Security for Moving Targets: BYOD Changes the Game

Mobiles devices of all shapes and sizes are entering the enterprise at an alarming rate. Smart-watches, wearable devices, tablets and, of course, beloved smartphones. The Bring Your Own Device (BYOD) mantra has morphed from a movement into business-as-usual for a growing majority (40%) of enterprises, according to Gartner. IT Security Administrators are struggling to adopt best practices quickly for protecting this new world of moving targets.

CIOs and CISOs are challenged to develop corporate policies that embrace BYOD – without falling short on security. The complexity requires striking a balance between the user's desired expectations (flexible experience, privacy, and instant data access) and the organization's need to secure corporate data, protect against insider threats and comply with corporate governance initiatives.

However, simply treating mobile devices as an extension of an endpoint strategy will fall far short. Existing security solutions designed for the desktop lack visibility to mobile traffic and are easily compromised by targeted mobile attacks. First-generation mobile management solutions are designed to control access to data and systems, not to secure against outsider threats.

This paper will take a look back at the BYOD movement and provide a framework for enterprises who are struggling to adopt mobile security best practices. We'll explore:

- Top risks BYOD brings to the enterprise today
- What to consider when planning and designing for BYOD
- Current mobile security solutions available today

BYOD – How Four Letters Changed Everything

Mobile users today expect full corporate privileges on privately paid personal devices, including the freedom to work anywhere, anytime. Mobile devices bring new capabilities to the market that enterprises race to adopt – without always considering the security implications.

IT departments today need to:

- Keep employees mobile, satisfied and productive
- Manage and secure an explosion of WiFi and cellular enabled devices and smartphones
- Devise policies for device and user eligibility, roll-out, cost sharing, security, and support
- Stop non-compliant/jailbroken devices from connecting to the corporate network/services (email/VPN/WiFi)
- Control who has access to corporate data and where data is transmitted
- Secure mobile devices against cyberattacks that can steal corporate data
- Enable collaboration tools that promote productivity: secure file sharing, sync capabilities and freedom to work on the go
- Respect a user's right to privacy

According to principal research analyst at Gartner, Amanda Sabia,

"The lines between work and play are becoming more and more blurred as employees choose to 'use their own device' for work purposes whether sanctioned by an employer or not. Devices that were once bought purely for personal use are increasingly being used for work and technology vendors and service providers need to respond to this."

Top Risks for the Enterprise

While the risks are many, organizations need to ensure they don't over-engineer their BYOD initiatives either. There's no way to securely protect every mobile device in a BYOD or a corporate issued environment all of the time. Enterprises invest in solutions to mitigate risk by enforcing policies to control data access, prevent non-compliant devices from accessing corporate services (email, apps, data, VPN, WiFi) and stop compromised devices from infecting other devices, and in turn the corporate network.

Organizations are not investing the same amount of time and energy to prevent against the silent killer – invisible attacks on employees' mobile devices. How much damage can one compromised mobile device achieve? The short answer: A lot. With a single attack, a hacker can wreak havoc on the enterprise. A true mobile security solution must not only guard against the insider threats – it must have the ability to detect and protect against cyberattacks designed to access sensitive business assets including:

- Emails, apps and data containing PII, corporate IP or healthcare information
- Critical business systems: Customer Relationship Management (CRM), Enterprise Resource Planning (ERP), Electronic Health Records (EHR), and more
- Corporate IP, patents, M&A plans, financial results

