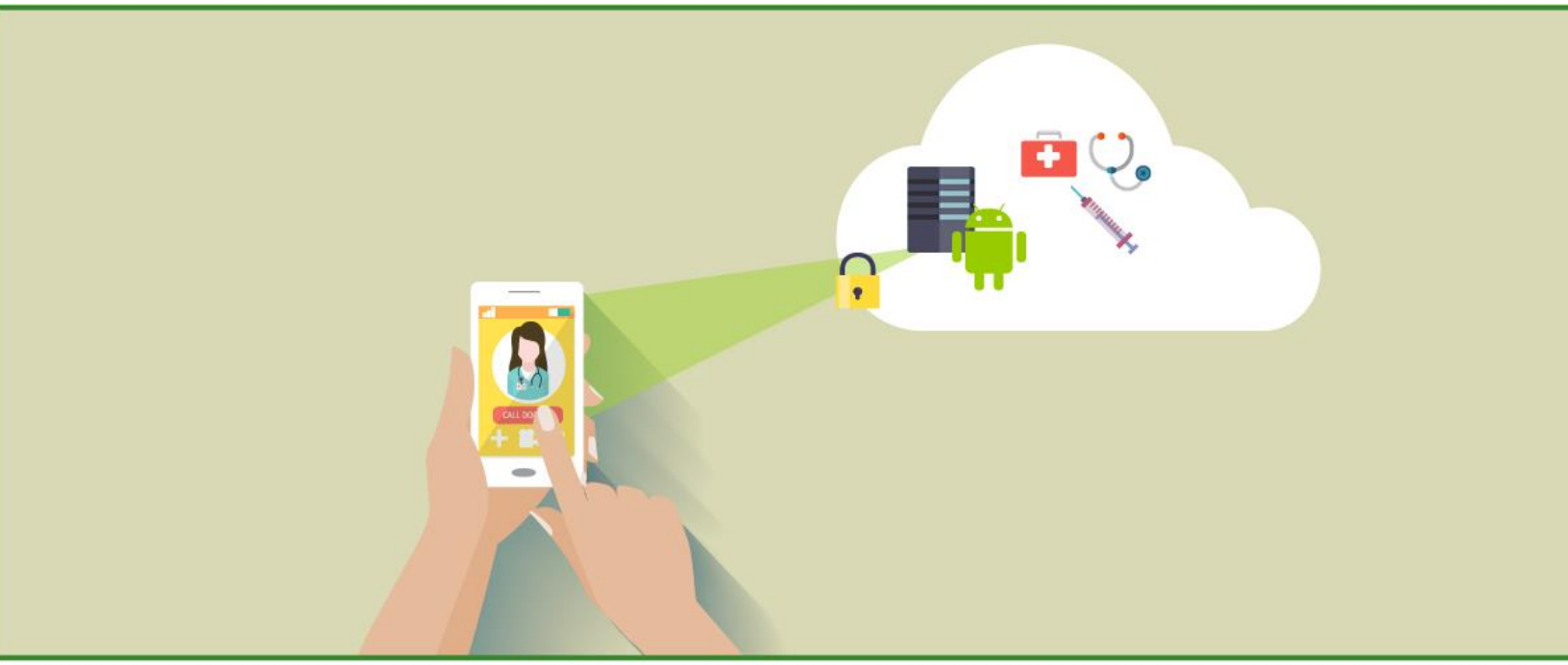
sierraware

7 Things You Need to Know about Virtual Mobile Infrastructure



Executive Summary

Employees are bringing their phones and tablets to work in droves. This tidal wave of unmanaged devices has forced IT departments to change the way they administer, support and secure business data. Users want to access email, CRM, ERP, and other apps from their phones, but they also want to maintain full control over the devices they've purchased. IT must find a hands-off way to monitor and protect data in a new mobile world.

This white paper describes the challenges introduced by BYOD and the advantages and drawbacks of today's mobile security solutions. This paper also introduces virtual mobile infrastructure (VMI) lays out the seven requirements that organizations should consider when evaluating VMI solutions.

Introduction

The Bring Your Own Device (BYOD) phenomenon vows to boost productivity, improve employee satisfaction, and lower capital costs.

But as BYOD takes hold, organizations must:

- Develop mobile apps for a myriad of different devices running distinct operating systems.
- Provision, upgrade and patch mobile apps on each end user device
- Prevent mobile malware from accessing business apps and data
- Monitor user activity for unauthorized access or data exfiltration
- Enforce strong authentication and encryption

So how can organizations successfully navigate through today's minefield of IT risks and requirements foisted on them by BYOD? Some organizations are turning to Mobile Device Management (MDM) or Virtual Desktop Infrastructure (VDI) as solutions, but each alternative comes with its own special set of problems.

Mobile Device Management – A Solution Whose Time Has Come…and Gone

MDM software allows IT departments to secure employees' mobile devices by detecting jailbroken phones, enforcing password protection, supporting remote wipe and report lock, distributing software updates, encrypting data, and configuring other device and application settings.

