

Cloud App Isolation

Cloud Application Security with Our Isolation Core™



Menlo Security's Cloud App Isolation uses cloud-based isolation to provide unmatched safety for networks that rely on SaaS applications. Cloud App Isolation outperforms non-isolated, less reliable solutions by providing complete control and visibility into cloud app traffic data.

Cloud Applications Are a Point of Attack

With 29 percent of all attacks using legitimate cloud services to launch an attack, protecting your digital workforce is a challenging task. And once an attacker is inside the network, they can use the same cloud app to siphon valuable information out of the organization.

Cloud apps are potential vectors for attack. Workers frequently use cloud applications that are hidden to network administrators—a common problem known as “shadow IT.” These apps may contain vulnerabilities that are invisible to the admin and pose a risk to the network.

In this environment, network administrators will find themselves struggling to keep up with new threats arriving from unsanctioned cloud applications day after day.

Cloud App Isolation for Application Security

Menlo Security's Cloud App Isolation solution works with an external cloud access security broker (CASB) service to provide management control, visibility, and data loss prevention for cloud apps used within your network.

Key Differentiator

Cloud-based isolation enhances the protective measures of CASB. As with our Cloud DLP product, our Isolation Core™ controls the channel between the endpoint device and our cloud server. That feature allows us to more reliably discover and block file uploads through cloud-based apps.

Top Use Cases at a Glance

Granular Policy Control

- Discover and control access to unsanctioned (unauthorized) cloud apps
- Allow, block, or isolate apps according to policy settings

Data Loss Prevention

- Prevents data exfiltration through cloud applications
- Menlo Security provides 100 percent data inspection with our Isolation Core™



Cloud App Isolation provides the visibility and management tools that admins need to protect their network. Cloud App Isolation works by controlling cloud application traffic based on a list of sanctioned cloud apps supplied from the CASB admin.

The feature then enables admins to view policies globally and manage access to cloud apps on a per-user basis. App-specific policies can be controlled via your external CASB provider.

The Bottom Line

Cloud App Isolation works with other Menlo Security product suite features to create a powerful solution that isolates cloud apps to stop data loss from occurring through these apps and to prevent shadow IT. With global insights, admins are able to pinpoint problem users by monitoring activities across cloud apps, web browsing behavior, and document uploads.

Feature	Benefits
Isolated Access to Cloud Apps	<ul style="list-style-type: none">• Allow, block, or isolate cloud apps according to policy settings• Place risky, unsanctioned cloud apps into read-only mode
Data Loss Prevention for Cloud Apps	<ul style="list-style-type: none">• 100% cloud app data inspection through our Isolation Core™• Protect company data from accidental uploads or malicious extraction to the web• Notify users and administrators when a policy violation occurs
External CASB Integration	<ul style="list-style-type: none">• Connect to selected external CASB providers for fast, flexible implementation• Apply app-specific policies using an external provider
User/Group Policy and Authentication	<ul style="list-style-type: none">• Apply policies quickly across the entire organization• Reporting tools to help admins keep track of their environment• Locate risky users in the organization
Analytics and Reporting	<ul style="list-style-type: none">• Built-in and custom reports and alerts with detailed event logs and built-in traffic analysis• Built-in and custom queries for flexible exploration and analysis of data• Export log data using API to third-party SIEM and BI tools



Menlo Security's Product Suite

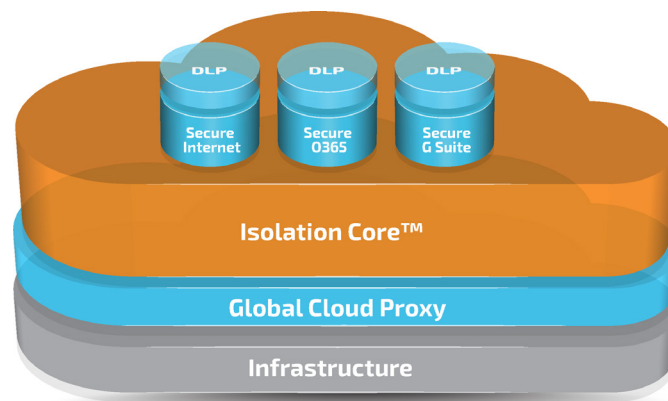
Menlo Security's Cloud App Isolation has been crafted to help customers with moving security to the cloud along with our suite of enterprise-ready products.

Global Cloud Proxy—Provides SSL inspection and direct-to-Internet connectivity for fast access to SaaS services. Compatible with SD-WAN implementations.

Secure Internet—Extends the features of Global Cloud Proxy with the addition of our Isolation Core.™

Secure Office 365—Ensure that Office 365 deployments remain secure without user performance degradation when accessing Office 365 applications via the Menlo Security Global Cloud Proxy. Menlo Security's Isolation Core™ uniquely protects against malicious email links and attachments as part of this suite. Optionally, you can add data protection capabilities in the form of Cloud DLP for email.

Secure G Suite—Many organizations are adopting G Suite email, and with the Menlo Security Isolation Core™, they're protected from malicious email links and attachments. Optionally, you can add data protection capabilities in the form of Cloud DLP.



To learn more about how to prevent data loss and ensure secure cloud access for your employees without posing a risk to the organization, visit menlosecurity.com or email us at ask@menlosecurity.com.

About Menlo Security

Menlo Security protects organizations from cyberattacks by seeking to eliminate the threat of malware from the web, documents, and email. Our cloud-based Isolation Platform scales to provide comprehensive protection across enterprises of any size, without requiring endpoint software or impacting the end-user experience. Menlo Security is trusted by major global businesses, including Fortune 500 companies and financial services institutions.

© 2020 Menlo Security, All Rights Reserved.

Contact us

menlosecurity.com

(650) 614-1705

ask@menlosecurity.com

