MENLO SECURITY

Data Sheet

Last-Mile Data Protection

Stop deliberate or accidental leakage of critical business information.

Whether by malicious intent or by accident through the use of artificial intelligence (AI) based tools like ChatGPT, users may expose personally identifiable information (PII) such as Social Security numbers, credit card numbers, and other sensitive data that should not be publicly available, potentially making businesses liable for damages resulting from the error of a single person.

The introduction of generative AI tools such as ChatGPT have been widely adopted to increase efficiency and productivity. These revolutionary platforms are designed to offer highly-personalized conversations and unique messaging that can imitate natural language responses tailored to the user's data input.

In turn, however, this poses a significant risk to organizations and must be addressed in order to protect users and their sensitive data. But for modern businesses, it provides a competitive edge, so prohibiting these tools could mean missed opportunities as well.

Three things to know:

The risk of unauthorized data exfiltration grows exponentially as users continue to spread out from corporate headquarters.

Legacy security tools are unable to provide enterprise security teams with visibility into and control over corporate data beyond the perimeter, which inhibits compliance efforts and increases risk.

Menlo Security Last-Mile Data Protection uses an isolation-based approach to identify and prevent sensitive data from leaving the company.

Product overview

Menlo Last-Mile Data Protection identifies and prevents sensitive data from leaving your company. It provides 100 percent reliable inspection of all file uploads and user input for both isolated and non-isolated browsing sessions by creating an air gap between the user and the Internet through which all traffic flows. This isolation technology-powered approach controls the channel between the user and the isolated browser, enabling the system to inspect everything. Menlo Last-Mile Data Protection helps organizations monitor every device in their ecosystem with completely reliable data inspection.

ChatGPT Privacy

As organizations leverage new generative AI tools such as ChatGPT to increase efficiency, security leaders must make sure users aren't accidentally uploading sensitive information or customer data into the wrong hands while trying to increase productivity. Whether it's to protect intellectual property, personally identifiable information PII or other private data, companies should make sure they have policies and safeguards in place to protect users and prohibit sensitive information from being uploaded.

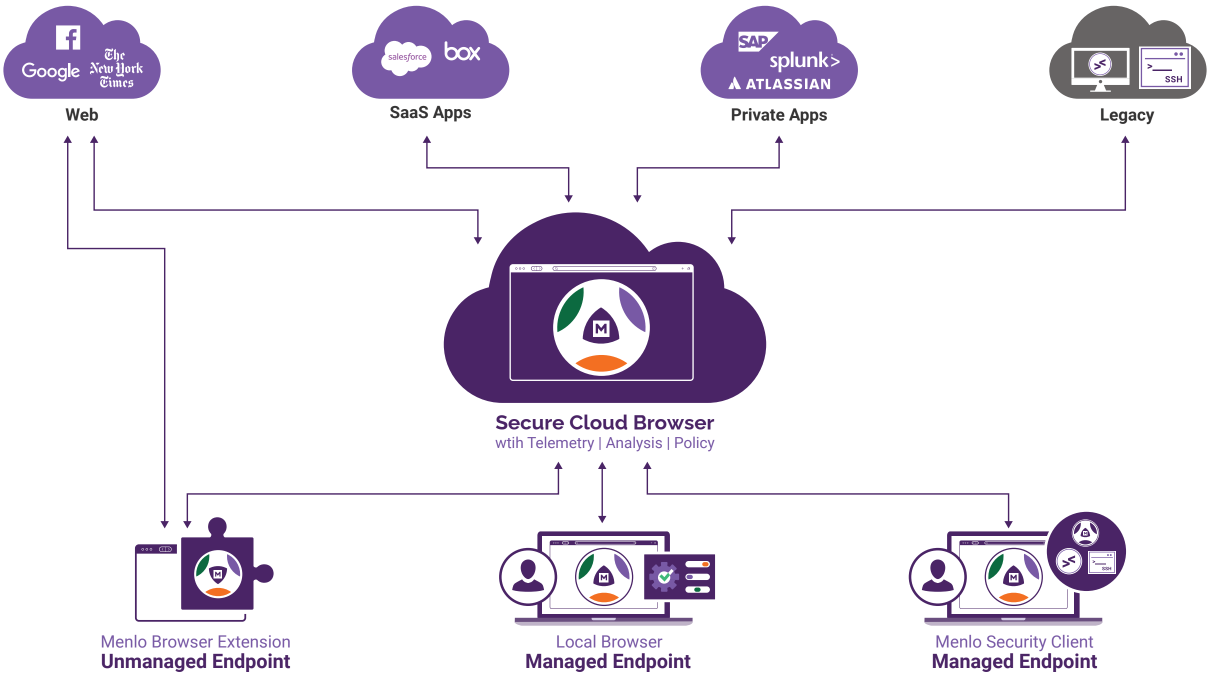
Menlo Last-Mile DLP functionality provides security teams with the ability to control data input into AI platforms and safeguard sensitive content from being uploaded. This gives security organizations peace of mind knowing that any potential risk of data leakage is mitigated within an isolated layer as we begin to see organizations adopt AI tools over time.

