PARTNER:
SOLUTION BRIEF

Menlo Cloud Security Platform Powered by an Isolation Core™ and VMware Workspace ONE

Protecting mobile devices from web threats

The challenge

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, etc.

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 via emails and other apps
- Global Elastic Cloud with low latency and connectivity from any location

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 the URL is in an app that unknowingly connects to a malicious ad network or the URL is in a link in a personal email designed to trick the user into unwittingly offering corporate credentials.

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

Menlo Cloud Security Platform—Powered by an Isolation Core™

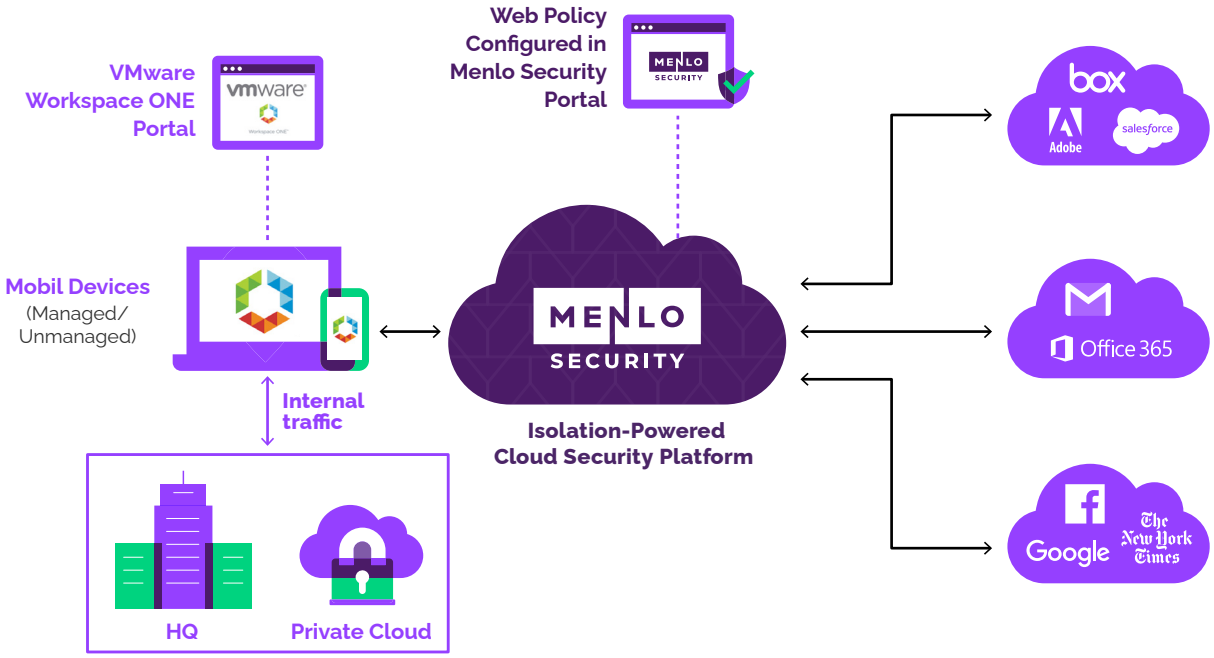
The Menlo Cloud Security Platform enables safe viewing of web content and documents by executing all active content in the cloud—away from the endpoint device—while providing a native and seamless user experience. Unlike legacy solutions, the Menlo Cloud Security Platform does not rely on a detect-and-respond approach, but rather on the assumption that all web content is risky and hosts potentially malicious content. This approach eliminates the need to make an "allow or block" determination based on coarse categorization and detailed analysis.

The Menlo Cloud Security Platform instead offers an option to "isolate" potentially risky or uncategorized websites. Once content is isolated, malware-free content is delivered safely and efficiently to the end user's browser, with no impact on user experience or productivity, and without requiring an endpoint agent or browser plug-ins. All active content such as JavaScript and Flash, whether good or bad, is fully executed and contained within Menlo Security's cloud-based Isolation Core™. This eliminates the possibility of malware ever leaving the isolated web browsing session and infecting the endpoint. This approach restores 100 percent confidence in the security posture and enables security teams to empower worry-free and productive clicking, downloading, and browsing for end users.

The Menlo Cloud Security Platform also gives administrators the ability to set and enforce acceptable use policies to block malicious activity, including file uploads and downloads. Policies can be applied by user, group, file type, or website categorization to determine when content is blocked or rendered in “safe preview” mode.

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.



Menlo Cloud Security Platform Powered by an Isolation Core™ combined with VMware Workspace ONE

The Menlo Cloud Security Platform along with the VMware Workspace ONE UEM platform 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 enables isolation of web traffic from the Workspace ONE secure browser or other third-party browsers on both iOS and Android devices.

Workspace ONE UEM directs web browsing traffic to the Menlo Cloud Security Platform by creating an SDK profile for both iOS and Android that uses the Menlo Proxy Auto Configuration (PAC) URL. The web traffic can then be controlled in Workspace ONE UEM with policies and rules set in the Menlo Cloud Admin portal. This enables the integrated solution 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.

To find out how Menlo Security can provide your company with protection against cyberattacks, visit menlosecurity.com or contact us at ask@menlosecurity.com.

MENLO SECURITY

To find out more, contact us:

menlosecurity.com

(650) 695-0695

ask@menlosecurity.com

About Menlo Security

Menlo Security enables organizations to eliminate threats and fully protect productivity with a one-of-a-kind, isolation-powered cloud security platform. It's the only solution to deliver on the promise of cloud security—by providing the most secure Zero Trust approach to preventing malicious attacks; by making security invisible to end users while they work online; and by removing the operational burden for security teams. Now organizations can offer a safe online experience, empowering users to work without worry while they keep the business moving forward.