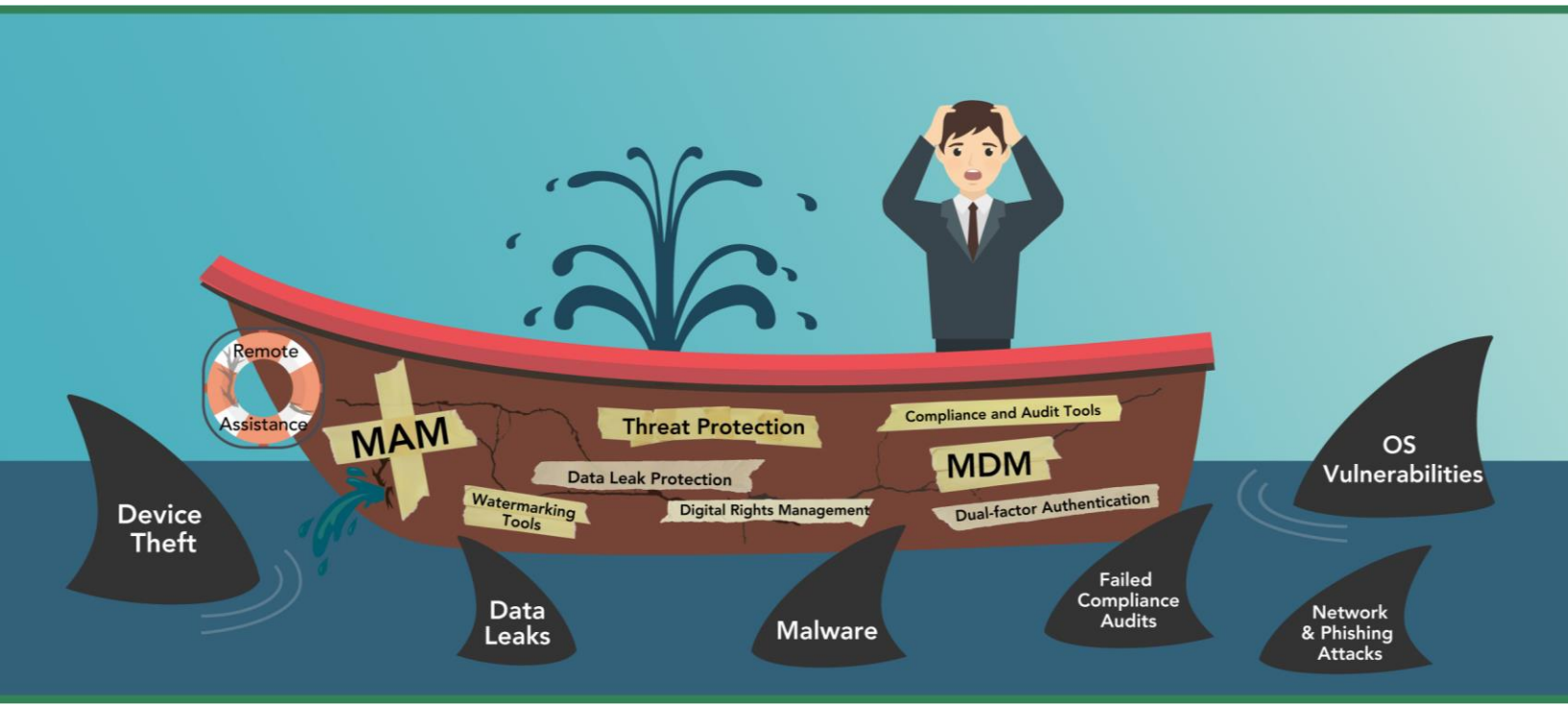
sierraware

Moving Beyond MDM

Why Legacy Mobile Security Products Don't Work



Introduction

Today's workforce is mobile. Now, users can access business data from any mobile device and any location. The tidal wave of mobile users that have embraced the Bring Your Own Device (BYOD) trend have forced organizations to develop comprehensive and user-friendly mobile security strategies.

To protect mobile apps and data, organizations must:

- Ensure data cannot be accessed if a mobile device is lost or stolen
- Enforce strong authentication and encryption
- Prevent mobile malware or third-party apps from accessing business data
- Monitor user activity for unauthorized access or data exfiltration
- Provision, upgrade, and patch mobile apps

Unfortunately, the mobile security status quo—a motley assortment of products—are impractical, unpopular with employees, and do not address all of today's security and compliance requirements.

MDM: Device-Level Security Only

To protect mobile devices, security vendors and phone manufacturers developed Mobile Device Management (MDM) technology. MDM provides device-level management of phones and tablets, enabling organizations to remotely wipe devices, limit which apps can be installed, and configure other device-level settings.

