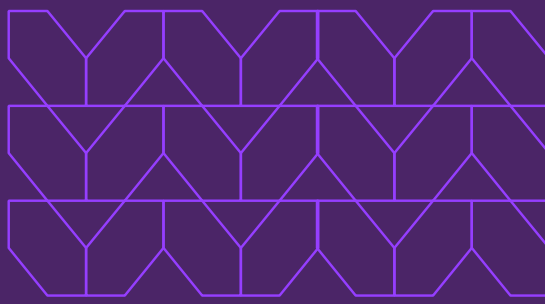
MENLO SECURITY

Data Sheet

Cloud Access Security Broker (CASB)

Empower users with safe access to SaaS platforms.

Work today is done largely on the Internet and in the browser. Highly distributed and mobile users connect and collaborate through dynamic, flexible Software-as-a-Service (SaaS) platforms that bring powerful functionality and capabilities to workers wherever business takes them. However, SaaS platforms introduce risk by requiring a direct, persistent connection between the user and the platform—leading to a lack of enterprise visibility and control that malicious actors can leverage by using SaaS as an attack vector. Security teams need a new approach for securing SaaS access for users without inhibiting today's highly distributed, collaborative culture.

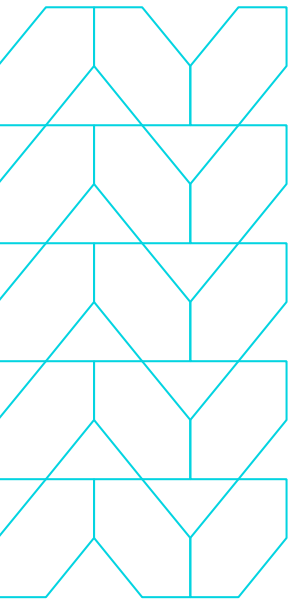


Three things to know:

Modern applications in the form of cloud apps and services allow today's users to access critical business information and tools wherever business takes them.

These apps often require a direct, persistent connection between the user and the platform—effectively cutting out the enterprise security team.

Menlo Security CASB allows highly distributed and mobile users to directly access SaaS platforms safely and confidently, without interruption.



Product overview

Menlo Security Cloud Access Security Broker (CASB) gives users safe access to SaaS platforms while providing security teams with the deep visibility and control they need to stop malware in its tracks. Menlo does this with an isolation-based approach that allows users to securely access modern applications while eliminating the need to backhaul Internet traffic to a central data center. This allows organizations to provide secure local Internet breakouts to distributed and remote users at cloud scale.

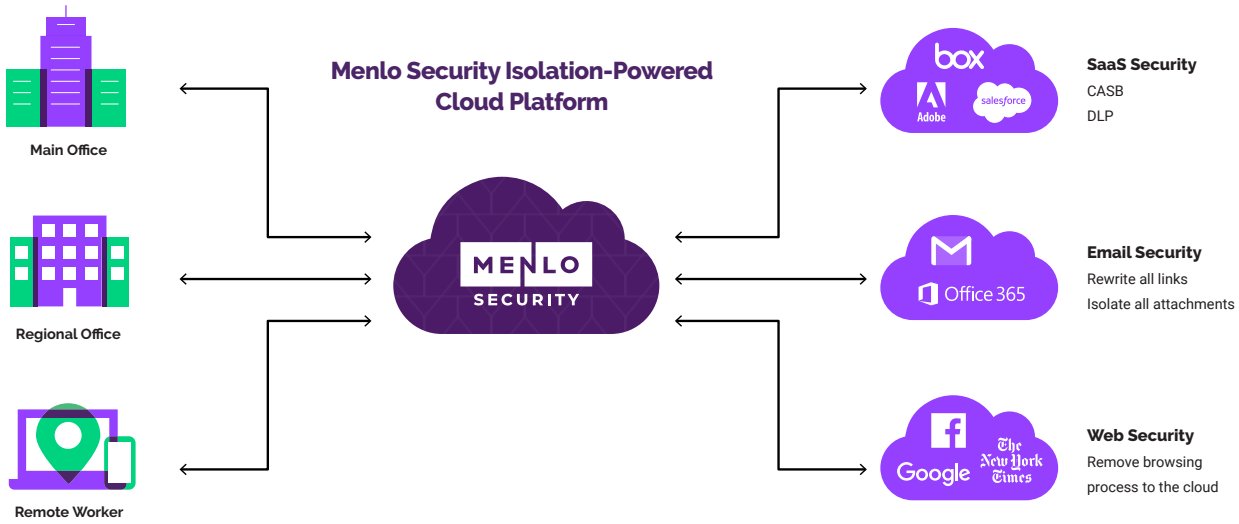
These flexible, mobile, cloud-delivered local Internet breakouts allow users to safely connect directly to SaaS platforms with all the same security, visibility, and controls that protect the data center.