Elements of MDM form a rock-solid foundation for security, but MDM also has its limitations. While MDM can manage mobile device settings, it has little control over applications. In addition, many end users that have purchased their own phones do not want their employer to tell them what apps they can install and they do want their employer wiping all of their personal data when they misplace their phone.

While related technologies that fall under the broader Enterprise Mobility Management (EMM) umbrella try to address these shortcomings, they often fail to perform important functions like tracking user activity for unauthorized access or data leaks. And full-featured EMM deployments often require tight integration with applications, forcing enterprises to integrate their software with container solutions or force employees to use often inferior browser, email and calendar apps from EMM vendors rather than popular apps from Google, Apple, Microsoft and others.

Organizations often struggle to support the continuous stream of new mobile operating systems and APIs. Just developing apps that work on all of their employees' devices is challenging enough. When you layer on security measures like MDM integration, containers, wrapping, data storage and data backup across apps multiple vendors, EMM becomes even more untenable.

And even after organizations have gone to the effort of implementing EMM, they would have a hard time auditing which users accessed what business data from their phones. Once data is in end users' hands, it is difficult to contain, creating blind spots for forensics investigators after a breach.

Virtual Desktop Infrastructure: Perfect for Desktops, Not-so-Perfect for Mobile

Another way that organizations can prevent corporate data from seeping out to unmanaged mobile devices is to host applications centrally on data center servers rather than installing apps and data on mobile devices. With Virtual Desktop Infrastructure (VDI), mobile users can access remote Windows apps from a browser or a client application.

VDI offers a wealth of advantages to businesses. However, VDI also has its shortcomings. VDI was designed for desktops, not mobile devices (hence the "Desktop" in Virtual Desktop Infrastructure). Here are a few reasons why VDI isn't the answer:

- Screen size and touch input: Windows desktop applications were designed for large monitors and for cursor and mouse input, not for handheld devices with small screens and touch input. While VDI can translate touch to mouse clicks, it is difficult to achieve left, right, and double mouse click behavior on a touch screen. This creates a cumbersome experience for mobile users.
- Cost: VDI licensing fees are exorbitant. Software, hardware and management expenses can easily run over $700 per user. If organizations were hoping to cut costs by embracing BYOD, these savings will quickly evaporate because of VDI licensing fees.
- Access to a burgeoning array of mobile apps: App development has undergone a sea change over the past few years. Many developers are writing apps directly for mobile devices. Mobile users want to access these apps on their mobile devices; they don't want ungainly desktop apps. The world is moving towards mobility. Organizations must evolve also to keep users happy.
- Bandwidth: VDI vendors developed their communications protocols assuming that users were accessing VDI infrastructure from high-speed wired or wifi connections.

Virtual Mobile Infrastructure to the Rescue

To protect mobile data and monitor user activity, organizations must look beyond current solutions like MDM and VDI. 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.

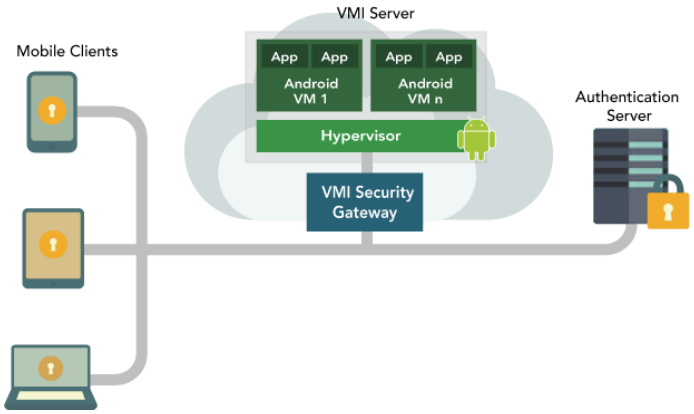


Figure 1: VMI deployment diagram, with phones, tablets and laptops accessing a VMI server hosting Android remotely.

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, Android phones, Blackberry devices, Windows phones, and even Windows desktops.

VMI helps organizations:

- Prevent data loss from device theft
- Slash app development costs – With VMI, app developers can build apps once and instantly support all types of mobile devices.
- Lower operating expenses – IT administrators avoid managing apps on end user devices.
- Satisfy compliance by enforcing strong encryption and authentication

7 Things You Need to Know about Virtual Mobile Infrastructure

VMI offers clear benefits to organizations that wish to support mobile and BYOD initiatives. However selecting the right solution in a nascent market is tough. What features should you look for? And what hurdles might you encounter after you have deployed a solution? Will your solution support every mobile app, including apps built for mobile phone hardware? Will your solution scale?

To make it easy, we listed seven features you should look for when evaluating VMI.

1. **Reduce hardware and operating costs with high-density VMI deployments.** There are two main VMI architectures today: (1) virtualizing individual Android applications—also called mobile app virtualization—and (2) running a full Android runtime per user. Mobile app virtualization delivers eight to ten times better density compared to running a separate Android Instance per user,[1] so mobile app virtualization reduces the number of servers needed to host VMI. As a result, it lowers hardware costs and operating costs and it streamlines management.

