ZIMPERIUM®
ADVANCED MOBILE SECURITY

The Government IT Leader's Guide to Securing BYOD

Implementing Bring Your Own Device (BYOD) programs in the government presents unique challenges for agencies and IT departments. Agencies are adopting these new policies to increase employee satisfaction, support mobile productivity and innovation, and save the agency money.

Allowing employees the freedom to use their personally owned mobile devices, while still ensuring data security and meeting the additional responsibility of public trust, can be a daunting task. How do IT and security administrators protect information and connected systems on a device that often lives outside the policies, procedures, and security systems that have traditionally protected the agency's information?

These mobile endpoints are exposed to a spectrum of risks, from compromised devices, rogue networks, malicious applications, and phishing threats, resulting in serious security implications. And just like traditional endpoints, mobile devices are increasingly targeted by zero day vulnerability and malware attacks that compromise both personal and corporate data.

The legacy approaches to mobile security are not able to keep up against these increasingly technical attack vectors. While malicious apps still exist on common app stores and represent a significant threat, the increase in popularity of unofficial app stores hosting rogue applications, often riddled with both known and never before seen threats, continues to show the weakness is legacy mobile threat security products. And determined parties are favoring more rigorous, targeted device, network and phishing attacks against specific agencies, groups, or individuals – yielding much richer results.

These concerted attacks are exceptionally damaging, with new instances daily. Compromised examples include banking, social media companies, government, and the high-tech industry. These threats are amplified when a device and its use fall outside the IT department's full control as the opportunity to more easily execute focused techniques and exploits is significantly higher. Once infiltrated, the mobile device's data can be harvested and further leveraged to access the organization's enterprise resources, damaging sensitive information, stealing data, compromising other employees, and/or creating a foothold within enterprise systems.

Just as traditional endpoints are shored up with threat detection, so must mobile endpoints. While organizations are addressing the management of these devices through traditional solutions, they miss the mark in supporting Zero Trust architecture initiative by leaving mobile device attestation and dedicated threat defense out of the equation. And in order to best support BYOD initiatives, IT and security teams need to address mobile threat-based detection.

Known Gaps in Existing Tools/Management is Not Security

As mobile device adoption has increased in the workspace, most existing security infrastructure is unable to provide the coverage necessary to directly secure these devices. And misinformation and a false sense of security have brewed over many years related to mobile device security. And the number of security breaches across many industries continues to highlight the inadequacies of the current mobile toolset, largely deployed by many organizations.

The biggest areas of adoption for mobile device support have been around mobile device management (MDM) toolsets, enabling IT and security administrators to enforce base-level policies of access and control on both owned and BYOD assets. Most MDM's provide rudimentary jailbreak/root detections based on known signatures and infrequent timed (6- 12 hours) intervals. But these checks cannot detect zero-day exploits and are simple to bypass for attackers. The MDM platforms also cannot provide malware detection, app analysis, network threat detections, or phishing attacks, leaving any security team in the dark on critical data.

And when it comes to supporting BYOD policies, MDM solutions are often viewed as invasive to the personal device, taking the control out of the owner's hands and placing it with an administrator. With the ability to scan personal messages, view photos, and access other personal, non-essential information, as well as wipe the phone with no warning, these management solutions leave little to be desired outside corporate owned endpoints.

Simply put, MDM enforce and manage settings on the mobile device but provide little in the terms of detections or analysis for threats and risks, and all at the expense of user data privacy and control.

Some IT organizations have started to approach mobile endpoints with container solutions, or mobile application management (MAM), that instead of managing the entire device, only manage an application, or a set of applications that share common code and connect to the same administrative back end, allowing a container of managed applications to form on the device. Containers enable administrators to manage and enable these applications, with additional application level security control, without requiring a full device management. This approach is particularly attractive for BYOD scenarios as it does not introduce the potential friction and liability of having to manage both work and personal data on the device that an MDM approach may introduce. But just like the traditional implementations of containers, the security around them is not impenetrable. If the device is compromised, all security controls around the container and the applications therein are null and void. In fact, in 2019 container technology was in the top 10 vectors of attack for enterprises. Containers also do not address the existing mobile attack surface of compromised networks, phishing attacks, and host malware detection.