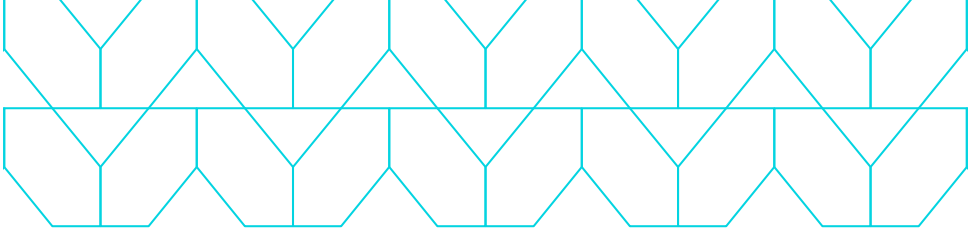
Menlo Security CASB provides real-time visibility and controls access for user activity across sanctioned and unsanctioned applications. The fully integrated service simplifies policy creation and administration, allowing you to outsmart known and existing threats as well as unknown and future threats.

Unique to Menlo is its Isolation Core™, which protects users from unsanctioned applications as SaaS content—including files and documents—is securely accessed through the Menlo Security Cloud Platform.. Menlo Security efficiently delivers only safe and authorized content to end-user browsers, with no impact on application experience.

CASB from Menlo Security also gives security teams visibility and the ability to apply the appropriate security controls to all traffic, regardless of physical location or the underlying connection. This includes data loss prevention (DLP) for controlling the upload of sensitive information to cloud sharing sites such as OneDrive, Google Drive, Box, and Dropbox—as well as the ability to control application functions such as login, upload, download, share, create, and delete. Administrators can even apply less restrictive policies to sanctioned apps versus unsanctioned apps while still retaining threat protection capabilities through Menlo's document isolation, content scanning, and integrated DLP.

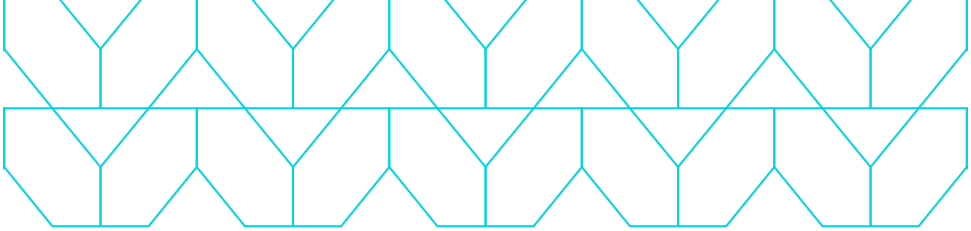
Most importantly, Menlo provides this visibility and control across modern apps without relying on vulnerable VPN services or physical security appliances that impact performance and add IT overhead.



