

AI Adaptive DLP

Enhance Productivity While Preventing Data Exfiltration and Loss

Intelligent Data Security

Enhanced User and IT Productivity

Data Security for Modern Apps and Workforces

Can Your DLP Keep Up with Your Business?

Tools like data loss prevention (DLP) and Data Security Posture Management (DSPM) are falling behind the needs of the modern, hybrid workforce.

- Traditional endpoint DLP isn't sufficient for modern workflows, workforces and applications, burdening IT security with time-consuming rollouts, implementation failures, and retreats to monitor mode without enforcement. With most daily work is in browsers using SaaS, endpoint DLP struggles to detect and secure sensitive data in web content, increasing risk with the use of kernel presence and driver interference.
- Traditional DLP operates at the level of an entire file, blocking files altogether upon detection of sensitive data. This forces users to manually modify files to share them, wasting countless hours and creating a guessing game as the user attempts to delete the right content to satisfy DLP restrictions.
- With heavyweight endpoint agents, it can be impossible to install DLP on contractor and employee BYOD devices.
- While DSPM is intended as a modern assist to DLP, it is limited to data at rest and serves mainly to identify gaps in Data Access Governance, delivering alerts to the IT security team.

Clearly modern organizations need data security that protects data at the speed of business.

KEY BENEFITS

Enhanced User Productivity

Keep modern workflows humming for all users by delivering secure files.

Fast Path to Compliance

Users stop working around blockages. IT stops disabling DLP enforcement. GRC, CISO and CIO have confidence in compliance with data protection regulations.

Enhanced IT Productivity

Cloud-based with fast rollouts, fewer help desk calls, and no software installation or updates.

Protect Data and Enhance Productivity with Menlo AI Adaptive DLP

Menlo AI Adaptive DLP enhances both user and IT productivity, giving the modern hybrid workforce secure use of modern applications, workflows and storage. Menlo AI Adaptive DLP core attributes include:

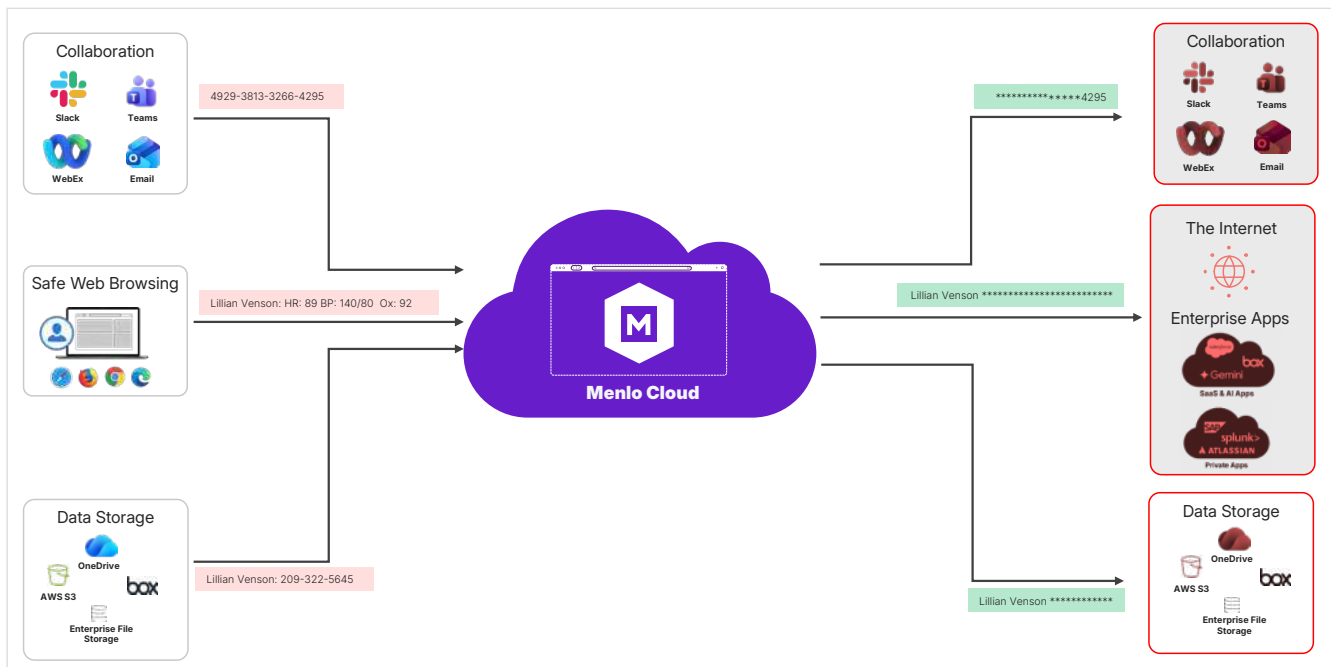
- **Cloud-based**, AI Adaptive DLP involves no software installation, making it ideal for BYOD and third-party users like contractors
- **Fast, simple policy creation** and deployment for efficient, smooth rollouts
- **AI-driven sensitive data detection** is available for the common and country- and region-specific personally identifiable information (PII), personal health information (PHI) and fields related to financial data such as those subject to the payment card industry data security standards (PCI-DSS)
- **Automated data masking** protects sensitive data inside of files in real time and then delivering them, allowing users to complete workflows while making sensitive data invisible, eliminating the productivity hindrances posed by traditional DLP
- **Broad Enterprise Coverage** with a single set of policies for data everywhere:
 - In the browser for files uploaded to the internet or downloaded from internal web applications
 - Email and collaboration applications
 - User-aware storage such as OneDrive, SharePoint and Box.com
 - Mass storage such as Amazon Web Services S3
- **Real-Time Operation** masks data in files with application-specific integrations, dramatically reducing the need for extensive static access governance

