Menlo Security

BRIEF

Enforce Acceptable Use Policies with Secure Cloud Transformation Powered by Isolation

The Menlo Security Cloud Platform powered by an Isolation Core™ opens up more of the Internet to users without impacting the native web browsing experience.

Benefits:

- 100% malware-free email and web browsing
- AUP enforcement without impacting the native browsing experience
- Opens up more of the Internet to users
- Saves IT costs by eliminating help desk requests to unblock legitimate sites

It's no secret that business today is conducted over the Internet. Yet the Internet is fraught with malicious content, from fake login portals to malware-infected sites that look legit and are designed to trick users into providing access to corporate systems. Legacy secure web gateway (SWG) solutions give enterprises the ability to allow or block Internet content based on policies, but how do you know what to block and what to allow? You can't block all Internet access. Nor can you simply allow unfettered access. A new approach is needed.

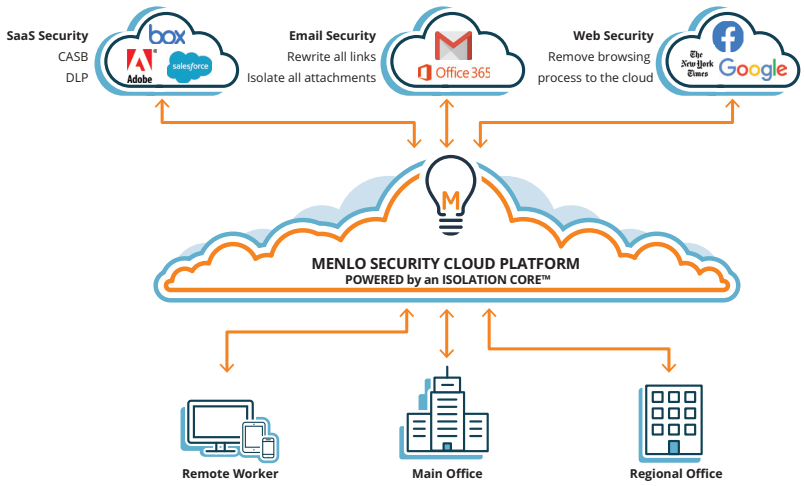
The Isolate-or-Block Approach with Menlo Security

Rather than determine what web content is legitimate, organizations should just assume that all web content is risky and all websites host potentially malicious content. The resulting zero trust approach eliminates the need to make an allow-or-block determination based on coarse categorization. An isolate-or-block policy is needed instead. Menlo Security enables this approach by intercepting all web browsing sessions so acceptable use policies (AUPs) can be applied to each session.

With Menlo AUPs, all web content is fetched and executed in the Menlo Security Cloud Platform powered by an Isolation Core™ instead of on users' browsers. It is here that AUPs can be enforced, authorizing or blocking web interactions at a granular level. For content that is allowed, Menlo Adaptive Clientless Rendering™ (ACR) efficiently delivers authorized content to the end user's browser with no impact on user experience or productivity, and without requiring special client software or plug-ins. This approach restores 100 percent confidence in the security posture for security teams, enabling a worry-free and productive clicking, downloading, and browsing experience for end users.

The Menlo Security Cloud Platform safely and confidently allows users unrestricted access to unknown and uncategorized websites without impacting productivity or risking malware attacks.

Zero Trust Internet Architecture



Enabling AUPs

The Menlo Security Cloud Platform powered by an Isolation Core™ safely and confidently allows users unrestricted access to unknown and uncategorized websites without impacting productivity or risking malware attacks. This also extends to documents, allowing users to access all documents on the web without worrying about malware being downloaded on their device. Users are also prevented from entering credentials or exposing personally identifiable information (PII) on suspicious web forms by making the site read-only. Security administrators can also use Menlo to enforce AUPs by blocking inappropriate or offensive content on the web.

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

Contact us
menlosecurity.com
(650) 614-1705
ask@menlosecurity.com