app APK directly to the device. Users can often find APK files on file sharing sites, which are a known haven for malware and spyware distribution.

It is a best practice to enforce policies through EMM that restrict sideloading by disabling the user's ability to install applications from unknown sources. On Android for example, an applicable policy would ensure that all applications are installed from either an enterprise app catalog on the device or through a trusted source like Google Play.

Data Security

Email and Content Forwarding

Mobile devices have always been used for personal and business use. Corporate email accounts have long been used to send personal emails to a spouse or a friend, and personal email accounts have been used to forward sensitive corporate information to accounts outside the corporate firewall.

Fast forward to today, and the stakes are even higher. Mobile devices come equipped with cloud-connected storage available out of the box, and it is increasingly common to see these capabilities integrated into the operating system. The proliferation of free cross-platform messaging apps poses a risk to sensitive corporate data by making it incredibly easy for employees to instantly forward information to another user anywhere around the globe.

Without the appropriate safeguards in place, users are able to easily forward sensitive corporate content including messaging and files to personal email accounts or cloud storage providers from an unsecured device. A best practice is to employ data loss prevention (DLP) capabilities to keep sensitive corporate data from leaving the organization. Ensure your EMM has OS agnostic content management policies that can control which applications are allowed to open documents from an enterprise domain.

Recording Hardware Features (Camera, Microphone)

Cameras and microphones are standard features on all modern mobile devices, regardless of operating system, form factor, or price point. The recording capabilities on mobile devices are widely used in the enterprise to help mobile users with their day to day responsibilities – by enabling users to capture whiteboard drawings, record voice notes, and dictate email communications. Although recording capabilities are very useful for enterprise use, in certain highly regulated or high-security use cases, it may be necessary to prohibit or restrict their use.

Enterprise IT, at a minimum, needs the capability to provision device policies that restrict recording capabilities via the camera or microphone or enable them only in certain circumstances or locations. For example, a location-based policy could be created to prohibit recording capabilities in an organization’s testing labs, but allow the same capabilities in the corporate office. Similarly, within the same building, location-based policies could be used to permit or restrict access to corporate data based on the access point that devices are attached to.

Operator SMS/MMS

Despite the growth of over-the-top (OTT) messaging use on mobile devices, operator SMS/MMS communications remain one of the most widely used data applications. Each day, 20 billion SMS messages are sent across the world's wireless networks[3]. Enterprise use of SMS/MMS messaging is widespread and often used as an informal communications channel within the workplace. SMS is also used to send automated notifications to subscribers and emergency notifications. There is also an increased use of two-factor authentication for many popular web services that relies on SMS to deliver temporary authentication codes.

Unlike Wi-Fi that can be managed directly from the corporate network, cellular communications are outside the governance of the corporate IT department. Employees can easily transfer corporate data via SMS and often informally use this as a way to communicate internally. Hackers routinely deploy SMS phishing attacks by sending an SMS that encourages a user to click a URL for a free prize or even an emergency notification. Once the user clicks the URL, malware is downloaded to the device, allowing a third-party to take control over the mobile device.

In many ways, the best defense against SMS based attacks is to ensure corporate users remain vigilant and refrain from clicking on a URL that is unrecognized or unsolicited. For the most stringent security models, EMM software can disable incoming or outgoing SMS/MMS messaging on managed devices.

20 billion SMS messages are sent across the world's wireless networks

Regulatory Compliance

Security – for users, for enterprises, and for the protection of the public – is at the heart of many of today's regulatory frameworks, impacting security strategies for mobile computing in many organizations. Highly regulated organizations in industry sectors such as healthcare, retail, education, and government require advanced security, privacy, and audit tools to ensure compliance.

Healthcare (HIPAA)

In the United States, the Health Insurance Portability and Accountability Act (HIPAA) sets out policies and regulations to ensure the privacy and security of personally identifiable health data. HIPAA requires healthcare providers to abide by policies and procedures that govern the privacy of individually identifiable health information. Most countries around the world have similar or even more restrictive standards and legislation in place to protect the confidentiality of patient data. Healthcare providers are continually challenged with balancing the demands of regulatory requirements with the need to take advantage of the latest innovations to increase patient care and drive down costs.

The use of mobile devices continues to accelerate throughout healthcare, both on the practitioner side and patient side, to improve the standard of care overall. On the practitioner side, mobile technologies are being used to speed diagnosis, provide timely distribution of information directly to the point of care, and streamline workflows for healthcare workers dealing with an increase in health services from an aging population. On the patient side, individuals are using mobile devices to become more involved in managing healthy lifestyles and are interfacing with healthcare providers through mobile applications and wearable technologies that contain a wealth of personally identifiable health data. Healthcare providers are beginning to see the benefits of this data for diagnostics and treatment purposes.