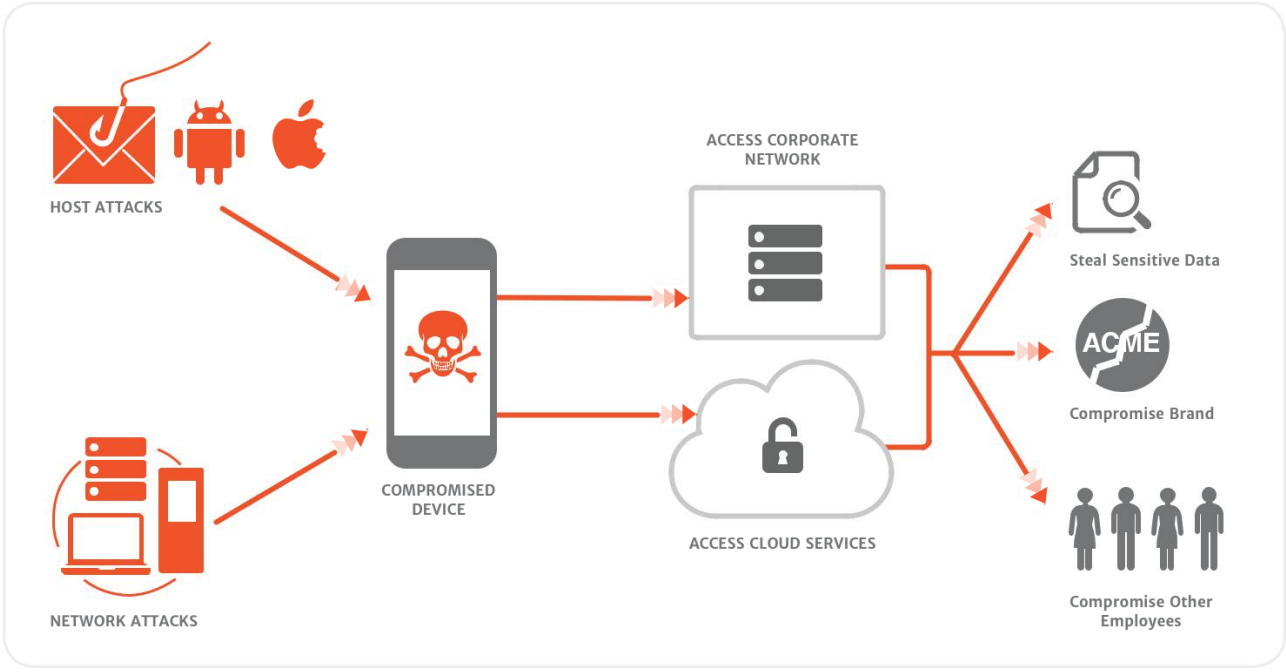


Figure 1. Nature of security threats

Now that we have identified the risks, let's examine the most widely deployed options utilized today by Fortune 500 companies. By reviewing each piece of the mobile management puzzle we'll be able to determine what's missing and what solutions enterprises need to adopt as part of their 2015 Mobile Security Best Practices. A complete mobile security solution will provide protection against host and network based threats, while providing a way to manage a fleet of mobile devices across the organization.

Designing and Planning for BYOD

The sophistication and continuous evolution of mobile threats is a serious problem for modern enterprises. Mobile malware, malicious apps, and targeted attacks on iOS and Android devices are introducing new challenges for IT security that a mobile device management solution can't protect against. Advanced techniques, such as polymorphic engines or runtime binary encryption, can easily evade traditional signature-based security methods like Mobile AV and compromise a mobile device.

Malicious attacks combined with unpredictable user behavior, jailbreaking devices, and increased reliance on WiFi networks introduce new security challenges that require IT Administrators to think outside the PC box.

According to a recent Mobile Security report published by Information Security, the key drivers for BYOD are about keeping employees mobile (57%), satisfied (56%) and productive (54%).

The Bring Your Own Device (BYOD) trend among organizations has led to a significant rise in the collaboration of data on mobile devices. This data travels between organizations to mobile devices across WiFi and cellular networks and back again. This data in transit is vulnerable to cyberattacks, threats, and loss. Many solutions (Mobile Content Management/Mobile Device Management/Mobile App Management) emerged to manage insider threats and provide secure access to corporate data across email, Intranet, Corporate WiFi, VPN and line of business apps. As cyberattacks on mobile devices increased, organizations recognized the need to complement these solutions with protection against malicious cyberattacks aimed at compromising the device and in turn jeopardizing the corporate network.