Menlo last-mile data protection works by first identifying specific data types deemed sensitive by file type, regular expressions, or set data-type libraries.

The data can either be contained in a file (such as an Excel spreadsheet) or a browser web form with user input. Because the Menlo Cloud Security Platform has visibility and control over traffic, it can reliably observe all data egress. This means that Menlo Last-Mile Data Protection can observe and prevent potential data leaks that arise from browser submission forms and non-browser traffic.

User traffic flows through the Menlo Secure Cloud Browser, which inspects encrypted web traffic and cloud services for potential data loss. It's here where DLP policies are enforced globally and consistently for every user and device.

The Menlo Secure Cloud Browser



Menlo Security's Data Loss Prevention: Key features and benefits

Feature	Benefits
The Menlo Secure Cloud Browser	Ensures 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 without impacting the native browsing experience.
Document Isolation	Ensures safe viewing of documents by executing all active or risky active content in the cloud, away from the endpoint.
	Offers the option to download safe cleaned or original versions of documents.
	Integrates with third-party CDR solutions to scan files.
	Provides granular policies to limit document access based on file type and user.
Global Cloud Proxy	Enables admins to centrally configure web security and access policies that are instantly applied to any user on any device.
	Provides hybrid deployment support with no differences in a policy.
URL Filtering and Acceptable Use Policies (AUPs)	Limits user interaction for specific categories of websites (75+ categories).
	Controls employee web browsing via granular policies (user, group, IP).
	Provides document access controls, including view only, safe, or original downloads based on file type.
Bandwidth Control	Enables user/group policy to predictably control bandwidth (such as video content) to enhance the user experience.
Content and Malware Analysis	Provides integrated file analysis using file hash check, anti-virus, and sandboxing.
	Integrates with existing third-party anti-virus and sandboxing solutions—such as Palo Alto Networks Wildfire and Cisco Secure Malware Analytics.
	Inspects risky content and detects malicious behavior for all original documents downloaded.

Feature	Benefits
Analytics and Reporting	Provides built-in and custom reports and alerts with detailed event logs and built-in traffic analysis.
	Offers built-in and custom queries for flexible exploration and analysis of data.
	Exports log data using API to third-party SIEM and BI tools.
Encrypted Traffic Management	Intercepts and inspects TLS/SSL-encrypted web browsing traffic.
	Offers provisionable SSL inspection exemptions to ensure privacy for certain categories of websites.
	Exposes hidden threats in encrypted sessions.
Global Elastic Cloud	Provides secure and optimal web access for remote sites and mobile users anywhere in the world.
	Features autoscaling and least-latency-based routing that allows connectivity from any location, scaling to billions of sessions per month.
	Enables 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.
	There’s no need to install or use a new browser.
	Provides smooth scrolling with no pixelation.
User/Group Policy and Authentication	Enables admins to set and fine-tune policies for specific users, user groups, or content type (all content, risky content, uncategorized).
	Allows admins to 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	Applies additional security controls on top of isolation services.
	Last-Mile Data Protection, FWaaS, Global Cloud Proxy

Feature	Benefits
Menlo Last-Mile Data Protection	Restricts document upload and form-based posts to the Internet.
	Integrates with third-party DLP (both on-premises and cloud-based DLP).
	Offers increased visibility for on-premises solutions.
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, SOAR
	SD-WAN and SASE integrations

Isolation is critical for full data inspection. Often, web pages may obscure the upload process, which prevents traditional DLP solutions from decoding the submissions. The advantage of isolation is that it provides complete visibility into the browser session—especially when compared to legacy proxies and network inspection devices. Menlo Security Last-Mile Data Protection is globally inclusive by maintaining a library of more than 300 data categories from all over the world—recognizing that sensitive data or regulatory requirements that might have relevance in one region, such as the U.S., might have little relevance in another, like Singapore or Brazil.

Data loss prevention is becoming more critical as users continue to work outside of corporate headquarters and as organizations progress through cloud transformation. Legacy DLP solutions are unable to provide enterprise security teams with visibility into and control over corporate data beyond the perimeter.

Menlo Last-Mile Data Protection identifies and prevents sensitive data from leaving your company, reducing the risk of costly and embarrassing data loss incidents. With the Secure Cloud Browser approach, it uniquely controls how information enters and exits the network, which enables Menlo to provide 100 percent reliable data inspection and user input.

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.

© 2023 Menlo Security, All Rights Reserved.