Menlo AI Adaptive DLP can replace many use cases currently covered by expensive, difficult, risky DLP, dramatically reducing false positive blocks, reducing costly renewals, and enhancing productivity for both users and the entire IT security team.

Key Capabilities

Cloud-Based Flexibility and Scale

Unlike heavyweight endpoint DLP agents, Menlo AI Adaptive DLP delivers cloud-based security as a service. With no heavyweight endpoint agents to install and maintain, organizations can support employee BYOD, third-party devices such as contractors and even merger and acquisition target user communities. Files are delivered to the elastic, global Menlo Cloud, guaranteeing low latency and fast performance even for large files. Detection and masking occur in the cloud, with a scalable architecture and dedicated resources per tenant.



Fast Policy Creation Assignable to Multiple Workflows

Unlike multi-month deployments with traditional DLP, Menlo AI Adaptive DLP enables data security administrators to, in a single operation, define what to detect and what to mask. Then, the policy can be applied to data across multiple modern workflow and data stores, including in the browser (uploads/downloads), e-mail and advanced collaboration tools, web portals, cloud storage and other data stores. Multiple policies can be applied to different types of data and to specific users or groups.



AI-Driven Sensitive Data Detection

Menlo AI Adaptive DLP offers advanced, automated, AI-based detection of the most common sensitive data types including

- Personally-identifiable information (PII)
- Personal health information (PHI)
- Fields related to financial data such as those subject to the payment card industry (PCI) data protection standards

Data to detect

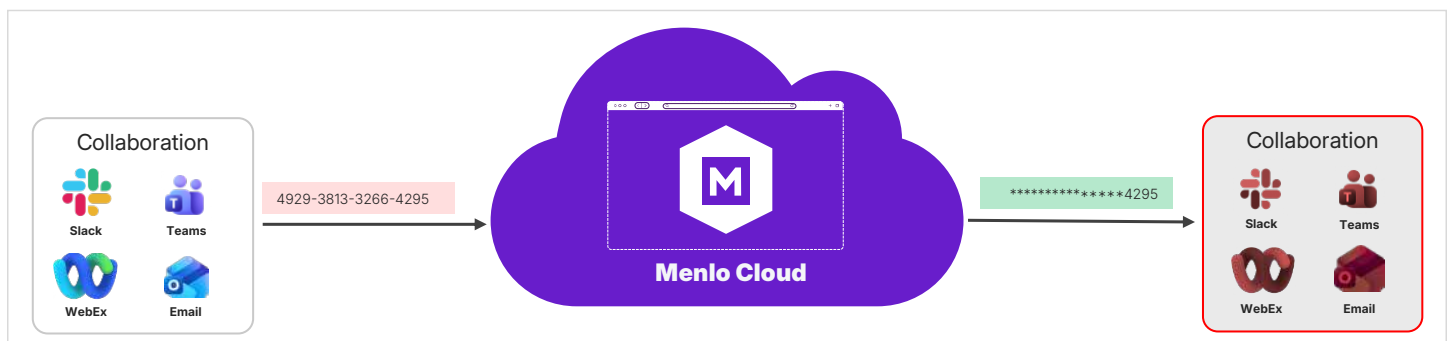
Image OCR Solution (might affect performance)

