

# Protecting Mobile Devices from Web Threats

Provides users with fast, secure, and reliable access to websites and applications from mobile devices.

## Benefits:

- Seamless integration with Workspace ONE UEM for iOS and Android
- 100 percent security against web-based threats without impacting the user experience
- Protection from web links accessed from emails and other apps
- Global Elastic Cloud with low latency and connectivity from any location

The combination of Menlo Security's Global Cloud Proxy with an Isolation Core™ and the VMware Workspace ONE™ platform powered by AirWatch provides 100 percent protection for your users' mobile web traffic—including protection from zero-day web malware, drive-by downloads, ransomware, and targeted phishing attacks. The integrated offering supports iOS as well as Android with the Workspace ONE secure web browser.

Unlike legacy security products, the Menlo Security Global Cloud Proxy with an Isolation Core™ does not rely on a detect-and-respond approach, but rather on the assumption that all web content is risky and potentially malicious, and thus neutralizes it by isolating it in the cloud.

The integrated offering provides users with fast, secure, and reliable access to websites and cloud applications from mobile devices running iOS and Android.

## Overview

Mobility and digital transformation have caused organizations to accelerate their journey toward Secure Cloud Transformation for economic and competitive reasons. As a result, organizations are faced with the challenge of providing secure access to corporate and SaaS applications from a variety of endpoints, including mobile devices.

The proliferation of mobile devices has significantly increased the attack surface for common threat vectors, such as:

- Phishing emails on personal or corporate accounts
- Text messages with shortened links to malicious websites
- Browser URL addresses that are obscured
- Apps containing URLs that download malicious plug-ins

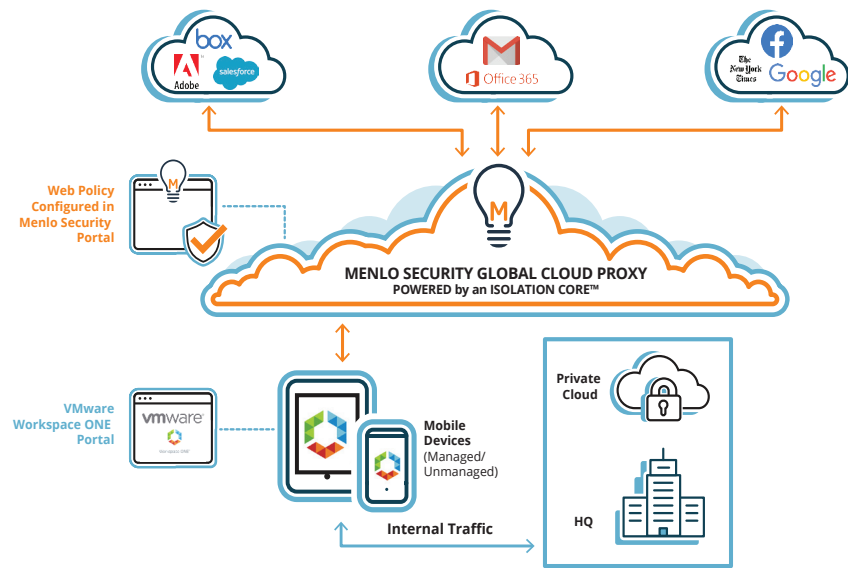


It takes only one tap on a mobile device to open the door for cyberattackers. That's because URLs are truncated to preserve user experience, making it impossible to determine if a URL connects to a genuine website. This problem exists whether it's a URL in an app that unknowingly connects to a malicious ad network, or a link in a personal email designed to trick a user into unwittingly offering corporate credentials.

## Menlo Security and VMware Workspace ONE

Workspace ONE UEM directs web browsing traffic to the Menlo Security Global Cloud Proxy by creating an SDK Profile for both iOS and Android that uses the Menlo Proxy Auto Configuration (PAC) URL. Web browsing traffic can then be fully controlled through the policies and rules set in the Menlo Cloud Admin portal.

The integrated offering enables isolation of web traffic from the Workspace ONE secure browser.



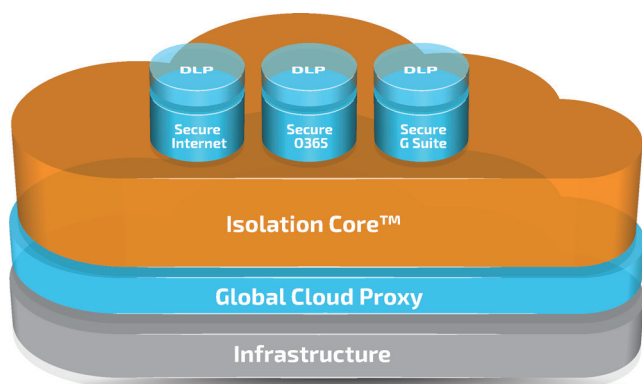
This integrated offering enables isolation of web traffic from the Workspace ONE secure browser to mitigate risks from malicious websites, downloads, and links from emails and messages—while enabling seamless access to corporate and SaaS applications in the cloud.

## Menlo Security Global Cloud Proxy

Menlo Security's Global Cloud Proxy with an Isolation Core™ enables safe viewing of web content and documents by executing all active content in the cloud, away from the endpoint, while providing a native and seamless user experience across all endpoints, including mobile devices.

In addition to providing 100 percent security with its Isolation Core™, Menlo Security gives administrators the ability to set acceptable use policies, such as for posting on social media sites, and to block malicious activity, including file uploads and downloads.

Policies can be applied by user, group, file type, or website categorization to determine when the content is blocked or rendered in read-only mode, or when the original content should be accessible.



Menlo Security's Global Cloud Proxy with an Isolation Core™ enables safe viewing of web content by executing all active content in the cloud, away from the endpoint.

## VMware Workspace ONE

VMware Workspace ONE UEM provides users with an intuitive browsing experience and seamless access to back-end services while protecting sensitive corporate data, configured via the Workspace ONE UEM console. Featuring a native user experience and single sign-on across websites and web apps, Workspace ONE UEM provides users with instant access to Internet and intranet sites without requiring a VPN connection. Seamless integrations with other business apps allow users to perform daily workflows on the go without compromising productivity.

To find out how Menlo Security can provide your company with protection against cyberattacks, visit [menlosecurity.com](https://menlosecurity.com) or contact us at [ask@menlosecurity.com](mailto:ask@menlosecurity.com).

## About Menlo Security

Menlo Security protects organizations from cyberattacks by eliminating the threat of malware from the web, documents, and email. Menlo Security has helped hundreds of Global 2000 companies and major government agencies achieve Secure Cloud Transformation. The Menlo Security Cloud Platform scales to provide comprehensive protection across enterprises of any size, without requiring endpoint software or impacting the end-user experience. The company was named a Visionary in the Gartner Magic Quadrant for the Secure Web Gateway.  
© 2020 Menlo Security, All Rights Reserved.

**Contact us**  
[menlosecurity.com](https://menlosecurity.com)  
(650) 614-1705  
[ask@menlosecurity.com](mailto:ask@menlosecurity.com)