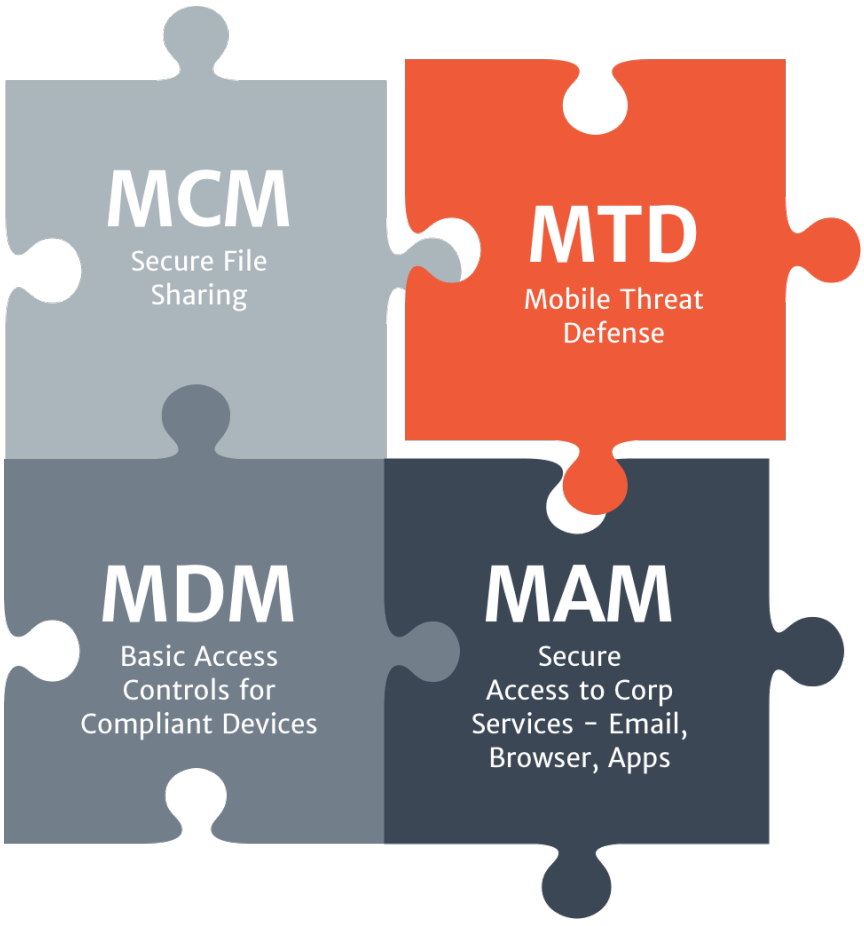


Figure 2. The Current Landscape

Mobile Device Management: Basic Controls for Compliant Devices

Mobile device management was just the beginning. It proved to be a safe bet, a way to dip a toe into the pond of mobile management. It was a brave attempt to control a sea of workers insistent on using their own mobile devices whenever and wherever they liked – for work and play – in the name of productivity!

Many organizations rely on Mobile Device Management (MDM) solutions to monitor and manage a fleet of mobile devices within their organization. MDM solutions do offer a reliable and trustworthy way to grant access to compliant mobile devices to connect to the corporate services such as email, VPN, WiFi and line-of-business apps. Perhaps their biggest advantage is their ability to enroll devices in an enterprise environment quickly, configure and update device settings over-the-air, and provide basic device security – like pin-code enforcement, remote lock and wipe, and compliance enforcement. MDM solutions provide a secure way to access corporate data on mobile devices and control against the insider threat.

However, solely relying on MDM for complete mobile security will not protect BYOD or corporate-issued mobile devices against cyberattacks such as mobile spear-phishing, malicious apps and Man-in-the-Middle attacks. Why? MDM solutions are not designed to look for security threats. If a mobile device is attacked unknowingly, and then successfully connects back to the corporate network, the compromised device will put the organization and its sensitive IP at risk. As MDM gives birth to Enterprise Mobility Management (EMM,) the security challenges remain the same. EMM will enable IT Administrators to manage devices, applications and content, but EMM still does not close the door for hackers.

