SierraVMI

Protect your mobile apps and data with a scalable, easy-to-deploy, and ultra-secure solution

Features and Benefits

- Safeguard business data by monitoring and controlling access to mobile apps
- Address HIPAA, FFIEC, and NIST SP 800-46 with multi-factor authentication, SSL encryption, and user auditing
- Build apps for Android and support access from any device or HTML5 browser
- Enable remote and field employees to work anytime and anywhere
- Increase employee productivity by enabling fast, easy access from employee-owned devices
- Streamline and centralize mobile application management
- Prevent data leaks with watermarking and anti-screen capture

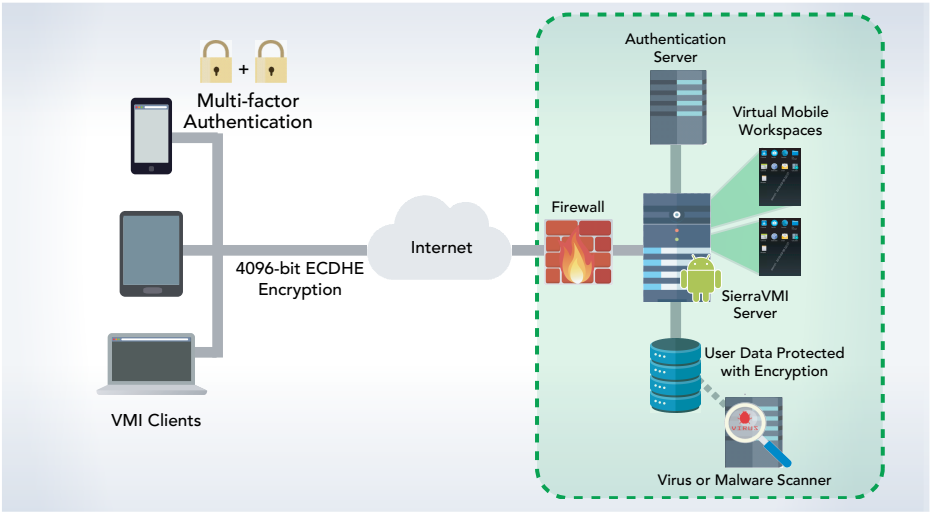
Today, IT must manage and secure mobile apps accessed from a myriad of different devices. Besides having to provision and upgrade software on all of these devices, IT must also protect against threats like device theft and data exfiltration.

While solutions like mobile device management (MDM) can reduce the risk of data loss, most employees do not want their employer managing their personal phones or controlling what apps they can install. MDM alternatives, such as app wrapping and containers, provide app management, but they require cumbersome SDK integration and only work with a handful of apps.

SierraVMI Virtual Mobile Infrastructure

Virtual Mobile Infrastructure (VMI) solves organizations' mobile security challenges efficiently and non-intrusively. VMI empowers organizations to host their mobile apps on servers and provide remote access to these apps from any device. By virtualizing mobile apps, VMI enables businesses to:

- Avoid costly data breaches by preventing users from downloading sensitive data to their devices.
- Monitor privileged user activity with detailed logging and screen recording for forensics.
- Support heterogeneous environments with Android, Apple, and Microsoft devices.
- Block unauthorized access using multi-factor authentication based on a combination of passwords, certificates, device IDs and one-time passcodes.



Enable secure access to business apps from tablets, smartphones, and laptops.

sierraware

Satisfy BYOD Demands

Employees today want to access their business applications from their own devices. While, traditionally, users needed to access Windows applications from their phones and tablets, a new generation of mobile applications have emerged, forcing IT teams to rethink their virtual desktop strategies.

In addition, many IT departments simply cannot keep up with the deluge of different devices in most corporate environments. SierraVMI enables all of these devices to access Android-based apps with a look and feel that has been specifically designed for mobile devices.

Avoid Data Loss from Device Theft

Ensure data is never stored on end user devices. With VMI, you don't need to worry that users won't report their lost phones or that thieves won't remove SIM cards before devices can be wiped.

Monitor Privileged User Activity

Maintain an audit trail by logging user activity or optional screen recording. If mobile users can access CRM, ERP, or accounting apps from their phone, record suspicious activity for forensics purposes.

Prevent Data Leaks

Deter users from saving or sharing confidential data with anti-screen capture and watermarking. Apply watermarks with a user name and timestamp to static content, like PDF files or images, and to dynamic content, like web pages and email messages.

