SOLUTION OVERVIEW

Omnissa Workspace ONE Mobile Threat Defense

At a glance

Secure your hybrid workforce with comprehensive, specialized mobile protection that's easy to deploy and manage, and seamlessly integrates with the Omnissa platform.

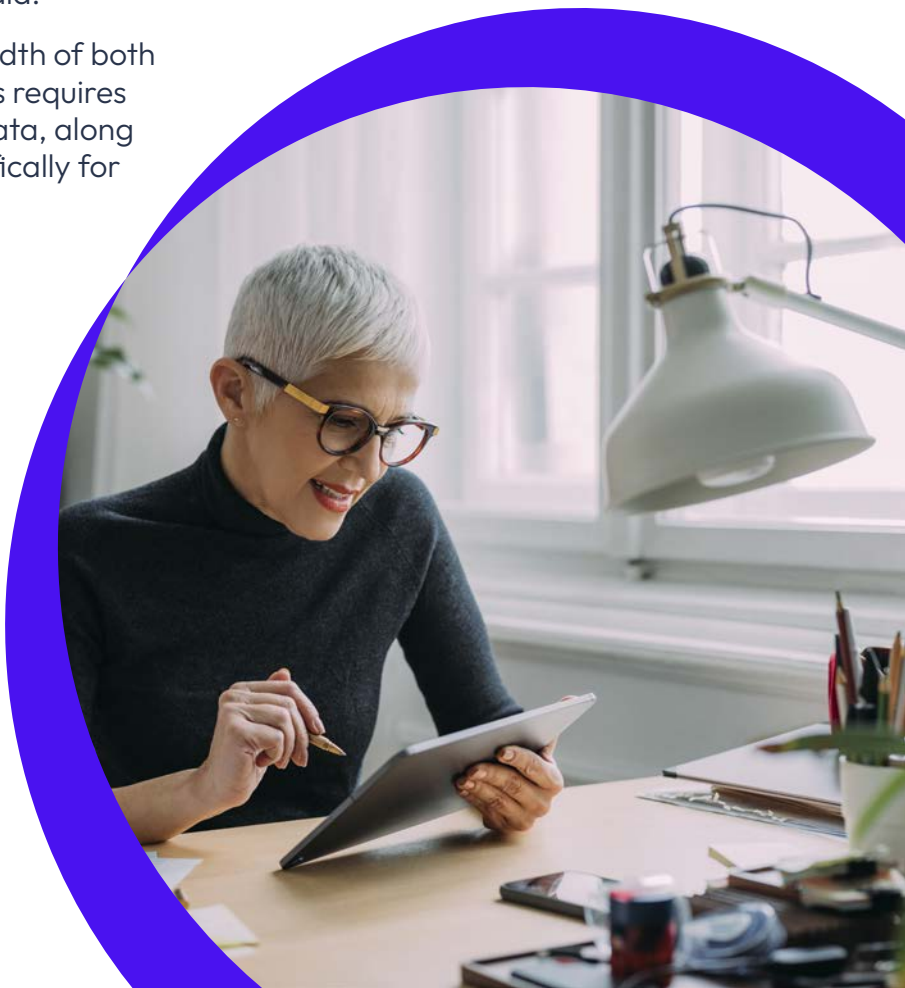
Advanced mobile security for corporate- and employee-owned devices

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 work on the go.

However, as mobile work continues to increase, so do mobile threats, both in quantity and variety. Just 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 both existing and yet-to-be-identified threats requires a large base of threat knowledge and data, along with on-device solutions designed specifically for mobile operating systems and apps.

This is where Omnissa Workspace ONE® Mobile Threat Defense comes in.



omnissa™

Comprehensive protection for mobile work

Workspace ONE Mobile Threat Defense is designed to address a full range of mobile threats including:

Application-based threats

These include mobile malware, app vulnerabilities, and risky application behaviors and configurations.

Web and content vulnerabilities

Initially exposed through phishing via email, SMS, and messaging apps, these vulnerabilities include malicious URLs; malicious web pages, videos, QR codes, and photos; and web and content behaviors and configurations.

Zero-day threats and device vulnerabilities

Device risks include OS version and update adoption, as well as jailbreaking and rooting.

Phishing and malicious web content

These threats are initially delivered via email, SMS, and mobile apps. Phishing and content protection is designed to detect and prevent access to malicious links across all mobile apps.

Machine-in-the-middle attacks

These include risky behaviors such as SSL certificate stripping; forcing weaker algorithm negotiation; anomalous application network connection activity; and vulnerabilities associated with rogue WiFi.

21 seconds
is the median time for users to click on a phishing simulation link*

68%
of breaches include the human element*

92%
of industries report ransomware attacks continue to be the top threat*

*Source: Verizon Data Breach Investigations Report, 2024.

The Mobile Threat Defense difference

Three main attributes make Mobile Threat Defense unique among mobile security solutions.

1. Integration with Workspace ONE Intelligent Hub

Intelligent Hub is where employees can find the tools they need to be productive, including single sign-on capabilities, a unified app catalog, people search, remote troubleshooting assistance, and more. Through a unique integration with Intelligent Hub, Mobile Threat Defense provides continuous, advanced mobile security via an application employees consistently use. There are no separate apps or agents to deploy, and vital information—remediation actions, for example—is conveyed directly via Intelligent Hub, simplifying the delivery of protection to both corporate and personal devices.

2. Phishing and content protection

Public information and turnkey phishing toolkits available on the dark web make it easy for threat actors to target large populations of employees via phishing attacks. Mobile Threat Defense provides protection against potential phishing activity across email, SMS, general web content, and messaging and social apps on iOS, ChromeOS, and Android devices.

Mobile Threat Defense detects attempts to load phishing and malicious web content from applications—and from background activities on the device—and blocks the content accordingly. This is achieved through an integration with Workspace ONE® Tunnel, which sends URLs that the device attempts to load to the Lookout Security Graph for advanced analysis. This feature leverages real-time intelligence, machine learning algorithms, and a comprehensive database of known phishing URLs.

3. Leading technologies and rich insights

Mobile Threat Defense incorporates innovative technologies from Lookout, a leader in mobile security application development, threat discovery, and analysis.

By interconnecting security and management, Mobile Threat Defense helps to eliminate silos, speed time to value of information, and address risks in real time. In addition, it helps management and security teams glean value from telemetry and threat information by aggregating data, applying AI and machine learning, and then triggering alerts and remediation.

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

> 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 Workspace ONE platform.
>
> **Petra Cremer**
> Information Security consultant, Municipality of Enschede

omnissa™

FY24-7688-OMN-WKSP1-MOBILE-THREAT-DEFENSE-SO-USWEB-A4-20241014 10/24

C2890471-1224