carahsoft

Lookout™

Virtual Mobile Infrastructure (VMI) Does Not Protect the Device. Period.

Thank you for your interest in exploring this content.

Carahsoft is the **Trusted Government IT Solutions Provider**® supporting a broad portfolio of industry-leading technologies through GSA, NASA SEWP V, ITES-SW2 and a wide range of other contract vehicles.

As the **Master Government Aggregator**®, Carahsoft connects government agencies, industry partners, and technology providers to deliver innovative, mission-focused solutions.

In partnership with Lookout, we provide technology solutions that drive modernization, strengthen operations, and ensure compliance with evolving government standards.

To learn more about how Carahsoft can support your technology needs, please visit carahsoft.com

Explore More Resources:
carah.io/LookoutResources

Join Events & Webinars:
carah.io/LookoutEvents

Discover Technology Solutions:
carah.io/Lookout

Learn About Procurement:
carah.io/LookoutContracts

Connect With Our Team:
Lookout@carahsoft.com
(844) 445-5688

FAILURE POINT ALERT

Virtual Mobile Infrastructure (VMI) Does Not Protect the Device. Period.

The mission threat: your warfighters' devices are wide open

Nation-state adversaries are not just targeting your network; they are weaponizing the mobile device itself as the easiest path to mission compromise.

VMI violates zero-trust: it trusts the untrusted endpoint

You deploy VMI for data isolation, yet you are guided by a harmful misconception: VMI does nothing to counter the mounting wave of zero-day exploits and sophisticated attacks that target the actual hardware and operating system on the mobile device. It violates the fundamental Zero Trust principle that no device or user should be implicitly trusted.

A compromised endpoint is not a setback—it is mission failure, guaranteed. Malicious apps, network interception, device rootkits, and devastating phishing attacks bypass VMI entirely.

For true, non-negotiable mission assurance and to enforce a true Zero Trust architecture, the DoW requires a three-pillar defense in depth approach:

- **Mobile Device Management (MDM):** For basic compliance and device lockdown (per the relevant MDM Security Technical Implementation Guide (STIG), e.g., Microsoft Intune MDM Service Desktop & Mobile STIG).
- **VMI:** For isolating sensitive mission data. A shield for data in the cloud, not the device in the hostile field.
- **Lookout Mobile Threat Defense (MTD):** Provides mandatory, continuous threat detection and advanced protection that stops the attack at the source—the device itself.

The Brutal Truth: VMI alone is insufficient as a defense

VMI does not protect the device. Without Lookout's device-level defense, attackers can still:

- **Record and steal everything:** Use surveillanceware (like Pegasus or Hidden Virtual Network Computing; HVNC) to secretly mirror screen activity, capture every keystroke, and lift credentials, regardless of the VMI app running.
- **Intercept critical communications:** Exfiltrate SMS messages, call logs, and crucial geolocation data—information VMI is designed to protect, but utterly fails to shield from a compromised OS.
- **Phish and smish without obstruction:** Launch targeted, high-stakes credential theft attacks that trick users on the device, immediately undermining the VMI's purpose.
- **Seize control of the OS:** Exploit kernel level access, instantly nullifying VMI's security assumptions and giving the adversary full control of the device.

Bottom line: VMI protects data in the hyper-isolated cloud. It offers ZERO protection for the warfighter's device in the hostile field environment. Your mobile endpoints, applications, and data are exposed.

Government-Furnished Equipment (GFE) vs. Bring Your Own Device (BYOD): The threat is universal

The distinction between Government-Furnished Equipment (GFE) and Bring Your Own Device (BYOD) environments is one of control, not *vulnerability*. Lookout's MTD is essential to satisfy the explicit requirement for device-level threat detection found in both.

Environment	Primary Control Mechanism	VMI's Role	Lookout MTD's Mandated Role	STIG/Policy Reference
Government Furnished (GFE)	Full MDM control over device and OS, enforcing policies (e.g., Apple iOS/ iPadOS 18 STIG).	Isolate classified/ CUI mission data within a virtual session.	Provides mandatory, continuous device, app, and network monitoring to ensure the GFE endpoint remains compliant and uncompromised—a specific requirement of the device STIGs.	Apple iOS/iPadOS STIG (e.g., V-276204: DOD Apple iOS/ iPadOS devices must have an MTD app installed).
Bring Your Own Device (BYOD)	Limited MDM to a managed segment; user privacy must be maintained (per DoD policy).	The primary security measure to prevent any DoD data from residing on the personal, un-trusted device.	Detects threats on the entire underlying personal device that could steal credentials, mirror the screen, or compromise the virtual session, ensuring the non-government device is a trusted viewer.	DoD CIO Use of Non-Government Owned Mobile Devices Memo (mandates protection/isolation on personal devices).

Lookout: The Unbreakable Shield for the Warfighter and the Mission

Lookout's MTD solution is essential, not optional.—it is the critical security layer that closes this unacceptable gap. It defends the entire mobile attack surface—the device, the apps, the networks, and the warfighter. Unlike basic virtualization, Lookout terminates threats before they ever get a foothold near mission systems, directly addressing the requirements of the Apple iOS/iPadOS STIG for Mobile Threat Detection.

To learn more, visit lookout.com

Conclusion: The Only Path to Mission Assurance

The answer for security-conscious DoD organizations is brutally clear: The Triad of Protection:

- MDM: Enforces compliance and device lockdown
- VMI: Isolates sensitive data in the cloud
- Lookout (MTD): Protects the device, the warfighter, and the mission against Zero-Day and advanced attacks

This is the only triad that ensures a true Zero Trust approach, and guarantees secure access to mission-critical data while protecting the warfighter.