Workspace ONE Mobile Threat Defense

Solution Overview

Advanced Security for:

Corporate Smartphones

Employee Smartphones (BYOD)

Managed and Unmanaged Devices

Mobile Threats

Machine in the middle attacks and rogue networks

- SSL certificate stripping
- Forcing weaker algorithm negotiation
- Port scans

Malware

- Spyware and surveillance ware
- Sideloaded apps

Phishing and malicious content

- Email, SMS, messaging and social media apps
- Malicious URLs, web pages, videos, and photos

Mobile Vulnerabilities

- OS version and update adoption
- Out-of-date applications

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.

Mobile threats are increasing, both in quantity as well as in diversity. 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.

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.

Easy to Deploy and Manage

Integrated with Intelligent Hub; or via the Workspace ONE Mobile Threat Defense mobile app

Types of Mobile Devices Supported

Android phones and tablets

iOS phones and tablets

Chrome OS (limited features)

Integrated and Automated

Connect with Workspace ONE Intelligence or Workspace ONE Risk Analytics in order 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

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

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.

Bringing together management and security with Workspace ONE

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:

Protection Built into Workspace ONE Intelligent Hub

By integrating mobile security protection into Hub, security become easier to deploy across devices. Hub integrated protection addresses vulnerabilities, behaviors and configurations, and threats including malware, zero day, and machine in the middle attacks.

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.

For phishing and content protection, or implementation without UEM:

Application-Based Protection via the Workspace ONE Mobile Threat Defense App

The Workspace ONE Mobile Threat Defense app is required for phishing and content protection. The app is also required for Android devices when dual enrollment of work and personal profiles is required; this is a use case where personal profile security is required in addition to work profile security. When the app is

implemented, all Workspace ONE Mobile Threat defense security functions including detection and notification will occur via the app. The Workspace ONE Mobile Threat Defense app can be installed on non-Hub enrolled devices, lending support to unmanaged device scenarios. In the case of unmanaged devices, the Workspace ONE Mobile Threat Defense app can be distributed to users via email.

This advanced mobile security is powered by Lookout, an industry leader.

Best-in-class mobile security powered by Lookout

Lookout protection leverages AI and behavioral insights generated from over 200 million devices, 150 million apps, and 4.5 billion web items. Machine learning and predictive intelligence help detect known and emerging threats.

With more than 175 patents and a record in mobile security that includes creating the first mobile security product, Lookout is an innovative partner. In addition to powering Workspace ONE Mobile Threat Defense, Lookout is a Workspace ONE Trust Network partner, providing integrations between their mobile security solution and Workspace ONE Intelligence.

Eliminate silos and automate reporting and remediation 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 can help 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.

Coordinated endpoint protection

Workspace ONE Mobile Threat Defense extends advanced security in the Anywhere Workspace to Android, iOS, and Chrome OS devices. Endpoint protection solutions available from VMware include Carbon Black Cloud, offering protection for virtual desktops and Windows, Mac, and Linux devices.

How to get started

For more information, contact your sales representative or reach out to VMware at https://www.vmware.com/company/contact_sales.html.