Filter privacy labels

PII	PCI	PHI
<input type="checkbox"/> ACCOUNT NUMBER	<input type="checkbox"/> BANK ACCOUNT	<input type="checkbox"/> BLOOD TYPE
<input type="checkbox"/> AGE	<input checked="" type="checkbox"/> CREDIT CARD	<input type="checkbox"/> CONDITION
<input type="checkbox"/> DATE	<input checked="" type="checkbox"/> CREDIT CARD EXPIRATION	<input type="checkbox"/> DOSE
<input type="checkbox"/> DATE INTERVAL	<input checked="" type="checkbox"/> CVV	<input type="checkbox"/> DRUG
<input type="checkbox"/> DOB	<input type="checkbox"/> ROUTING NUMBER	<input type="checkbox"/> INJURY
<input type="checkbox"/> DRIVER LICENSE		<input type="checkbox"/> MEDICAL PROCESS
<input type="checkbox"/> DURATION		<input type="checkbox"/> STATISTICS
<input type="checkbox"/> EMAIL ADDRESS		

Automated Data Masking in Real-Time

Menlo AI Adaptive DLP works inside of files to detect and mask sensitive data in real time and **delivers files to their destinations**. Traditional DLP operates at the level of an entire file. With traditional DLP, if a user gets a block, they might enter a repetitive cycle of trying to remove sensitive data, getting blocked again, and trying again. The cycle could continue, and countless hours are lost. Unlike traditional DLP, Menlo AI Adaptive DLP enables work to get done fast.



Extensible Detection

Menlo AI Adaptive DLP includes extensible detection with new detection rules based on regular expressions (RegEx). Rule creation includes a testing mechanism.

Rule Name:	<input type="text" value="Global Corp Worker ID"/>
Regular Expression:	<input type="text" value="/^[A-Z]-\d{7}-.{1,4}\$"/>
Rule Action:	<input checked="" type="checkbox"/> Mask
Test Pattern:	<input type="text" value="T-4573496-ISRA"/>
Match	<input checked="" type="checkbox"/>

Broad Enterprise Coverage

Menlo AI Adaptive DLP is a modern data security solution aligned to the modern enterprise. It covers collaboration applications, storage locations, and, perhaps most importantly, the web browser, where most users spend most of their days, accessing enterprise SaaS, internal, and GenAI portals.

Zero-Compromise Data Security

Your organization is moving fast every day. Worker productivity demands that workflows keep moving. Executive sign-off on compliance requires confidence that your chosen data security solutions remain enforced. Departments and business units collaborate with vendors, contractors, and even customers and prospects, demanding that documents be available at speed. Menlo AI Adaptive DLP will help your users stay productive and ensure that IT security is the partner for the business, users and other stakeholder communities.

About Menlo Security

[Menlo Security](#) is the pioneer of unified browser security, protecting the modern enterprise's dual workforce: humans and AI agents. Our Browser Security Platform is the only solution that provides a unified trust layer for the modern enterprise, delivering architectural immunity to all actors, both agents and humans.

By focusing security on where the work happens- the browser session- Menlo provides industry-best zero-day threat prevention that eliminates threats before they reach the user device or agent, advanced file and data security that keep users safe and productive, and secure access to applications. These key capabilities are tailored for the security and access needs of users and agents, within a unified control, visibility, and policy framework.

Menlo doesn't just bundle security features; we collapse the distance between security, productivity, and innovation.

This is Menlo. Let's get started. © 2026 Menlo Security, All Rights Reserved.



Learn more: <https://www.menlosecurity.com>
Contact us: ask@menlosecurity.com

