Data Sheet

FedRAMP® Authorized Cloud Security Platform powered by an Isolation Core™

Empower your agency with the FedRAMP Authorized Internet security platform you need to eliminate threats and protect sensitive data.

What's stopping malware?

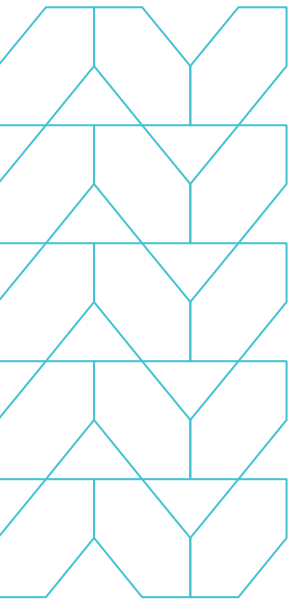
The work-from-anywhere policies necessitated by the global pandemic have created more flexibility for the world's workers, but an unwanted result was an increase in security vulnerabilities. With the broader range of ways that your agency's workers, remote personnel, and field staff are connecting to your networks every day, the concept of a secure perimeter is officially obsolete. Until now.

Three things to know:

While recent work-from-anywhere policies have created more flexibility for the world's workers, they have also led to increased security vulnerabilities, as the browser is still the most common attack vector.

Menlo Security adopts a Zero Trust approach to this security challenge through its FedRAMP Authorized Isolation Core™ technology, which prevents attacks from reaching users in the first place by moving the browsing process off the desktop and into the cloud,

Menlo Security consolidates all Secure Web Gateway (SWG) capabilities—including CASB, DLP, RBI, proxy, sandbox, FWaaS, and private access—into an end-to-end single cloud-native platform. The platform also integrates with SD-WAN to provide an integrated Secure Access Service Edge (SASE) solution. It is also extensible via an API framework and features a single interface for policy management, reporting, and threat analytics across all the consolidated services.



[1]Source Google

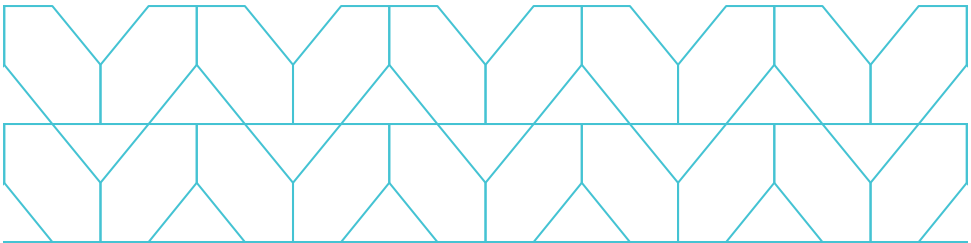
Amidst this rise in cyberattack surface area and opportunity, the browser continues to be both the most important productivity tool and the most common attack vector. In fact, users spend 75 percent of their workday in a web browser or virtual meetings.[1]

Cyberattacks often begin with users falling for bogus emails and infected attachments, websites, and downloadable documents. Yet the security industry insists on the same old approach—detect and remediate—which attackers have learned how to bypass. According to the 2022 report there were 914,547 incidents analyzed with 234,638 confirmed breaches. Worse: The average cost of a data breach rose to $4.24 million. Additionally, organizations that had more than 50 percent of their workforce working remotely took 58 days longer to identify and contain breaches than those with 50 percent or less working remotely.

This means that the two primary defense methods—blocking an attack and then detecting a breach once it has occurred—are failing miserably.

Unfortunately, many solutions today use these methods. While they are designed to identify threats and prevent them from reaching the network, no product on the market can evaluate with 100 percent accuracy whether something from the Internet—including a file, an image, or a document—is safe.