Figure 2: Mobile app virtualization provides a secure, isolated app instance per user for maximum density.

[1] Density estimate based on a 16 MB mobile app running on a 1 GB Android system.

Figure 3: Full Android virtualization requires a separate instance per user, reducing user density.

Besides relying on Linux virtualization, many VMI products use QEMU emulation or VNC for remote rendering. SPICE, VNC were designed decades ago for LAN and desktop access. QEMU emulation reduces performance and adds overhead because display data is typically transferred from Android VMs to the base operating system for encoding.

If organizations plan to host a unique Android VM for every user in the cloud, they could quickly rack up expensive bills. This is because most cloud providers charge for every VM instance. If an organization has one thousand concurrent users, they would need to pay for hundreds VMs. Managing VMs in a corporate data center would be equally expensive; organizations would incur higher IT management and capital costs. Plus, hosting so many low user density VMs would necessitate high-performance storage hardware—similar to what Windows VDI customers must purchase today.

Mobile app virtualization offers the following advantages over alternative solutions:

- Support for camera, microphone, GPS, display and video redirection in a unified protocol.

- Very low server CPU and memory requirements
- Ability to serve graphics intensive applications like Medial Imaging, Maps using desktop class GPUs
- Fast "boot up time" when users launch VMI sessions.

Instead, organizations should consider a VMI solution that virtualizes the individual mobile application. Rendering images inline and processing display data and input events at the application level will maximize performance and density. Mobile app virtualization is the scalable solution for virtual mobile infrastructure.

2. Support a broad range of Android applications.

Most Android applications are written in Java and can run easily on any platform, including Intel-compatible x86 and ARM architectures. Since Intel servers outstrip all other types of server architecture in data centers, VMI solutions should support servers with Intel-compatible processors.

However, some Android applications leverage Android's Native Development Kit (NDK) APIs and are only tested on ARM-based architectures, the predominant CPUs used in smartphones and tablets. For example, Word processing apps, mobile video games, and 3D imaging apps may only run on ARM architectures. To ensure compatibility with the most mobile apps possible, select a VMI solution that supports both ARM and Intel servers.

3. Deliver an excellent end user experience with GPU acceleration.

VMI solutions that leverage Graphics Processing Unit (GPU) cards on servers will deliver a much richer and faster experience to end users. Some mobile apps will automatically eliminate user interface (UI) features like overlays and shading if GPU hardware is not detected. GPU acceleration offloads virtually all aspects of user display, from rendering images, vectors, and pipelines to delivering advanced graphics like blending background and foreground apps. To improve session density, improve VMI density, and ensure an optimal user experience, look for VMI solutions that supports GPU acceleration.

4. Provide efficient and smooth video playback.

To deliver reliable multimedia playback and reduce server load, VMI solutions should support multimedia redirection. With multimedia redirection, videos are directly streamed to client devices rather than the VMI server rendering and then compressing video files. Using Android OMX re-direction for audio and video files, VMI solutions can provide full screen play back and efficiently stream videos with ultra-low latency.

5. Enforce multi-factor authentication.

Just relying on simple user name and password authentication is not enough for sensitive applications like healthcare or military applications. To correctly verify users' identities, look for VMI solutions that can support multi-factor authentication such as passwords, software or hardware tokens, certificates, one-time passwords, and out-of-band authentication.

6. Support a broad range of clients.

To ensure that VMI sessions can be accessed by any device, choose VMI solutions that support HTML5 access as well as client apps for iOS, Android, and Windows Phone. Since

modern web browsers support HTML5, you can be assured that any user can take advantage of your VMI infrastructure without device or version incompatibilities.

7. **Address advanced security and compliance requirements with session recording, watermarking, geo-fencing.** Leverage all of the capabilities of VMI to granularly control user sessions and prevent data loss. Use detailed logging and screen recording to monitor privileged user activity. Apply anti-screen capture and screen watermarking to stop users from capturing and sharing screen images. And restrict the location and time that users can login to avoid unauthorized activity. VMI not only prevents users from downloading data to their phones—it can do so much more to control and protect business data.

Conclusion

Trends like BYOD have forced IT departments to change the way that they manage and secure end points. IT must rethink the way that they monitor and protect business data, while still allowing users to access vital business applications.

Virtual Mobile Infrastructure (VMI) solves many of the challenges introduced by employee-purchased mobile devices. 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.

If organizations decide to implement VMI to secure mobile apps, then they need to define a set of evaluation criteria. This white paper suggests criteria that organizations might want to look for when evaluating VMI solutions – criteria such as support for a broad array of mobile devices and mobile apps. Equipped with this information, organizations can make well-informed decisions and deploy the best solutions with the fewest surprises and issues.

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. SierraVisor Hypervisor and SierraTEE Trusted Execution Environment for ARM® TrustZone® deliver embedded virtualization platforms for ARM-based architectures.

sierraware

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