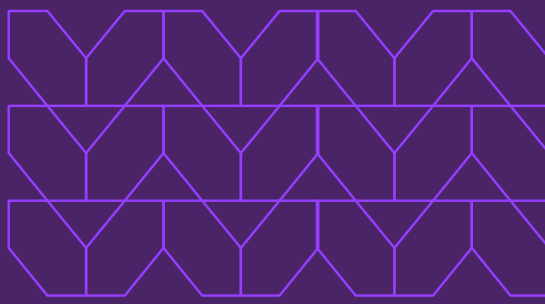
MENLO SECURITY

Data Sheet

Browser Isolation

Protect work by eliminating threats from Internet malware.

There's no way around it. The Internet is a mission-critical business tool for today's enterprises. Widely distributed users need fast, reliable access to websites, cloud apps, and Software-as-a-Service (SaaS) platforms to complete their day-to-day tasks. But the Internet is rife with malicious threats that pose an enormous risk for enterprises. Security teams need a new approach for securing web browsing for users without impacting their ability to work harder and smarter wherever business takes them.



Three things to know:

To be productive, users need safe and reliable access to web-based information, SaaS applications, online documents, collaboration, and other business tools.

Legacy detection-based security approaches fail to protect against modern-day threats such as zero days, credential theft, and ransomware.

Menlo Security Browser Isolation uses a fundamentally different approach to help you stay ahead of the game and eliminate these threats completely.

Product overview

Menlo Security Browser Isolation gives enterprise security teams the visibility and control they need to enable a Zero Trust approach to protecting against Internet malware. Rather than trying to identify threats as malware breaches the perimeter, browser isolation works by routing all web traffic through a cloud-based remote browser before delivering only safe content to the endpoint. It doesn't matter if the web content is good or bad, categorized or uncategorized—Menlo Security Browser Isolation adopts Zero Trust principles by assuming that all content is malicious and treating it accordingly.

Along with browser isolation, Menlo Security converges all secure web gateway capabilities into a single cloud-native platform—including CASB, DLP, RBI, Proxy, FWaaS, and Private Access—to provide extensible APIs and a single interface for policy management, reporting, and threat analytics.

The Menlo Security Cloud Platform is uniquely powered by an Isolation Core™ that enables elastic scaling to support the rapid onboarding of as many users as the enterprise needs.

In addition, fluctuating workforce needs and traffic volumes are accommodated without requiring capacity planning cycles or complex configuration of clients deployed on endpoint devices. This automatically ensures that granular access and security policies are enforced, data leaks are prevented, cloud apps are secure, and compliance is ensured across all devices and locations—while allowing users to natively access the web-based information and productivity tools they need.

In addition to fully enabling the way people work, Menlo Security Browser Isolation gives administrators the ability to set acceptable use policies to block malicious activity—including compromised websites, cybersquatting, file uploads and downloads, social posting, and other unknown threats. Policies can be applied based on user, group, file type, website category, or cloud application to determine when content is blocked, when it is rendered in read-only mode, or when the original content should be accessible. Menlo Security Browser Isolation does this with unmatched performance and scale.

Browser Isolation ensures direct-to-cloud Internet access while providing core proxy capabilities. Being a web proxy, the gateway terminates and proxies Internet traffic, and addresses that traffic through security checks, including URL filtering, sandboxing, data loss prevention, anti-virus scanning, cloud access security broker (CASB), and other converged technologies delivered as a secure web gateway (SWG).

Menlo Security Browser Isolation: 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.
	Smart DOM leverages the power of the DOM to provide a transparent user experience while retaining the security benefits that come with executing active content away from the endpoint.
	DOM Reconstruction confers Smart DOM with key benefits that make it ideal for mobile browsers.
	Accurate rendering that is agnostic to the particular endpoint browser in use and the web features used by the page.
	Power-efficient rendering improves CPU utilization and reduces overall power draw.
	Prioritized bandwidth allocation enables Smart DOM to minimize network usage in the interest of optimal battery life while preserving the user experience.
	Smart DOM does not send active content of any kind to the endpoint, thus breaking the kill chain of modern-day exploits.
	Compatibility with the broader browser ecosystem by transforming the Layer Tree into a semantically rich DOM where text nodes expose text semantics, anchor elements export link semantics, and < i n p u t > elements trigger password manager auto-fill.
Document Isolation	Safe viewing of documents by executing all active or risky active content in the cloud, away from the endpoint.
	Depending on policies in place, offers an option to download safe cleaned or original versions of documents following content scanning, CDR, or third-party malware engine scanning.
	Granular policies to limit document access based on file type and user.
	Provides a completely safe, sanitized, high-fidelity version of the original file with support for print, search, copy/paste, and sharing capabilities. Fully supported on desktop and mobile devices.
	Breadth of supported document types can be rendered in the web-based, secure document viewer.
	Ability to safely view and access files inside Archives through isolation.
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.

Feature	Benefits
Cloud Security Platform	Centrally configure web security and access policies that are instantly applied to any user on any device in any location.
	Hybrid deployment support with no differences in a consistent policy.
Menlo Security Isolation-Powered Secure Web Gateway (SWG)	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, as well as upload and download controls.
	Enable user/group policy to predictably control bandwidth in low-latency, high-bandwidth environments (such as video content) to enhance the user experience.
	Integrated status and dynamic file analysis using file reputation check, anti-virus, and sandboxing.
	Integration with existing third-party anti-virus, sandboxing, and Content Disarm and Reconstruction (CDR) solutions that protect against known and unknown threats contained in documents by removing executable content.
	Inspect risky content and detect malicious behavior of all original documents downloaded.
	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.
	Flexible data retention periods for up to one year.
	Ability to create custom queries with Menlo Query Language.
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.
Data Loss Prevention (DLP)	Restrict document upload to the Internet.
	Integration with third-party DLP (both on-premises and cloud-based DLP).
	Increased visibility for on-premises solutions.
Cloud Access Security Broker (CASB)	Deep visibility of SaaS application traffic to ensure compliance.
	Integration with third-party CASB solutions.
	Granular policy control for SaaS applications.

Feature	Benefits
Encrypted Traffic Management	Intercept and inspect TLS/SSL-encrypted web browsing traffic at scale.
	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
Connection Methods and Endpoint Support	Proxy Automatic Configuration (PAC)/Agent-based traffic redirection
	IPSEC/GRE network traffic redirection support
	Seamless integration with top SD-WAN providers
API Integrations	Seamless SaaS integration to secure web sessions
	CDR, SSO
	Highly extensible set of standards support, APIs, and third-party integrations
	Content APIs
	Policy APIs
	Log APIs
	Validated third-party integrations for SSO, SIEM, MDM, firewall, proxy, AV, sandbox, 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. Using a fundamentally different approach, Menlo Security eliminates threats from malware completely, fully protecting productivity with a one-of-a-kind, isolation-powered security platform that is cloud-native, elastic, and extensible. 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.

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.