Mobile App Management: Secure Access to Corporate Services (Email, Browser, Apps)

Many MDM vendors have added mobile app management (MAM) features in an attempt to separate business data from personal data residing on the same mobile device. Whether it be a strict persona approach that has a separate container for all business apps or an "app-wrapping" approach that creates a container around each app, both methods are subject to compromise by cyberattacks.

While MAMs are useful in remotely installing, updating, removing, auditing and monitoring software programs installed on mobile devices, they leave the data-at-rest on the device open to cyberattacks. Thus, if the device itself is compromised via a root or kernel exploit, the data on the device would be at risk.

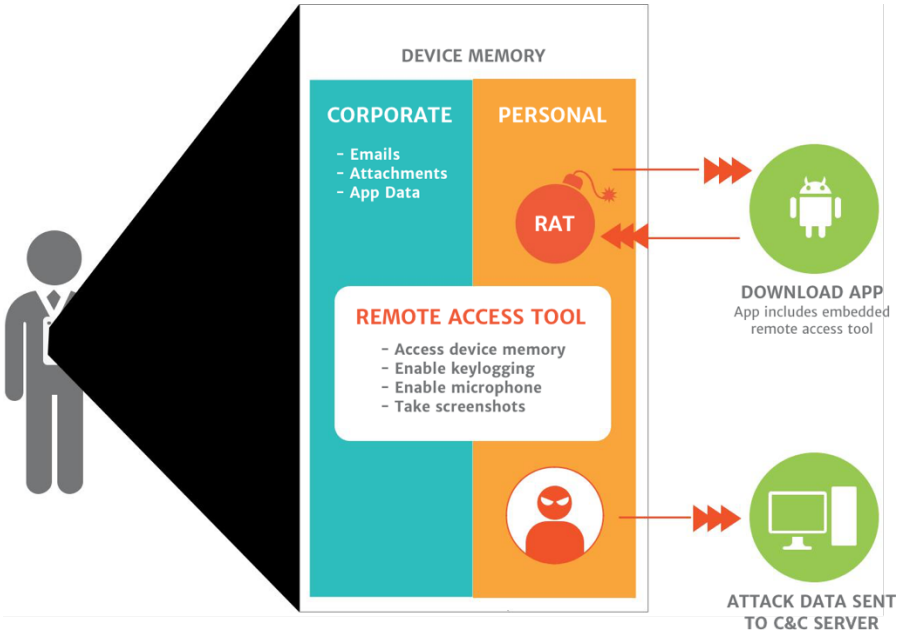


Figure 3. The Current Landscape

For example, a user could download a malicious app or malware from the native browser on the personal side of the device, enabling a cybercriminal to gain root privileges over the device. Once compromised, the cybercriminal can elevate privileges and take complete control of the mobile device. This type of attack not only poses risks to the personal and corporate information stored on the device, but also exposes the corporate network and corporate services the device is authorized to connect to.

All mobile apps need to communicate frequently with a server to complete updates and receive instructions from third party systems. With this type of architecture, employees open themselves up to download and execute attacks (e.g. Time-bombs).

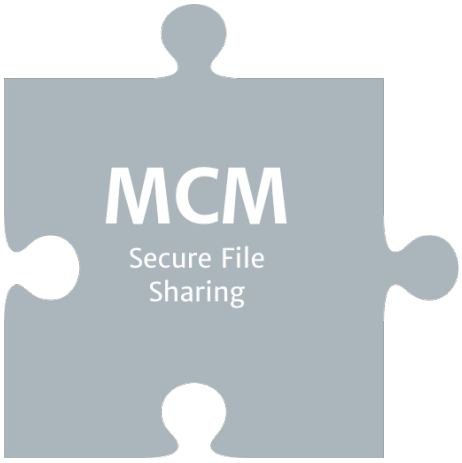
It's simply the nature of the beast for every mobile app on the market today.

