Data Sheet

Secure Web Gateway (SWG)

Protect productivity and outsmart threats with the Menlo Secure Cloud Browser

Business systems and users are moving to the cloud, yet traditional cybersecurity solutions were not designed for the cloud and are failing to protect users from modern threats and Highly Evasive Adaptive Threats (HEAT) attacks. The existing approach to web security and malware prevention has created a sprawl of appliances and overburdened security teams, and it's ineffective and expensive to operate. The result is that web-based attacks are far too common and successful. It's clear that today's threat landscape and cloud transformation challenges require a fundamental rethinking of the network architecture—replacing it with an architecture that's designed for the cloud and supports Software-as-a-Service (SaaS) applications by default.

Three things to know:

Cloud transformation is changing the way users communicate, collaborate, and work productively on the web.

Traditional network and security architectures were not designed for the cloud or remote working, making it tough for them to protect users.

Your users are falling prey to phishing, social engineering, credential theft, zero days, and other Highly Evasive Adaptive Threats (HEAT) attacks—putting users and the organization at risk.

Product overview

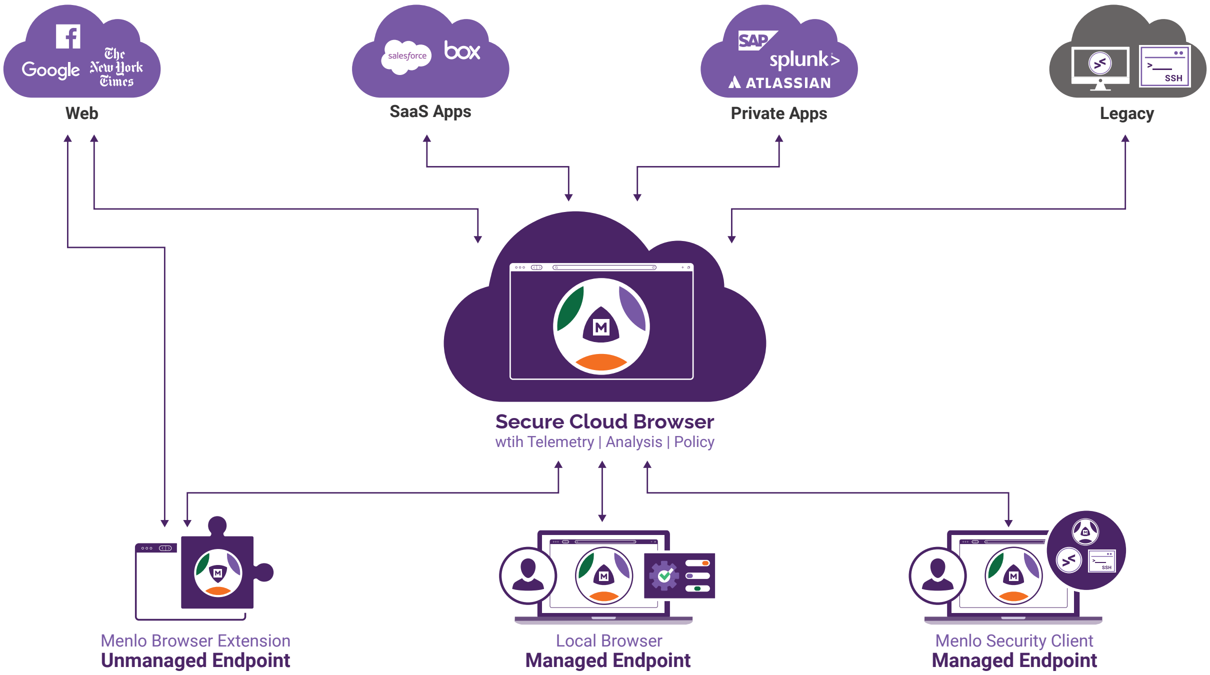
Using a fundamentally different approach, the Menlo Security Secure Web Gateway (SWG) powered by an Secure Cloud Browser delivers the capabilities enterprises need to achieve Secure Cloud Transformation. Menlo Security converges all SWG capabilities into a single cloud-native platform—including, Last-Mile Data Protection, RBI, Proxy, FWaaS, and Secure Application Access—to provide extensible APIs and a single interface for policy management, reporting, and threat analytics. Delivered from a global elastic cloud as a service, the Menlo Security SWG allows users to connect securely to the Internet from anywhere business takes them. Enterprises can be assured that they're protected from web-based cyberthreats and Highly Evasive Adaptive Threats (HEAT) attacks; granular access and security policies are enforced; web traffic is controlled, monitored, and protected; data leaks and credential theft are prevented; cloud apps are secure; unauthorized applications are shut down; and compliance is ensured across all devices and locations. The Menlo Security SWG does this with unmatched performance and scale—allowing organizations to outsmart known and existing threats as well as unknown and future threats.

The the Menlo Secure Cloud Browser assumes that all web content is risky and poses a danger to the organization.

This approach eliminates the need to make an allow-or-block determination based on coarse categorization, filters, and hard-to-maintain policies. The Menlo Security SWG allows organizations to employ an isolate-or-block policy instead. 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 with no need for special client software or plug-ins. This restores 100 percent confidence in the security posture for security teams, as well as worry-free and productive clicking, downloading, and browsing for end users.

Menlo protects millions of users on its Cloud Security Platform today. It includes flexible deployment options hosted on-premises or delivered as a cloud service. It integrates with existing network infrastructure and supports any device—desktop, laptop, and mobile devices.

The Menlo Secure Cloud Browser



Menlo Security Secure Web Gateway: Key features and benefits

Feature	Benefits
The Menlo Secure Cloud Browser	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 <input> 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.

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.
	Works with native browsers with broad browser support.
	Hybrid deployment support with no differences in a consistent 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, as well as upload and download controls.
Bandwidth Control	Enable user/group policy to predictably control bandwidth in low-latency, high-bandwidth environments (such as video content) to enhance the user experience.
Content and Malware Analysis	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.
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.
	Flexible data retention periods for up to one year.
	Ability to create custom queries with Menlo Query Language.

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
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.
Menlo Last-Mile Data Protection	Restrict document upload to the Internet.
	Integration with third-party DLP (both on-premises and cloud-based DLP).
	Increased visibility for on-premises solutions.

Feature	Benefits
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

Cloud transformation is well underway and 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 as they innovate quickly and respond to dynamic customer demands.

To learn more about protecting productivity, 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.