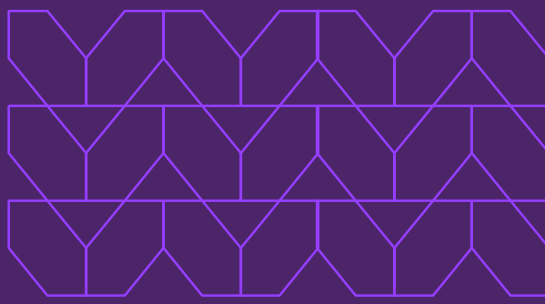
MENLO SECURITY

Data Sheet

Firewall as a Service (FWaaS)

Protect internet traffic for all users, applications and locations with the only cloud native security platform powered by an Isolation Core.

Today's hybrid workforce requires employees to be able to work anywhere, and from everywhere—whether that be in a corporate office, home, branch offices, or even shared work spaces. In addition, employees can work from any device using new cloud applications and Software as a Service (SaaS) platforms. But the acceleration of this new normal has forced organizations to focus on fast, reliable over security, leaving traditional firewall appliances ill-suited to protect users and their traffic. Inconsistent firewalls policies across your users and locations lead to increased risk which can ultimately compromise your networks—and choosing the wrong firewall can lead to poor user experience, degraded performance, and costly breaches.



Three things to know:

Expanded visibility and control
Security teams receive the real-time visibility and control needed to troubleshoot issues, perform post-event analysis, and most importantly, make adjustments that protect productivity.

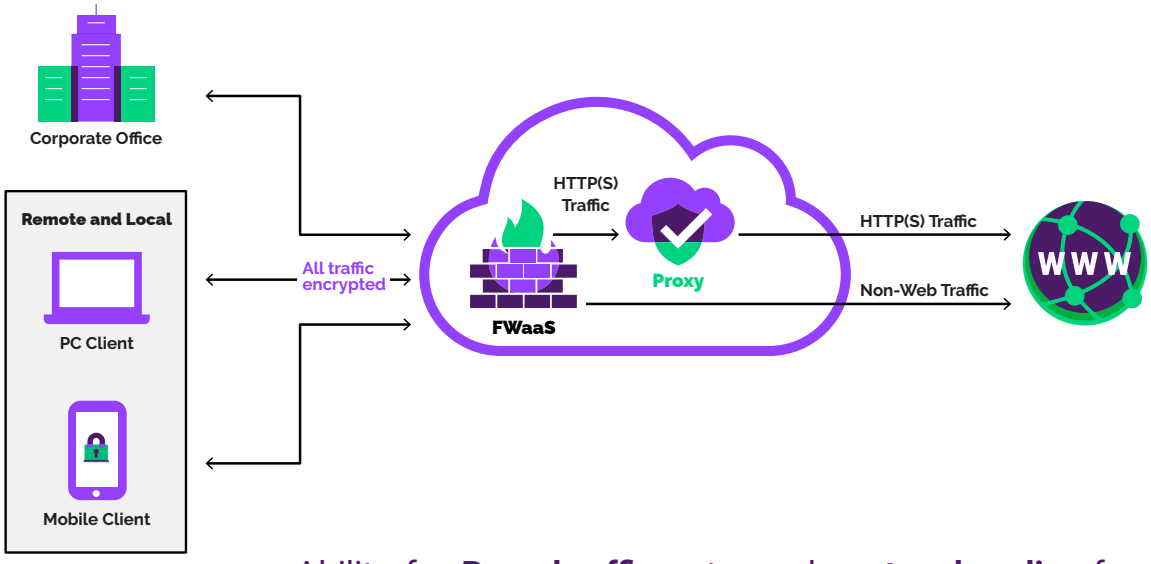
Protecting the anytime anywhere workforce
Advanced threat detection delivered through web isolation in the cloud that strips suspicious content and preserves the native browsing experience.

Flexible, scalable security
Our flexible, cloud-delivered local Internet breakouts allows users to connect directly to mission-critical cloud apps at scale, without the need to expensive security appliances or expanded bandwidth.

Product overview

Menlo Security's Firewall as a Service (FWaaS) enables fast and secure Internet for organizations, and because it's 100% in the cloud, there's no traditional hardware to buy, deploy, or manage. FWaaS takes a software-based approach to delivering security services to distributed and mobile users throughout the cloud—eliminating the need to backhaul cloud app and SaaS traffic to a central data center. This allows organizations to provide secure local internet breakouts to remote users at cloud scale.

Menlo Security Client with FWaaS



- Ability for **Branch offices** to apply **network policy** for all traffic without requiring on-prem firewall
- **Secure all web traffic** by sending to Menlo Isolation
- **Monitor and Secure** all traffic for roaming users

These flexible, mobile cloud-delivered local Internet breakouts allow users to connect directly to powerful cloud apps—such as Microsoft 365—with all the same security visibility and controls that protect the data center. With Menlo Security Isolation Core™, cloud apps and SaaS content are fetched and executed in the Menlo Security Global Cloud instead of on users' browsers. Menlo Security efficiently delivers only safe and authorized content to end-user browsers, with no impact on application experience.

FWaaS along with the Menlo Security Client gives security teams visibility into traffic and the ability to apply the appropriate security controls to all traffic regardless of physical location or the underlying connection. And we do this without relying on vulnerable VPN services or physical security appliances that impact performance and add IT overhead. Remote users have the same application experience they expected from the office.

Cloud-based simplicity and scale

Delivering firewall controls and unmatched security to all employees and roaming users no matter their location, and all ports and protocols.

No physical appliance in sight

Traditional physical firewall appliances aren't suited for the modern workplace. We were born in the cloud and built to secure it.

Accelerating productivity

Traditional firewalls result in increased latency and network bottlenecks. We've erased those issues, focusing on preserving the employee experience, making security invisible to the end user.

Menlo Security Firewall as a Service (FWaas): 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	Agent-based traffic redirection
	IPSEC 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.