Clipboard policies can also prevent users from copying data from business apps to personal apps.

Block Unauthorized Access

To prevent malicious users from gaining access to corporate data, SierraVMI provides multi-factor authentication. Authentication methods include:

- Password/PIN
- IMEI for device-level identification
- Client certificates
- One-time password

In addition, single sign-on (SSO) reduces IT helpdesk calls. Once a user logs into their VMI workspace, they can access all of their apps without re-authenticating.

Simplify and Secure Video Distribution

From training webcasts to recorded presentations and more, videos have become an essential platform for education and news. However, many organizations struggle to distribute videos securely to a wide range of devices.

SierraVMI includes a built-in video player with optional watermarking. IT administrators can restrict access by user and prevent employees from downloading or sharing sensitive videos.

SierraVMI provides multimedia redirection to enhance users' audio and video playback experience. SierraVMI streams HD video directly to the client rather than playing multimedia files on the server and then compressing the content and streaming it to clients.

Multimedia redirection delivers smooth, consistent playback of multimedia content. It also decreases bandwidth usage—because video files are often more optimally compressed—and it reduces the load on VMI servers.

Satisfy Compliance with Strong Encryption

SierraVMI can enforce 4096-bit SSL encryption for all business apps. Encryption safeguards against Wi-Fi and micro-cell-based man-in-the-middle attacks.

Support Device Peripherals and Components

To provide a seamless user experience, SierraVMI supports all mobile device elements, including:

- Microphone
- Audio
- GPS
- Printing services
- Background notifications (suspend/resume)
- Screen rotation
- GPU acceleration

With GPU acceleration, SierraVMI not only improves performance, but it also supports a wide range of mobile apps that require GLES or OpenGL 3.0 for rendering graphics and shaders.

Best-of-Breed Virtual Mobile Solutions

SierraVMI provides organizations of all sizes an ideal, cost-effective solution for virtual application and desktop infrastructure. SierraVMI enables organizations to:

- Lower the risk of data loss by isolating each SierraVMI application instance with Firefall AppVM technology.
- Protect sensitive data without wiping phones or restricting which apps users can install.
- Streamline app management by eliminating the need to install individual apps on every device.
- Reduce the risk of unpatched phones by hosting apps on centralized servers. When new vulnerabilities like Stagefright and XcodeGhost emerge, IT departments must rely on carriers or device vendors to patch phones, but many will not patch older phones. With SierraVMI, the Android server is always up to date.
- Scan mobile apps for viruses and vulnerabilities. With VMI, organizations can use powerful, server-grade anti-malware scanners or sandboxing (ATP) solutions to analyze apps for malicious behavior.