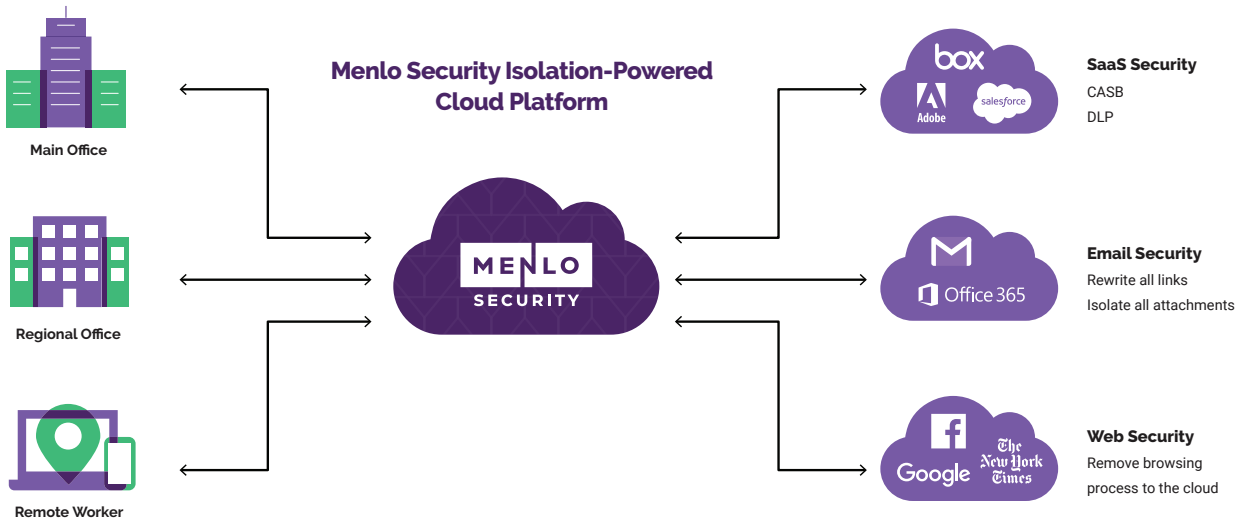
So, although many government organizations have made significant investments of time and money in cybersecurity, attacks are still getting through, breaches are happening, and agencies are impacted. New architectures that support work from anywhere and Software-as-a-Service (SaaS) demand a new approach to security.



Zero Trust and isolation: Rethinking email and web security.

Zero Trust has emerged as the best way to approach the unthinkable: 100 percent safe email and web access. At Menlo Security, we approach Zero Trust through our FedRAMP Authorized Isolation Core™ technology. By taking the browsing process off the desktop and moving it to the cloud, we effectively prevent any active and potentially malicious content from reaching the networks. Any breaches or attacks are completely isolated away from the endpoint user, who sees no interruption or difference in the browsing experience. This same Isolation Core™ architecture also provides protection for email links and attachments, as well as DLP and CASB services.

Applying this isolation capability across multiple regions, agencies, and employees, each using multiple browsers and devices, requires a platform that can scale on demand up to millions of users without compromising the user experience. Your government organization needs a preventive, flexible, and extensible security solution that can connect to their existing networks, from anywhere, while supporting their agile digital transformation objectives.



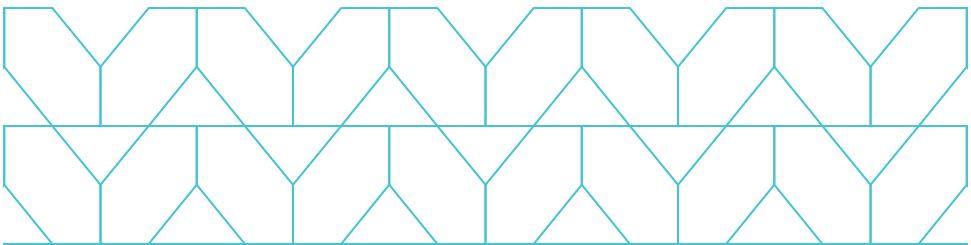
Scaling isolation with an all-in-one cloud security platform.

The Menlo Security Cloud Platform is an all-in-one, cloud-native security solution that eliminates malware threats completely, connects to your networks from anywhere, and scales elastically based on real-time traffic patterns and demands. With this one-of-a-kind platform, government organizations can:

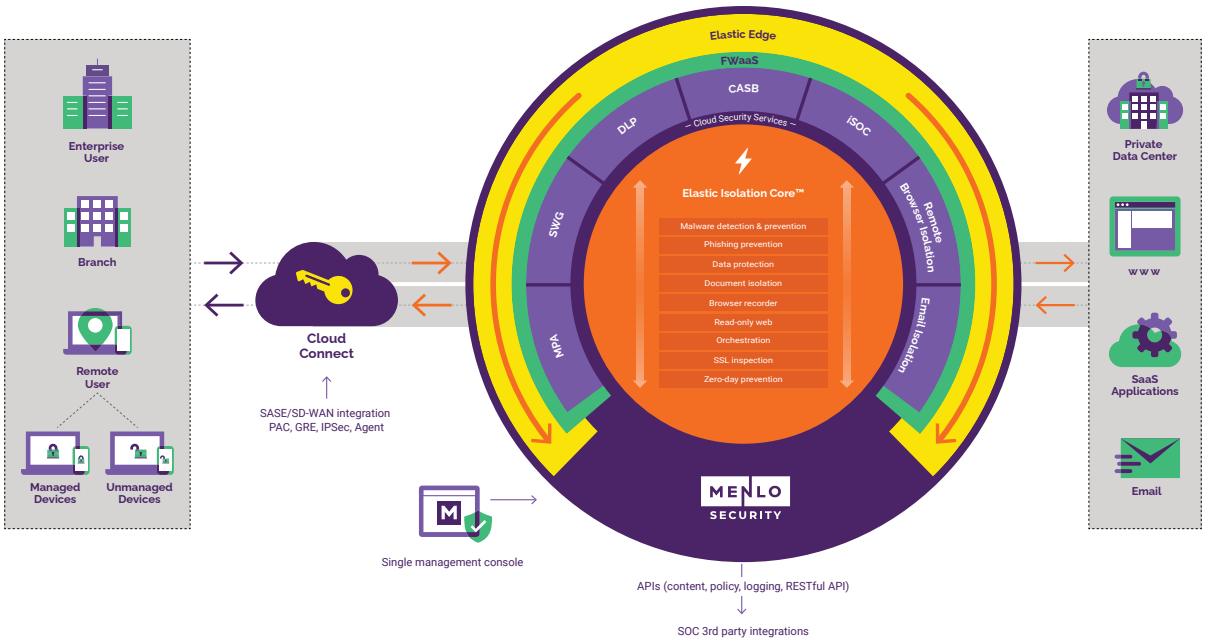
1. **Eliminate Malware Threats Completely at Scale**—Menlo's Elastic Isolation Core technology scales on demand vertically, by fully protecting employees' browsing no matter the use case or device. And Menlo's Elastic Edge technology scales isolation horizontally to millions of users, across offices, regions, and networks. These capabilities provide a seamless user experience without compromising functionality.

2. **Streamline Operations and Increase Efficiency with Cloud-Native Software**—The Menlo Security Cloud Platform was born in the cloud and dynamically scales with enterprise-level growth and demands. Users experience high uptime and responsiveness with low latency.

3. **Increase the Value of Current Tools with Third-Party Integrations and APIs**—The Menlo Security Cloud Platform is agnostic to connection type, making it open and accessible no matter the network configuration. It's also extensible to third-party integrations and APIs, allowing organizations to repurpose previous investments and provide the security foundation for their future Secure Access Service Edge (SASE) architecture.



The Menlo Security Cloud Platform is an all-in-one, cloud-native security solution that eliminates malware threats completely, connects the enterprise from anywhere, and scales elastically based on real-time traffic patterns and demands.



Menlo Security's isolation-powered platform

Feature	Benefits
Cloud Connect	Flexible ingress routing and traffic steering that directs browser traffic seamlessly to Menlo's cloud and renders content back to the user in seconds
	Authentication that identifies users/customers so the appropriate policy can be enforced
	IPSec, GRE, PAC, Prepend, Proxy Chaining, Transparent Proxy, Firewall Integration
	Endpoint agent (Menlo Connect)
	MDM integration for mobile devices
	SD-WAN integration
	SAML, IP-based, X-headers
Elastic Edge	On-demand scaling to support new user populations—no need for capacity planning or for hardware investments to scale VPN capacity
	Five 9s availability with a cloud-native, highly redundant architecture
	Global presence
	Auto-scale, no need to provision for peak capacity
	35 million isolated sessions daily; 4 billion transactions monthly
	<100ms latency connections with Tier 1 peering
	SSL termination for ALL sessions by default with no performance degradation
	Multi-tenant layer-7 firewall to manage/steer non-HTTP outbound connections
	Bring Your Own Certificate for customer-specific certificates
	Cloud HSM that meets the most stringent corporate, contractual requirements
	Compliance: SOC II, FedRAMP, and ISO 27001 with third-party audits
Elastic Isolation Core	Extends elasticity to the edge, optimizing for individual user traffic patterns and demands, with no compromise in functionality or experience
FedRAMP Authorized	Menlo Security is FedRAMP Authorized for our Cloud Security Platform powered by Isolation Core.™ FedRAMP Authorized solutions meet the highest level of security standards, are rigorously tested and must be are continuously tested to maintain the FedRAMP status in order to continue to do business with government agencies.

