MENLO SECURITY

Menlo Security Data Loss Prevention

Protecting data to the last mile

The web browser is at the center of the enterprise workspace. Workers start their day in the web browser via single sign-on applications, entering a portal where every tile is a web application. The rest of the day is spent in the browser as users access apps and data, collaborate, share files, and much more.

Looking closely at enterprise users' web activities, we find a mix of productivity and SaaS apps available on the public internet and internal web-based applications, many of which have enjoyed long tenure in the enterprise. One attribute shared by many web applications across internal, SaaS, and productivity is the ability to upload and download files and archives.

Unfortunately, the movement of files between users and the internal and internet-based applications they use is typically hidden from mainstream data loss prevention (DLP) tools and technologies.

Browser Context

Browser context refers to the environment and conditions in which a web browser operates, and the operations specific to a session. It includes factors that can impact both the security and behavior of the browser, such as:

- User identity
- Device posture
- Network location
- Website and application content
- Browser settings and configurations
- Web page document object model (DOM)

SOLUTION BRIEF

The Limitations of Traditional DLP

Traditional DLP solutions rely on network-level monitoring and inspection, limiting them from inspecting traffic commonly seen in the enterprise:

- **Encrypted traffic:** Given the now-ubiquitous encryption of web traffic, network-level DLP has no visibility into this traffic, which makes it almost impossible to detect sensitive data being transmitted. For example, some cloud access security brokers (CASBs) attempt to identify data that needs to be protected against loss by inspecting unencrypted data headers, which is clearly insufficient.
- **Password-protected files:** For files with a user-applied password and corresponding encryption, inspection may not be possible. Such files are often blocked, impacting productivity, when they could be deemed safe and accessible with a browser-friendly mechanism to prompt for a password.
- **Web-based applications:** Some web applications use varying techniques to obscure data uploads, preventing traditional DLP from accurately identifying and blocking sensitive information from upload.
- **Unmanaged devices:** The rise of BYOD and remote work means that many devices accessing corporate data are not managed by the organization, making it difficult to enforce DLP policies.

These limitations are creating data loss risks to modern enterprises:

- Files downloaded from internal web applications may contain enterprise intellectual property (IP), personally identifiable information (PII), protected health information (PHI), or other data deemed sensitive or proprietary to the organization.
- Files uploaded to the internet may contain proprietary or protected information.

There is a crucial need to prevent data loss that leverages browser context.

Menlo Security Data Loss Prevention

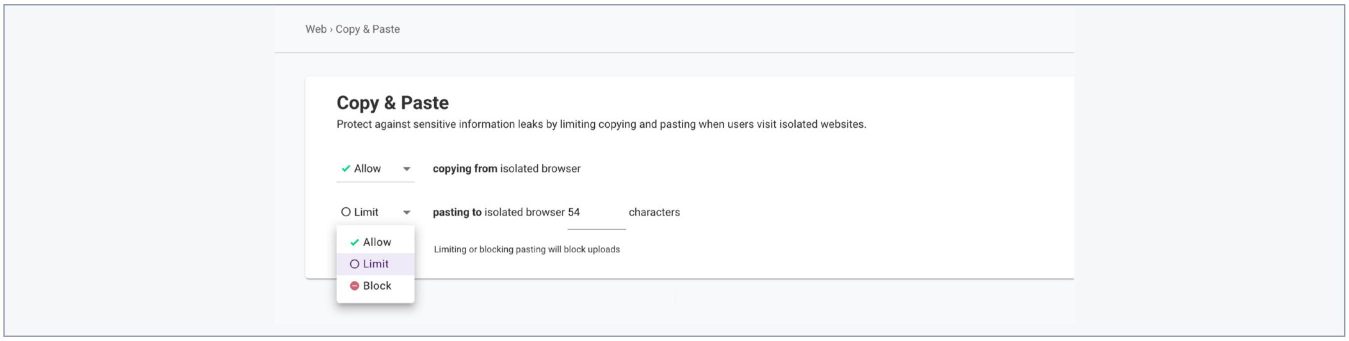
Menlo Security offers a DLP approach that leverages the Menlo Secure Enterprise Browser architecture to help close the security gap that prevents most DLP products from preventing data loss through web browsing. Menlo Security DLP is included in both the Menlo Protect and Menlo Secure product offerings.