Unfortunately, MDM alone does not really protect business data. This is because MDM does not control apps. While it can restrict which apps users install, it can't limit what users do with their apps. As a result, users can download sensitive files onto their phone or copy data from business apps into personal apps—which is a big "no no" for many compliance regulations.

MDM also does not provide application-level controls to regulate access or prevent data tampering. There are a myriad of use cases where employees should not be allowed to modify files or photos and MDM, without any application-level protection, cannot audit or prevent data tampering.

In addition, MDM is often unpopular with employees because they do not want their employer dictating what apps they can install or wiping their personal data when they misplace their phone.

On top of these limitations, crafty users have discovered ways to circumvent MDM controls and side-load unsanctioned mobile apps. But even if users do not disable MDM policies, MDM cannot protect mobile data from cyber-attacks and insider threats.

Mobile Application Management for a Handful of Pre-Integrated Apps

To address the shortcomings of MDM, many mobile security vendors developed Mobile Application Management (MAM). MAM solutions can manage and sandbox business apps, enforce app-level user authentication, and report on app usage.

Unfortunately, in order to add MAM capabilities to their apps, app developers must integrate complicated MAM SDKs into their apps. As a result, most mobile security vendors only support a few dozen mobile apps in their partner ecosystems—a small fraction of the million-plus apps in Google Play or the Apple App Store. Employees must either use these apps or use second-rate productivity apps developed by the mobile security vendors themselves.

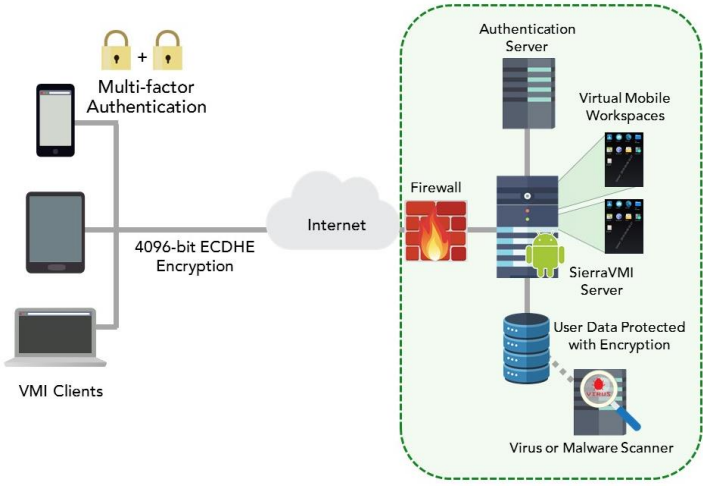
Threat Protection, Network Security, and Auditing for Compliance

Even with MDM and MAM solutions, organizations often need separate products for anti-malware, single sign-on, document watermarking, and user activity auditing. If departments within the organization wish to share confidential videos, like training videos or recorded presentations, then IT teams will also need to provision digital rights management (DRM) for mobile devices.

The total cost to roll out a mobile security program that safeguards against network, malware, and insider threats and addresses compliance requirements is many times greater than the base price to manage and wipe devices with MDM. If organizations plan to allow users to access financial, PII, or healthcare records from their phones, they need to look beyond MDM and legacy mobile security solutions.

Virtual Mobile Infrastructure

To address all aspects of mobile security, organizations need a comprehensive, effective, and ultra-secure solution. This is where Virtual Mobile Infrastructure (VMI) comes in. VMI solves the security challenges imposed by BYOD, allowing organizations to protect corporate data and achieve compliance. VMI is similar to VDI, but instead of virtualizing Windows desktop applications, VMI virtualizes Android operating systems and applications.



A VMI deployment, with phones, tablets and laptops accessing a VMI server hosting mobile apps remotely.

Benefits of VMI

With VMI, organizations host Android instances in their data center or in the cloud. Mobile users can then access Android applications remotely from iPhones, iPads, Android devices, HTML5-enabled Windows phones, Blackberry phones, and even Windows desktops.

VMI helps organizations:

- Prevent data loss from device theft by ensuring data is never stored on end user devices. With VMI, you don't need to worry that users won't report their lost phones.
- Monitor privileged user activity with detailed logging and screen recording. If mobile users can access CRM, ERP, or accounting apps from their phone, record suspicious activity for forensics purposes.
- Prevent data leaks with anti-screen capture and watermarking. Clipboard policies can also prevent users from copying data from business apps to personal apps.
- Satisfy compliance by enforcing strong encryption and authentication. VMI provides multi-factor authentication and 4096-bit SSL encryption for all business apps. These measures also safeguard against brute force and Wi-Fi man-in-the-middle attacks.
- Centralize app and operating system patching. When new vulnerabilities like Stagefright and XcodeGhost emerge, IT departments must rely on device vendors to release patches to end users. Unfortunately, many device vendors will not patch older phones. With VMI, organizations can receive and apply patches centrally in their data center.
- Reduce IT helpdesk calls with single sign-on. Once a user logs into their VMI workspace, they can access all of their apps without needing to re-authenticate.
- Scan all mobile apps for viruses and vulnerabilities. With VMI, organizations can use the anti-malware solution of their choice to scan files or analyze mobile apps for malicious behavior. If new app or platform vulnerabilities are discovered, IT teams can quickly patch them in the data center rather than waiting for device manufacturers to patch end user devices.
- Lower operating expenses by eliminating the need to install, configure and support mobile apps on a myriad of end user devices.