Feature	Benefits
Session Replay	Empowers security teams to quickly investigate incidents with high-fidelity replays of user browsing sessions
	Provides unmatched visibility into browser sessions compared with network based proxies, firewalls, etc.
	Shows how users have been targeted and what data has been potentially compromised
	Can be used by security teams to automate research and data collection
	Secures storage/encryption/chain of custody to maintain integrity of forensic data
Document Isolation	Protects against weaponized documents and other file-based attacks
	Safely renders common document/file formats into a completely safe isolated viewer
	Rewrites and isolates embedded links within documents
	Provides full visibility into password-protected files
	Provides safe PDF versions of original attachments for offline viewing
	File REST API integrates with third-party malware analysis engines and Content Disarm and Reconstruction (CDR) tools
Read-Only Web	Permits safe access to social media sites
	Permits users to log in while disabling form-based input and other functionality
	Read-only browsing sessions remain fully isolated from any harmful active content, while preserving the native end-user experience
	Inline CASB expands this capability to other widely used cloud applications
	User can control access to sites based on app function, including login, share, search, upload, create, and more

Cloud Security Services	
Feature	**Benefits**
Malware Detection and Prevention	Complete protection against: • Zero-day browser vulnerabilities • Drive-by downloaders • Browser exploits • Malicious web downloads • Links leading to malicious documents • Multi-stage attacks
Phishing Prevention	Zero-hour credential phishing protection, including for unclassified sites or those categorized as benign
	Prevents users from inputting credentials into suspicious sites by rendering links in read-only format
	Proprietary link risk-scoring algorithm
	Customizable banners that provide “teachable moments”
	Extends credential phishing protection to mobile users
	Prevents account takeovers that lead to lateral attacks
	Stops attackers from using email accounts to hijack other services
	Stops attackers from accessing email, calendar events, contacts, and sensitive data in file shares
Data Protection	Detects and prevents exfiltration of sensitive data via file uploads and data input
	Hundreds of predefined/built-in data classifiers accurately identify PII, PHI, and other sensitive content
	Prevents attempts to upload sensitive data to sanctioned and/or unsanctioned cloud apps
	Stops data exfiltration from users copying content to personal email accounts and online file storage
	Defines policies to detect and control sharing of Microsoft Information Protection (MIP)–labeled documents
	Meets regulatory compliance mandates such as HIPAA, GDPR, GLBA, and PCI-DSS

Feature	Benefits
Orchestration	Augments your security operations with automation and tools to quickly and effectively triage, investigate, and respond to email attacks
SSL Termination	Offers low-latency, high-performance, transparent user experience while providing security at scale
	Inspects encrypted web traffic for advanced threats, data loss, and malware
	Cloud-native architecture provides autoscaling SSL/TLS inspection, leveraging the near-infinite compute capacity of cloud resources
Zero-Day Protection	Remote browser isolation provides complete protection against zero-day browser vulnerabilities
	Full visibility (forensics) into zero-day attacks via insights, Isolation Security Operations Center (iSOC) feed, and browser recorder/session replay
	Assumes all content is risky and isolates everything without impacting user experience
	Executes active content such as JavaScript or Flash in cloud-based disposable virtual containers
	Browser isolation renders non-executable, malware-free content indistinguishable from the user's native experience
API and Verified Integrations	Content APIs
	Policy APIs
	Logging APIs
	RESTful API
Third-Party Integration Categories	SSO
	SIEM
	MDM
	Firewall
	Proxy
	AV
	Sandbox
	CDR
	SOAR
	SD-WAN/SASE
	Custom

Protecting against modern security threats is a top priority for government agencies, and 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.