Browser-Centric DLP Features

While traditional DLP is usually file- and archive-centric, the Menlo Secure Enterprise Browser solution includes a range of controls on browser use that enable data loss prevention via non-file activities. They include:

Copy and Paste Restrictions

With specific permissions based on users or groups, web applications can be blocked from pasting or the number of characters pasted can be limited.



Web › Copy & Paste

Copy & Paste

Protect against sensitive information leaks by limiting copying and pasting when users visit isolated websites.

✓ Allow **copying from** isolated browser

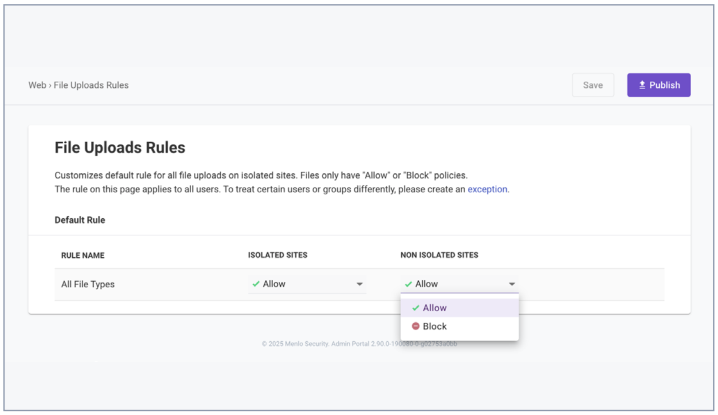
○ Limit **pasting to** isolated browser 54 characters

Limiting or blocking pasting will block uploads

Copy and Paste Controls

File Upload and Download Controls

Any internal or web application may be prevented from uploading or downloading files, or both. A use case for disabling file **uploads** is to prevent the inappropriate use of generative AI, and is typically utilized with Menlo Protect.



Web › File Uploads Rules

File Uploads Rules

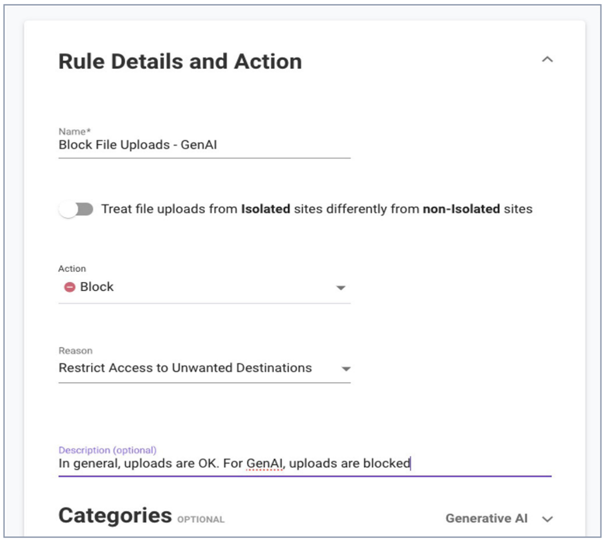
Customizes default rule for all file uploads on isolated sites. Files only have "Allow" or "Block" policies.
The rule on this page applies to all users. To treat certain users or groups differently, please create an exception.

Default Rule

RULE NAME	ISOLATED SITES	NON ISOLATED SITES
All File Types	✓ Allow	✓ Allow

© 2025 Menlo Security. Admin Portal 2.90.0-190080-0-g02753a0bb

Basic Policy: Allow File Uploads



Rule Details and Action

Name*
Block File Uploads - GenAI

Treat file uploads from **Isolated** sites differently from **non-Isolated** sites

Action
● Block

Reason
Restrict Access to Unwanted Destinations

Description (optional)
In general, uploads are OK. For GenAI, uploads are blocked

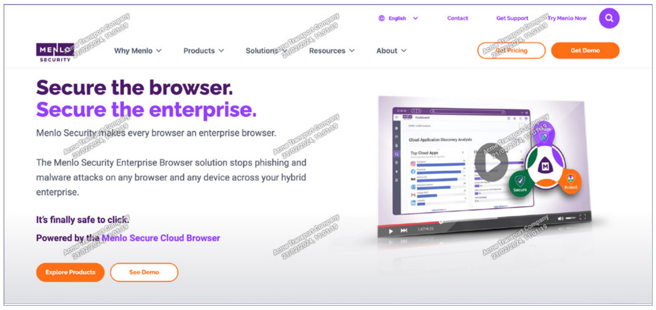
Categories OPTIONAL Generative AI

Exception: Block File Uploads for GenAI Category

A use case for disabling file **downloads** is to prevent untrusted users from downloading files from internal web applications. This is an important security capability of Menlo Secure Application Access.