Today, enterprises possess a false sense of security that app reputation will keep their employees safe and protected from mobile malware for two reasons: 1) employees can prevent the installation of the app and 2) employees can remove malicious apps. Both preconceptions are untrue. Due to the "rules" of a mobile device, the enterprise cannot remove an app they did not directly deliver to the device. Since most malicious apps originate from public app stores, there is little organizations can do to prevent an employee from downloading a malicious app. In addition, once the app is detected as malicious, simply removing the app will not remove the risk if the attacker has already elevated privileges on the device.

If the malicious app is not caught before it is installed, an organization can protect against this type of attack technique by temporarily preventing the compromised device from connecting to corporate services (via MDM enterprise wipe). In addition the device should be reset to factory defaults before allowing it back on to the corporate network.

Mobile Content Management: Secure File Sharing

Mobile Content Management systems were developed to solve yet another challenge mobile devices pose to organizations – how to securely store, control and deliver content to employees on their mobile devices. Mobile content, unlike content generated for PCs, has unique constraints including not only the screen size of the device but the security, ownership, storage capacity and comparatively weak processors.



Mobile content management (MCM) providers contribute a valuable piece of the mobile security puzzle by providing employees with access to corporate content on-the-go. Features include: secure file sharing services, file synchronization and sharing services to access sensitive data, to minimize risks to corporate data. MCM provides peace of mind for IT by essentially creating a corporate container for employees to securely access, store and update information from the device of their choice.

This also enables IT Administrators to have more confidence letting their employees use enterprise grade synch and share products to exchange content and improve productivity on the go - so they don't resort to non-secure products like DropBox.

MCM features, like MAM features, are largely getting absorbed into Enterprise Mobile Management (EMM) solutions. While these solutions offer a good "mobile DLP solution" that provides a compliant vehicle for employees to send and receive data - they do little to protect against malicious attacks occurring on the device itself. Just like the security gaps in MDM solutions, mobile content management products are vulnerable to the malicious attacker who preys on mobile devices as they roam from freely on publicly available WiFi networks.

The Mobile Security Gap – Protection against cyberattacks

Businesses need to think about expanding their BYOD initiatives to go beyond management of devices and controlling data access to protecting against cyberattacks.

The recent and very visible attacks on JP Morgan Chase, The Home Depot, Sony Pictures and now Anthem are headline news. Millions of credit cards, private information, corporate secrets and medical information has been disclosed. Cybercriminals pose a very real and present danger to enterprises. Failure to secure against these malicious attacks is like leaving the front door open to an organization's corporate network.