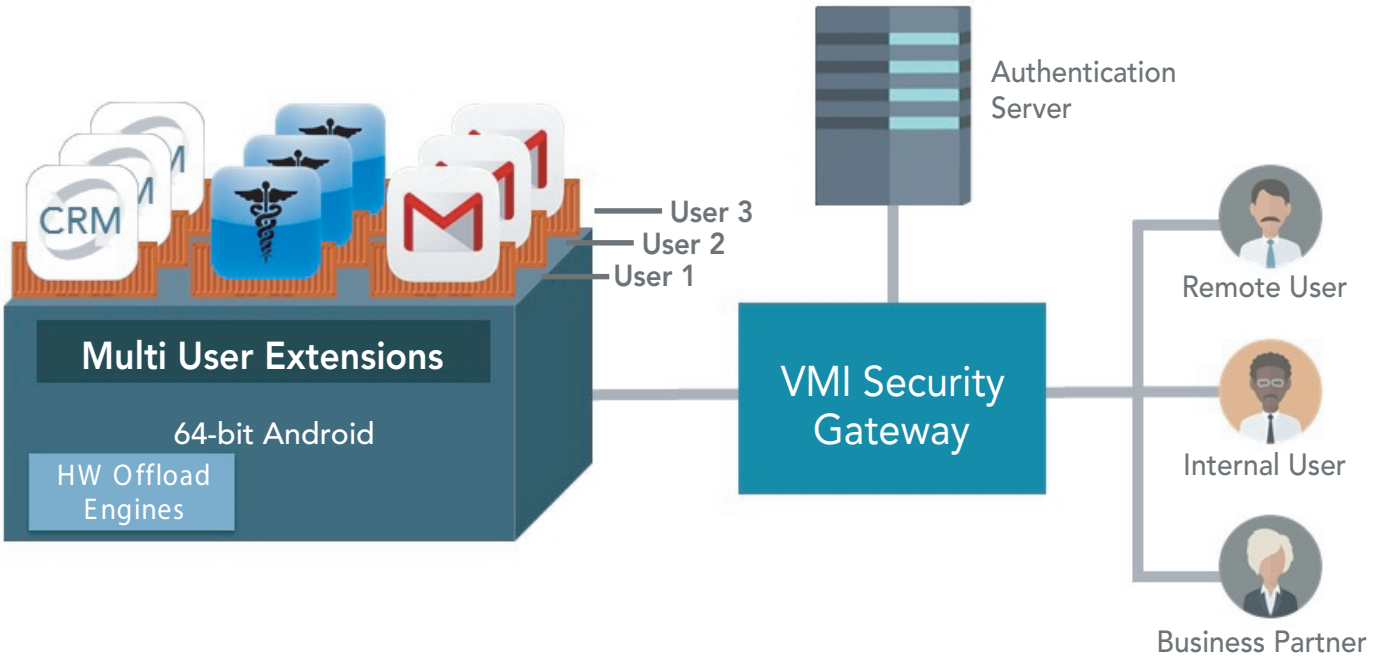
Integrated Mobile Client Security

SierraVMI includes a TrustZone-enabled Trusted Execution Environment (TEE) which allows virtual applications to run in a trusted world. Supported on devices that include the SierraTEE secure operating system, SierraVMI ensures that keyboard loggers cannot capture passwords.

Support high-density VMI deployments

SierraVMI offers a powerful and scalable platform for mobile security. SierraVMI leverages patent-pending mobile app virtualization technology to host thousands of users from one operating system instance. As a result, organizations need to provision fewer servers for on-premise deployments or purchase far fewer virtual instances for cloud deployments.

SierraVMI also eliminates the need for complicated cloud orchestration systems. Because of its high-density architecture, organizations can provision access to ten thousand users from a dozen servers. With SierraVMI, organizations can avoid provisioning racks upon racks of servers. They can install and set up SierraVMI in hours rather than days or weeks.



The SierraVMI architecture includes one or more multi-tenant Android virtual machines and a SierraVMI gateway that load balances connections to the Android virtual machines, performs management, and provides access to mobile apps.

SierraVMI Specifications

Device Monitoring and Management

- Protect against data loss by preventing data from being downloaded to phones
- Geolocation restrictions (geofencing)
- Time-of-day restrictions

Content and Video Protection

- Watermarking with timestamp and username for:
  - Static files (PDF, images, Word documents)
  - Dynamic content like email and web pages
- Anti-screen capture
- Clipboard controls to restrict copy and paste
- Secure distribution of 4K HD video files and audio files

Authentication

- Multi-factor authentication:
  - Password/PIN
  - IMEI for device-level identification
  - Client certificates
  - One-time password
- Single sign-on
- Integration with LDAP, Active Directory, RADIUS
- Brute-force attack prevention

App Compatibility

- Compatible with every Android-based app up to API 23 (Marshmalllow)
- Support for GPU GLES 1.0/GLES 2.0/OpenGL 3.0
  - Support for 3D games

Peripheral Support for iOS, Android, Windows Phone

- Microphone
- Audio
- GPS
- Printing services
- Background notifications (suspend/resume)
- Screen rotation
- GPU acceleration

VMI Server Security

- Encryption of data at rest on VMI server
- Encryption of data in transit, supporting up to 4096-bit ECDHE encryption to prevent Man-in-the-Middle attacks
- Hardened Android Operating System, latest version and patches (Marshmallow)
- Support for server-grade anti-malware and Advanced Threat Protection (ATP) solutions

Management

- Web management interface (HTTPS)
- SNMP
- User activity logging
- User screen recording - live monitoring of 8 user sessions
- SMS, email alerts for security violations and system errors
- Remote assistance of user sessions

Deployment Options

- x86 servers (Intel)
- ARM servers (Cavium ThunderX, AMCC)
- Amazon AWS
- Integrated redundancy and high availability

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

#PSB-SIERRAWARE-VMI-1013