VMware Workspace ONE Mobile Threat Defense

FedRAMP Moderate Authorized through the Lookout, Inc. Joint Authorization Board (JAB) P-ATO

Security Threats to Mobile Devices

- Malware
- Phishing and malicious content
- Machine in the middle attacks and rogue networks

Mobile Vulnerabilities

- OS version and update adoption
- Out-of-date applications
- iOS, Android and ChromeOS

Mobile Behaviors and Configurations

- Jailbreak / root access
- Wi-Fi auto join
- Leaky apps

Today's mobile threat landscape is diverse, and mobile workstyles call for specialized protection from phishing and application, device, and rogue network originated threats. VMware Workspace ONE Mobile Threat Defense was created with comprehensive mobile protection in mind. Through integrations with the Workspace ONE platform, mobile security is easy to deploy and manage, and offers enhanced protection designed to secure your workspace and enhance Zero Trust initiatives.

Why mobile devices need specialized security

By design, smartphones and tablets are a powerful way to connect with work and personal resources, from any location. In the hybrid workspace, mobile becomes a seamless part of an employee's experience to use a device of their choice, to work on on the go.

Mobile threats are increasing, both in quantity as well as in variety. Like desktops, mobile devices are at risk for phishing and content exploitation, and that risk extends from email to SMS, messaging apps, and social media. Anticipating and responding to the breadth of existing threats as well as yet-to-be-identified risks requires a large base of threat knowledge and data, and on-device solutions made specifically for mobile.

The Solution: Workspace ONE Mobile Threat Defense

Workspace ONE Mobile Threat Defense addresses the dangers of phishing and web content, as well as threats, vulnerabilities, and behaviors unique to mobile. Integrations with the Workspace ONE platform can simplify deployment and management. Protection and remediation can be automated to secure your workspace and enhance Zero Trust initiatives.

Mobile Threat Defense is Federal Risk and Authorization Management Program (FedRAMP) Moderate authorized through the Lookout, Inc. Joint Authorization Board (JAB) (Provisional Authority to Operate (P-ATO). Available as a cloud-hosted, multi-tenant Software-as-a-Service (SaaS) offering, Mobile Threat Defense integrates with Workspace ONE Unified Endpoint Management (UEM), along with Workspace ONE Access, Workspace ONE Intelligent Hub, and Workspace ONE Intelligence. For State, Local and Educational (SLED) customers, VMware Workspace ONE UEM, Workspace ONE Access, Workspace ONE Intelligence are StateRAMP Moderate authorized. Mobile

Preventative Measures to Address Mobile Security Threats

Connect with Workspace ONE Intelligence or Workspace ONE Risk Analytics to:

- Aggregate view of events across users and device types
- Interconnect endpoint, app, and identity analytics; CVE data; and threat data
- Automate remediation of devices back to secure and compliant state
- Flag users and devices for investigation and follow up
- Notify users of issues that require self-remediation

Threat Defense is StateRAMP Moderate authorized through the Lookout, Inc. Joint Authorization Board (JAB).

Workspace ONE Mobile Threat Defense addresses:

Application-based threats including mobile malware, app vulnerabilities, and risky application behaviors and configurations.

Web and content vulnerabilities exposed through phishing via email, SMS, and messaging apps. This includes malicious URLs; malicious web pages, videos, and photos; and web and content behaviors and configurations.

Zero-day threats and device vulnerabilities including jailbreak and root access detection. Device risk including OS version and update adoption.

Phishing and malicious web content delivered via email, SMS, and mobile apps. The phishing and content protection feature is designed to detect and prevent access to malicious links across all mobile apps.

Machine-in-the-middle attacks and risky behaviors such as SSL certificate stripping; forcing weaker algorithm negotiation; anomalous application network connection activity; and vulnerabilities associated with rogue Wi-Fi.

Workspace ONE Mobile Defense incorporates technologies from Lookout, a leader in the mobile security space. Workspace ONE Mobile Threat Defense employs innovations derived from Lookout investments in threat discovery and analysis and mobile security application development.

What makes Workspace ONE Mobile Threat Defense unique

With the advent of Workspace ONE Mobile Threat Defense, many threats can be simply and effectively addressed with Workspace ONE UEM via the unique integration of mobile security features into Workspace ONE Intelligent Hub.

Integration of Workspace ONE Mobile Threat Defense with Workspace ONE Intelligent Hub means that there are no separate apps or agents to deploy, and vital information is conveyed via a resource that employees use for work.

Exclusive to VMware, we offer:

Integration with Workspace ONE Intelligent Hub

By integrating mobile security protection into Hub, security become easier to deploy across devices. Workspace ONE Intelligent Hub integration can detect issues and notify users of remediation actions to take without the deployment of additional security applications to mobile devices. This integration is available via Workspace ONE Intelligent Hub enrolled and registered modes, simplifying the delivery of protection to both corporate and as personal devices.

Phishing and content protection

Workspace ONE Mobile Threat Defense helps address the risk of threat actors sidestepping security controls – including corporate

We can instantly identify and monitor advanced cyberattacks or data breaches on iOS or Android devices. This increases employees' mobility without compromising safety.

All this happens within the centrally managed VMware Workspace ONE platform.

-Petra Cremer, Information Security consultant, Municipality of Enschede

Web filtering has been challenging to enable on mobile devices in the past. Workspace ONE Mobile Threat Defense phishing and content protection is unique because it is built directly into Workspace ONE Tunnel and works seamlessly with other Tunnel capabilities, such as secure traffic tunneling to the data center or cloud-based applications; single sign-on; and posture-based access controls. Unlike traditional VPNs, Tunnel is a proxy for secure access that supports per-app or full device secure tunneling of traffic. Tunnel provides zero trust network access, limits corporate network exposure, and preserves employee privacy.

Why VMware

Workspace ONE Mobile Threat Defense offers an integrated approach to better visibility and control with the Workspace ONE platform.

Interconnecting security and management can help eliminate silos, speed time to value of information, and address risk in real time. Workspace ONE Mobile Threat Defense helps management and security teams glean value from telemetry and threat information by aggregating data, applying AI and machine learning, then triggering alerts and remediation.

Workspace ONE Intelligence makes it possible to associate telemetry data from endpoints, applications, and users with threat information from Workspace ONE Mobile Threat Defense. Reporting and insights can be displayed in aggregate for team review. Specific conditions can trigger auto remediation via Workspace ONE UEM so that risks are addressed in real time. Users can be automatically notified of issues that require self-remediation; users and devices can also be flagged for follow up.

How to get started

Please reach out to your VMware account manager or contact VMware Sales if you're interested in adding Workspace ONE Mobile Threat Defense to your existing FedRAMP environment. For more information on how VMware is helping agencies accelerate innovation across the public sector, please visit: VMware Cloud Trust Center.