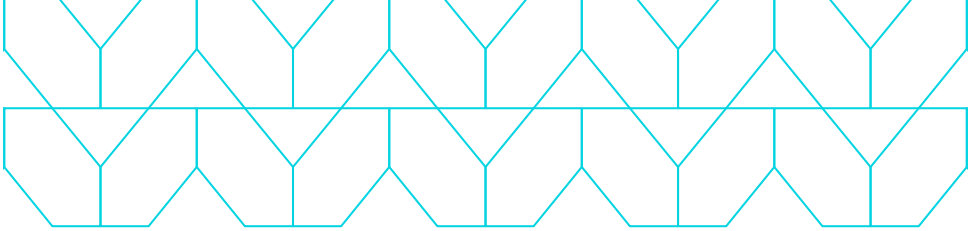


Menlo Security Cloud Access Security Broker: Key features and benefits

Feature	Benefits
Web Isolation	Safe viewing of websites by executing all active and risky web content (JavaScript and Flash) in a remote cloud-based browser.
	All native web content is discarded in disposable containers using stateless web sessions.
Document Isolation	Safe viewing of documents by executing all active or risky active content in the cloud, away from the endpoint.
	Option to download safe cleaned or original versions of documents.
	Granular policies to limit document access based on file type and user.
Cloud Security Platform	Centrally configure web security and access policies that are instantly applied to any user on any device.
	Hybrid deployment support with no differences in a policy.
URL Filtering and Acceptable Use Policies (AUPs)	Limit user interaction for specific categories of websites (75+ categories).
	Control employee web browsing via granular policies (user, group, IP).
	Document access controls, including view only, safe, or original downloads based on file type.
Bandwidth Control	Enable user/group policy to predictably control bandwidth (such as video content) to enhance the user experience.
Content and Malware Analysis	Integrated file analysis using file hash check, anti-virus, and sandboxing.
	Integration with existing third-party anti-virus and sandboxing solutions.
	Inspect risky content and detect malicious behavior of all original documents downloaded.



Feature	Benefits
Analytics and Reporting	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.
Encrypted Traffic Management	Intercept and inspect TLS/SSL-encrypted web browsing traffic.
	Provisionable SSL inspection exemptions to ensure privacy for certain categories of websites.
	Expose hidden threats in encrypted sessions.
Global Elastic Cloud	Secure and optimal web access for remote sites and mobile users anywhere in the world.
	Autoscaling and least-latency-based routing allows connectivity from any location, scaling to billions of sessions per month.
	Rapid provisioning of users.
	ISO 27001 and SOC 2–certified data centers
Native User Experience	Works with native browsers with broad browser support, allowing users to continue to interact with the web like they always have.
	No need to install or use a new browser.
	Smooth scrolling, no pixelation.
User/Group Policy and Authentication	Set and fine-tune policies for specific users, user groups, or content type (all content, risky content, uncategorized).
	Create exceptions for specific users, user types, or content types.
	Integrates with SSO and IAM solutions with SAML support for authentication of users.
Web Gateway	Apply additional security controls on top of isolation services.
	Email isolation, DLP, CASB, FWaaS, global cloud proxy



Feature	Benefits
Data Loss Prevention (DLP)	Restrict document uploads to the Internet.
	Increased visibility for on-premises solutions.
Cloud Access Security Broker (CASB)	Deep visibility of SaaS application traffic to ensure compliance.
	Option to integrate with third-party CASB solutions.
	Granular policy control for SaaS applications and control app functionality such as login, upload, download, share, create and delete.
Connection Methods and Endpoint Support	Proxy Automatic Configuration (PAC)/Agent-based traffic redirection, including an endpoint agent option for Windows and macOS.
	IPSEC/GRE network traffic redirection support
	Seamless integration with top SD-WAN providers.
API Integrations	Seamless SaaS integration to secure web sessions.
	Highly extensible set of standards support APIs and third-party integrations.
	Content APIs
	Policy APIs
	Log APIs with SIEM and log analytics tools such as Splunk, IBM QRadar, and Menlo iSOC
	Validated third-party integrations for SSO, SIEM, MDM, firewall, proxy, AV, sandbox (PAN Wildfire and Cisco ThreatGrid), CDR, and SOAR
	SD-WAN and SASE integrations

Protecting against modern security threats is a top priority for businesses, but existing solutions are limited and reactive. SaaS applications typically require a direct, persistent connection from the user to the platform—creating a critical security gap that malicious actors can leverage as an attack vector. CASB from Menlo Security enables a Zero Trust, isolation-powered approach to cybersecurity by preventing malware and other malicious content originating from SaaS platforms to access the endpoint. Menlo Security also prevents data exfiltration through file uploads to cloud platforms. Most importantly, Menlo ensures that security remains invisible to end users while they work online and removes the operational burden for security teams as they maintain a safe, seamless, and effective environment for all workers.

To learn more about securing the ways people work, visit menlosecurity.com or email 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.