Another approach to mobile data access has been virtual desktop infrastructure (VDI), providing users a remote desktop to access for all their productivity needs. This desktop virtualization has been a standard data access tactic on traditional endpoints as it enables employees to do the work they need without the actual data leaving a secured environment. But with BYOD policies, VDI solutions are being installed on unmanaged, personal devices that often don't meet the security standards of the organization. And without true on-device security providing threat analysis and device attestation, the attack surface grows with each new connection back into the enterprise data source.

Just like MDM, containers, and VDI do provide a simple layer of security through their fundamental architectures, but are still susceptible to attack as the technology is not built with a device security mindset. And while MDMs, containers and VDI do provide an easy point of access for users, on the backend, administrators must address network, host, and application security consistently, often a very manual and difficult process with the wide range of mobile endpoints and network configurations.

While these data access and management technologies are impactful and useful the reliance on them as a security layer leaves mobile endpoints susceptible to attack. And with the increasing size of the attack surface paired with the portability of mobile endpoints, the process of securing mobile devices is continuous. Ultimately, if the host device security is not addressed with a proactive, advanced security solution, these layers of data access become gateways of access for any skilled cybercriminal.

As NIST recently demonstrated with their SP 1800-22, *Mobile Device Security: Bring Your Own Device (BYOD)*, Mobile Threat Defense (MTD) is core to the BYOD platform. Without an advanced, on-device MTD, you cannot attest to having Device Integrity and declare a Zero-Trust environment.

Closing the Mobile Attack Surface Gap

As organizations address mobile security and align with the best practices and guidelines from NIST 800-124r2, Mitre, and Gartner, the significance of having a mobile threat defense (MTD) solution cannot be overstated. And as agencies and organizations adopt the 'never trust, always verify' architecture of Zero Trust, the need to have complete device attestation of all endpoints, tradition, and mobile is critical.

In order to address the security of mobile endpoints and support a complete Zero Trust security architecture, security organizations must adopt an advanced MTD solution. Providing continuous, on-device detection and risk assessment, an advanced MTD closes the gap in mobile endpoint security, enabling IT and security teams to address the attack vectors that put their users and data at risk. By sending critical device data back to administrators, as well as on-device security, advanced MTD solutions fill in the MDM and container security gaps.

> *"Emerging use cases envisage MTD as a component of zero-trust network access (ZTNA) architecture and of an extended detection and response (XDR) system for detection and response, which can serve as a pilot for unified endpoint security. This is in addition to the use of MTD for mobile phishing protection."*
>
> *– Gartner 2021 Market Guide for Mobile Threat Defense*

By reducing the security gaps of MDM and container layers, IT and security teams are able to shore up their mobile defenses, enabling their users to be effective outside the established physical security perimeter. And to best support the BYOD initiatives, security needs to be approached with an advanced mobile threat defense solution.

The Zimperium zIPS mobile threat defense application addresses the security gaps left by MDM, container, and VDI solutions with machine-learning powered real time, on-device protection. Built on the Zimperium z9 mobile threat defense platform, the machine learning engine is constantly analyzing billions of data points and training the threat model. This enabled Zimperium zIPS to secure mobile endpoints against known and unknown threats as well as phishing attacks, compromised and unsecured networks, and malicious applications that can put an enterprise's data at risk.

In order for any organization to confidently adopt a BYOD policy to support the distributed workforce, they must approach their mobile endpoint security with the same mindset as traditional endpoints. With Zimperium zIPS complementing their data access and device management solutions, they can not only enable their employees to be effective while mobile, but be confident in the security of their devices and support existing Zero Trust architecture.

About Zimperium

Zimperium, the global leader in mobile security, offers the only real-time, on-device, machine learning-based protection against Android, iOS and Chromebooks threats. Powered by z9, Zimperium provides protection against device, network, phishing and malicious app attacks. For more information, visit www.zimperium.com.

ZIMPERIUM®