Healthcare providers are also allowing practitioners to bring their own devices (BYOD) to use in clinical settings, and are continually evaluating security policies to ensure that the privacy and security of patient data is not compromised. The protection of personally identifiable patient data is critical to healthcare providers and practitioners who could be subject to significant fines and penalties for breaches of privacy and security that cause them to be HIPAA non-compliant. EMM can solve the problem by governing the use of mobile device policies to protect the privacy and security of data. Healthcare providers can deploy mobile devices securely throughout their organization with the following safeguards to help them keep HIPAA compliant:

Application Management – Mandate the use of corporate applications through the enterprise app catalog

Secure Networking – Mandate the use of VPN device-wide or on a per-app basis

Data Loss Prevention Controls – Secure content management with selective lock and wipe capabilities

Strong Encryption – Mandate the use of strong encryption across managed mobile devices to ensure data is protected in the event a device is lost or stolen

Strong Authentication – Enforce strong user authentication protocols including passcode complexity and passcode aging policies

Physical Control – Remotely lock or wipe devices to ensure data is protected

Location-Based Services – Invoke security policies through geofencing

URL Filtering - Whitelist and blacklist URLs to protect users from malware and spyware

Real-time Antivirus and Malware Protection – Actively schedule antivirus and malware detection and remediation to protect the integrity of mobile devices

Kiosk Mode – Ensures devices are used for mission critical clinical and point of care applications and services

Education (CIPA)

The Children's Internet Protection Act (CIPA) requires that K-12 schools and libraries in the United States use web filtering and related security measures to protect children from viewing objectionable and harmful online content as a condition for federal funding. To comply with CIPA legislation, educational institutions must meet four criteria:

- A technology protection measure
- An internet safety policy
- An education program
- A policy to monitor the use of technology by students

EMM can help educational institutions meet CIPA guidelines through the following features:

- Secure Browser – Allows students to experience the best of the educational Internet without access to objectionable content
- Web Filtering – Allows IT administrators to filter URLs based on categories or by using whitelists and blacklists
- Kiosk Mode – Mandates a subset of applications for student use, protecting students from downloading objectionable content or applications
- Geofencing and geolocation policies – Uses location to determine applicable device policies, including URL filtering and application availability

Retail (PCI-DSS)

The Payment Card Industry Data Security Standard (PCI DSS) is an information security standard for organizations that handle branded credit cards from the major card schemes including Visa, MasterCard, American Express, Discover, and JCB. The standard was created to increase controls around cardholder data to reduce credit card fraud.

As retailers expand the use of mobility across their operations, smartphones and tablets are used increasingly for accepting payments in retail locations. Mobile devices used as Point of Sale terminals (POS) to accept payments must adhere to the PCI-DSS standard to protect customer data.

EMM helps retailers adhere to the PCI-DSS standard by providing features that help retailers meet the requirements mandated by the PCI Mobile Payment Acceptance Security Guidelines, "Guidance for Securing the Mobile Device".

Step 1: Secure Device Access

Prevent unauthorized physical and logical device access

Step 2: Protect Against Malware

Protect the mobile device from malware

Step 3: Maintain Security

Ensure the mobile device is in a secure state

Step 4: Govern Device Functionality

Disable unnecessary device functions

Step 5: Migration Loss/ Theft

Detect device loss or theft

1. Secure Device Access – Prevent unauthorized physical and logical device access with the ability to:
- Configure a complex password policy with full complexity and aging controls
- Mandate full device encryption to protect data at rest
- Mandate user re-authentication at a specific interval to maintain authorized use
- Deploy location-based services and geofencing policies to ensure the correct security policies are applied based on location context

2. Protect Against Malware – Protect the mobile device from spyware and malware by:
- Using scheduling and quarantine features to offer real-time malware protection and remediation
- Introducing device rooting and jailbreak detection
- Application whitelisting and blacklisting to enforce installation of ‘trusted’ applications only
- Silently deploying security policies and applications to mobile endpoints

3. Maintain Security – Ensure the mobile device is in a secure state by:
- Ensuring that native device security controls are intact through rooting and jailbreaking detection
- Disabling USB debug mode on the device
- Invoking real-time malware and antivirus remediation policies to scan before implementation and during device service
- Alerting IT administrators when the secure state of a device has been comprised

4. Govern Device Functionality – Secure the use of mobile devices with the ability to:
- Provision devices in ‘Kiosk’ mode with only essential applications and services (e.g. POS software)
- Implement robust device hardware and software policies (e.g. disable camera, disable screen capture)
- Enforce trusted communications (e.g. disable cellular radio, mandate trusted Wi-Fi connection, mandate VPN connection)
- Employ application whitelisting and blacklisting (disable IM and social media applications)

5. Mitigate Loss/Theft – Allow organizations to protect themselves against loss or theft of devices with the ability to:
- Manage assets in real-time with device monitoring and diagnostics tools
- Enforce out-of-contact policies
- Mandate location-based policies including geofencing and geolocation policies
- Employ a periodic authentication policy
- Enforce complex passcode protection and mandate device encryption
- Use Remote Control to recover device
- Remotely lock and wipe device

Government (FIPS 140-2)

The Federal Information Processing Standard (FIPS) Publication 140-2 is a US government computer security standard used to accredit cryptographic modules. FIPS 140-2 accreditation for cryptographic modules is required for federal government use.