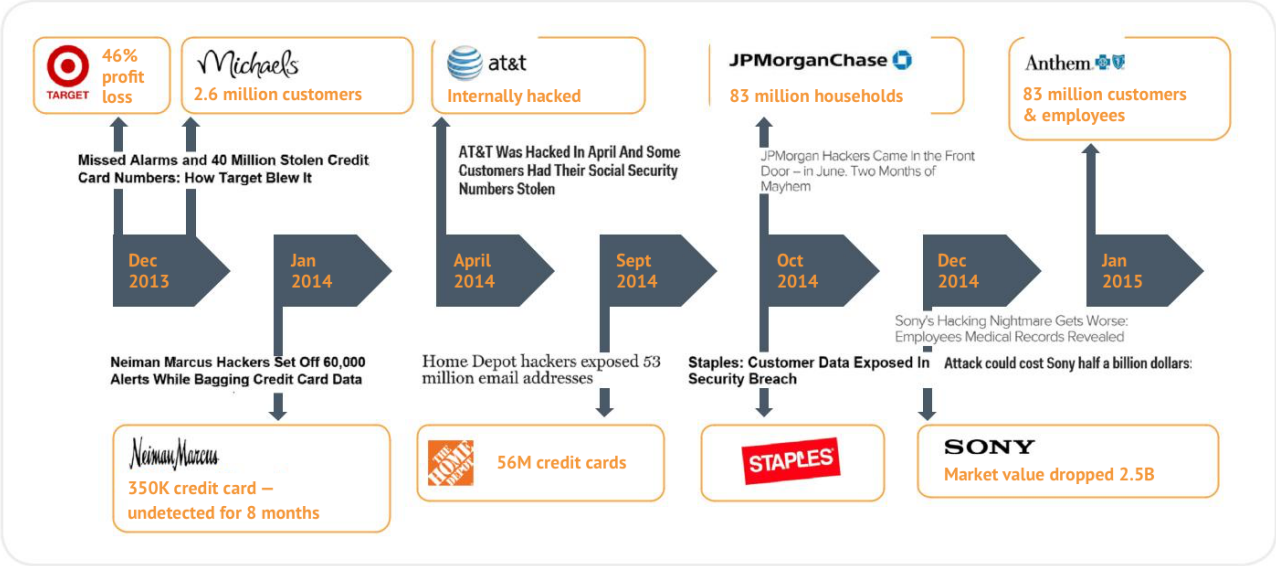


Figure 4. Visible Cyberattacks Are Headline News

Existing security solutions designed for the desktop lack visibility to mobile traffic - making it close to impossible to report against these very real attacks. One single compromised device can lead to a major outbreak as witnessed with Heartbleed, TowelRoot, Shellshock and more.

According to Cisco Visual Networking Index, by the end of 2014, the number of mobile-connected devices will exceed the number of people on earth, and by 2019 there will be nearly 1.5 mobile devices per capita. There will be 11.5 billion mobile-connected devices by 2019, including M2M modules—exceeding the world's projected population at that time (7.6 billion).

That's a huge, unprotected target for hackers to exploit.

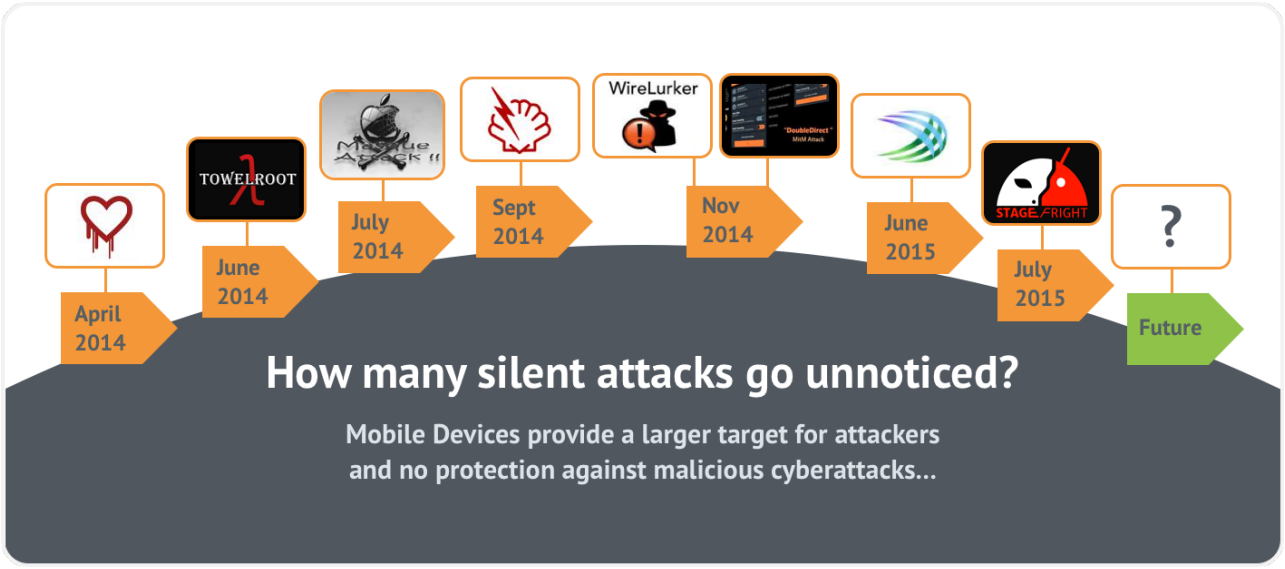


Figure 5. Mobile Attacks Are Increasing in Frequency

Zimperium recently developed a revolutionary mobile security system that provides complete enterprise protection against sophisticated network and host based threats for both iOS and Android devices. It is the only mobile threat defense system capable of monitoring processes outside of its own sandbox. Zimperium utilizes an on-device, behavior-based detection engine to continuously monitor and secure the entire device for malicious behavior (rather than just scanning apps at a single point in time) without introducing latency.