VMI offers a comprehensive and secure solution to manage and protect mobile apps. VMI is easy-to-deploy in the cloud or on standard servers.

Device Management Comparison

Device Management	Mobile Device Management (MDM)	SierraVMI Virtual Mobile Infrastructure
Password protection	Device-level	Device-level (active-sync), workspace-level
Data and apps storage location	On mobile device	Secure data center
Remote Wipe	✓	Yes, although not necessary because data is not stored on the phone and account can be deactivated by the SierraVMI admin
Encryption of data in transit	Device-level by configuring VPN client on device; customers must buy VPN server and redirect traffic through VPN. Does not encrypt traffic from apps to app servers.	App-level, can enforce 4096-bit encryption; VPN configuration optional
Encryption of data at rest	✓	✓
Check for rooted or jailbroken phones	✓	✓
Geolocation policies	✓	✓
Anti-screen capture	✓	✓
Centralized OS and app patching	App patching only; platform patching dependent on patches from device manufacturers	✓

Application Management Comparison

Application Management	Mobile Application Management (MAM)	SierraVMI Virtual Mobile Infrastructure
Multi-factor authentication	✓	✓
Single sign-on	✓	✓
App sandboxing	Containerization or app-wrapping	Business apps are hosted on a separate server
Secure file storage	If used in conjunction with Secure Content Management	✓
Clipboard controls to prevent copying data to other apps	✓	✓
User monitoring	Usage logs	Detailed activity logs, usage logs, screen recording of user sessions for compliance
Remote assistance	✓	✓
App compatibility	Very few legacy apps (<100)	All Android apps
Available without costly and time-consuming app integration		✓

Digital Rights Comparison

Digital Rights	Digital Rights Management Products	SierraVMI Virtual Mobile Infrastructure
Secure distribution of multi-media files • **Training videos** • **Recorded presentations** • **Manufacturing assembly instructions** • **Military guides**	Expensive custom solutions that need to support different devices and media players	In-built media player for streaming video and audio with anti-screen capture controls
Time of day, geolocation, and group-based policies	✓	✓
Media files cannot be downloaded or shared	✓	✓
Integration with device management		✓

Threat Protection Comparison

Threat Protection	Anti-virus, Anti-malware, Network Security	SierraVMI Virtual Mobile Infrastructure
Virus and malware detection	✓	Can integrate with anti-virus scanners, advanced threat protection (ATP)
Protection of employee information such as geolocation	Limited	✓
Protection against Wi-Fi and Man-in-the-Middle Attacks	✓	✓ Strong encryption

Enterprise Content Protection Comparison

Enterprise Content Protection	Copyright Protection Tools	SierraVMI Virtual Mobile Infrastructure
Well-defined content • **PDF files** • **Images** • **Productivity files**	✓	✓ Watermarking of user name and time stamp on VMI screen
Content generated at run-time • **Web content** • **Email messages** • **Mobile app screens**		✓ Watermarking of user name and time stamp on VMI screen

Conclusion

Legacy mobile security vendors force organizations to cobble together a patchwork of solutions to protect corporate data from device theft, attacks, and insider threats. Because IT departments must rely on varying controls from different mobile app vendors and device manufacturers, it becomes nearly impossible to enforce consistent policies across all users and all apps.

Virtual Mobile Infrastructure (VMI) solves many of the challenges introduced by BYOD. VMI offers secure, easy access to mobile apps from any mobile device or desktop client with an HTML5-enabled web browser. It reduces risks associated with physical device theft, since sensitive data is never stored on phones or tablets. Plus, it allows IT staff to centrally manage and upgrade mobile apps.

As organizations embrace BYOD, they need to develop a strategy to protect corporate data and satisfy compliance while supporting a broad array of mobile devices and apps. Virtual Mobile Infrastructure, with its inherent ability to keep sensitive data off of devices and its strong security, auditing, and tamper-resistant features, had become the easy and effective solution for protecting mobile apps and data.

About Sierraware

Sierraware is a leading provider of virtualization and security solutions that change the way applications are accessed and data is secured. Sierraware's virtual mobile infrastructure (VMI) software empowers developers to support all mobile platforms with a single app and to protect data and monitor user activity.

sierraware

1250 Oakmead Parkway
Suite 210
Sunnyvale, CA 94085
United States
Phone: +1 408-337-6400
Email: info@sierraware.com