An EMM solution with policy-based file encryption that uses FIPS 140-2 validated AES-256 encryption algorithms to secure mobile data is recommended. On-the-fly file encryption should be implemented easily and transparently without affecting the end users' experience and allows data to be encrypted and decrypted in memory when needed by mobile applications on the device.

Emerging Mobility

Wearable Technology

Wearable technologies are the next logical evolution of computing, making the experience more personal, more convenient, and more immediate. Consumer wearable technologies generally depend on Bluetooth and NFC communications to transmit data, and both protocols will need to be hardened for enterprise use. Enterprise-grade wearable technologies will emerge in the coming years to serve line of business needs in sectors such as manufacturing, healthcare, logistics, and field service, with enhanced capabilities and hardened security.

Smart Peripherals

With mobility maturing into the new computing platform for the enterprise, the demand for smart peripherals – connected printers, scanners, and projectors – is on the increase as the last mile of enterprise mobile computing. Deployments of smart peripherals are expanding in areas such as healthcare and retail as workflows migrate to mobile, and use cases range from mobile receipt, patient identification, and mobile ticketing.

Smart peripherals are a growing pain point for IT departments that are tasked with securing mobility across their organization. Many use cases involve the handling of sensitive financial and personally identifiable information, making it necessary to comply with regulatory requirements such as HIPAA and PCI-DSS. As the use of smart peripherals expands, enterprise IT will need to adapt security policies to include the use of smart peripherals, and will need to ensure that their EMM solution, for example, is capable of securing the devices that govern the last mile of mobile workflows.

Connected Smart Devices

Connected smart devices have become popular in the consumer world. Thermostats, refrigerators, and even household lighting are all now offered as a connected smart device, capable of connecting to the internet and being controlled remotely from anywhere in the world on a mobile device. In the enterprise, connected smart devices running mobile operating systems are in their infancy, but will soon become a part of the fabric of the Internet of Things (IoT). Authentication and security of connected smart devices will become a critical requirement as autonomous devices are increasingly deployed for line of business applications.

Bringing It All Together

Mobile security is a legitimate challenge to many enterprises expanding the use of mobility throughout their organizations. A mobile computing environment is made up of many diverse technologies – wireless interfaces, network infrastructure, enterprise mobility management, and security technologies. A holistic approach to mobile security considers each variable as a part of a larger security framework, with an emphasis on how technologies are layered to protect not only enterprise data, but also user privacy and security.

Many organizations make the mistake of assuming enterprise mobility is secured by technology alone, but it is important to remember that the security measures are built by humans, and can be defeated by humans with the right resources, access, and knowledge. Consider the human element of mobile security when designing a holistic approach — users will be happy to follow the rules if security is implemented with regard to the overall user experience.

In addition to a robust EMM solution, the best security strategies should actively involve the users in the process. By educating the users on best practices and acceptable use of mobile technologies, organizations can limit their exposure to risk and maintain a culture of vigilance. A key tenet of this practice is to consider the user in every aspect of designing a mobile security strategy, particularly in areas where a user has the choice to act in a secure manner or use shadow IT.

SOTI MobiControl can help your organization move forward with a holistic mobile security approach by securing device, data, connectivity, and applications with a unified, device agnostic policy framework. Leading organizations are using SOTI MobiControl to not only protect their existing investments in mobile technology across corporate-liable, BYOD, and line-of-business use, but as a platform for transformation that integrates emerging connected technologies to differentiate their business.

SOTI is a proven product innovator and EMM Industry leader. Over 16,000 customers across 170 countries rely on SOTI for their EMM needs. We empower the enterprise to take mobility to endless possibilities.

SOTI.net

[1] Report of Technological Advisory Council (TAC) Subcommittee on Mobile Device Theft Prevention (MDTP), December 2014 http://transition.fcc.gov/bureaus/oet/tac/tacdocs/meeting12414/TAC-MDTP-Report-v1.0-FINAL-TAC-version.pdf [2] Luke Dormehl. “This brute-force device can crack any iPhone’s PIN code,” http://www.cultofmac.com/316532/this-brute-force-device-can-crack-any-iphones-pin-code [3] Ben Evans. “WhatsApp sails past SMS, but where does messaging go next?,” http://ben-evans.com/benedictevans/2015/1/11/whatsapp-sails-past-sms-but-where-does-messaging-go-next