Managing Insider and Outsider Threats – Together

Zimperium has partnered with leading MDM/EMM providers to deliver a complete enterprise mobile security system that delivers unmatched threat detection and protection for mobile devices. The integrated solution secures devices against known and unknown threats to ensure corporate data, and networks are not compromised by a mobile attack. These integrated solutions enable enterprises to secure, monitor and manage a broad range of mobile platforms against host and network attacks. Together they enact risk-based policies to prevent a single device from compromising the enterprise.

Zimperium provides IT Security Administrators with a way to safely enable BYOD and strike the balance between empowering mobile employees to be more productive with the device of their choice, while at the same time securing mobile devices against advanced threats. Zimperium continuously detects threats and provides unmatched visibility to mobile security incidents both on and off the corporate network. This non-intrusive solution provides complete protection around the clock without impacting the user experience, violating user privacy or draining the battery.

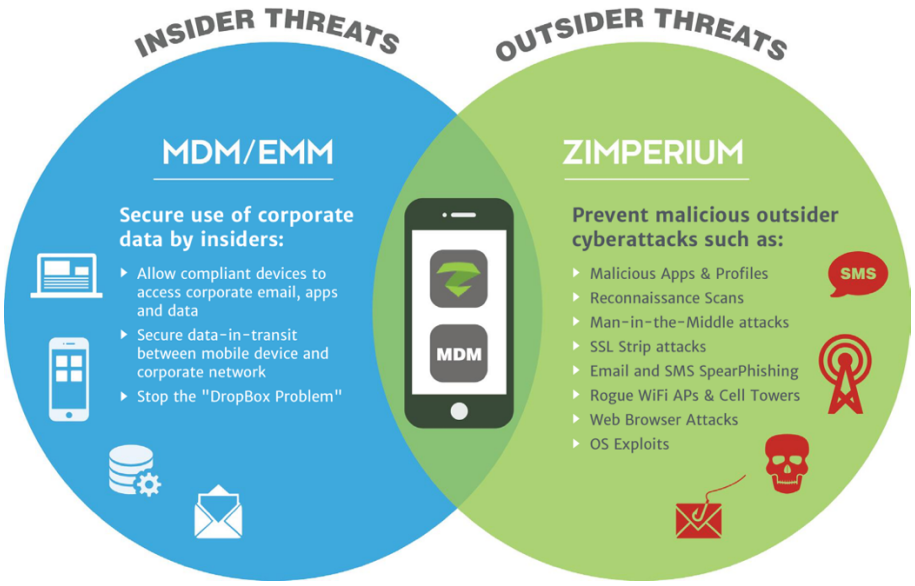


Figure 6. MDM/EMM + Zimperium equals Unparalleled Mobile Security

Recommendation

Organizations need to embrace a healthy mobile security policy that protects the organization and its sensitive IP while promoting productivity on mobile devices both in and outside of the corporate network. While some of the solutions mentioned in this white paper have valuable components for proper insider use and compliance purposes, they fall short on preventing cyberattacks on mobile devices from the outside. Organizations that are concerned with securing against advanced network and host based attacks need to know more than if the device has been rooted or whether a malicious app has been installed. A true mobile security solution needs to provide an enterprise with a way of measuring the risk to the whole device and the resulting impact to the business. Enterprises will be best served by implementing a mobile security solution that can integrate with existing MDM/MAM/MCM technologies to manage, secure and protect mobile devices from both insider and outsider threats – around the clock.

CONTACT US

101 Mission Street
San Francisco, CA 94105
Main: 415.992.8922 | Toll Free: 844.601.6760
sales@zimperium.com
www.zimperium.com