Watermarks

Company-defined watermarks can be displayed on any web application or applied to downloaded files. Watermarking offers rapid forensic evidence, providing a strong signal to a user that inappropriate use can be discovered.



Secure the browser.
Secure the enterprise.

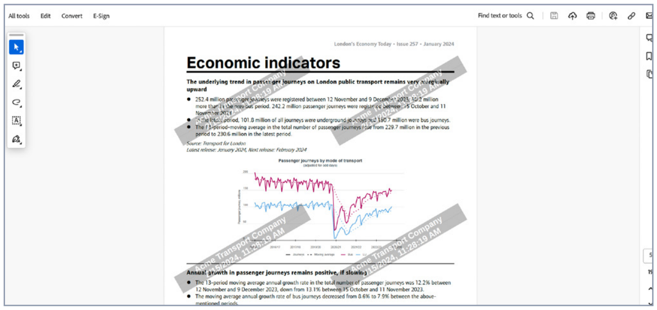
Menlo Security makes every browser an enterprise browser.

The Menlo Security Enterprise Browser solution stops phishing and malware attacks on any browser and any device across your hybrid enterprise.

It's finally safe to click.

Powered by the Menlo Secure Cloud Browser

Watermarked Web Page



London's Economy Today • Issue 257 • January 2024

Economic indicators

The underlying trend in passenger journeys on London public transport remains very marginally upward

- 252.4 million passenger journeys were registered between 12 November and 9 December 2023, 10.2 million more than in the previous period. 242.2 million passenger journeys were registered between 15 October and 11 November 2023.
- In the latest period, 101.8 million of all journeys were underground journeys and 150.7 million were bus journeys.
- The 13-period-moving average in the total number of passenger journeys rose from 229.7 million in the previous period to 230.6 million in the latest period.

Source: Transport for London
Latest release: January 2024, Next release: February 2024

Annual growth in passenger journeys remains positive, if slowing

- The 13-period moving average annual growth rate in the total number of passenger journeys was 12.2% between 12 November and 9 December 2023, down from 13.1% between 15 October and 11 November 2023.
- The moving average annual growth rate of bus journeys decreased from 8.6% to 7.9% between the above-mentioned periods.

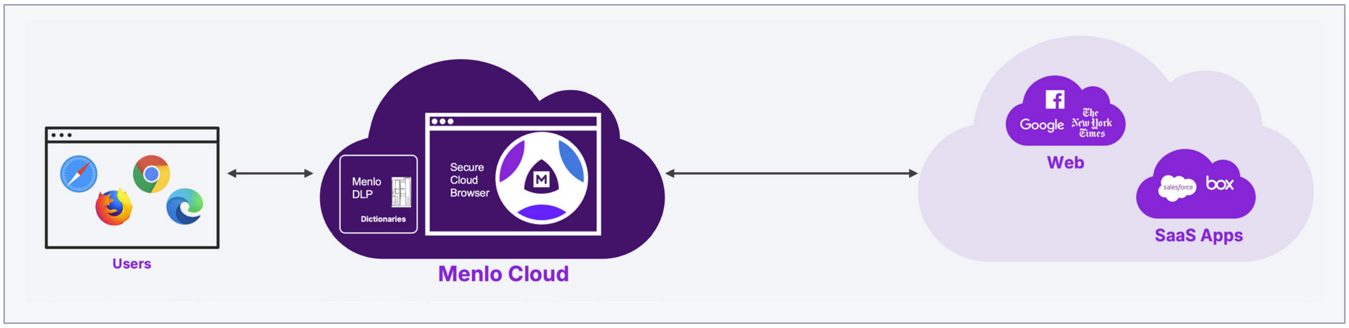
Watermarked Document

Dictionary-Based DLP for Files and Archives

For many organizations, disabling file uploads/downloads and managing exceptions to those policies can be onerous. Because one of the most common use cases for restricting file upload/download is to prevent the loss of data, Menlo also offers dictionary-based DLP with over 300 built-in DLP dictionaries, and it offers the flexibility to add more based on your specific data protection needs. You can gather dictionaries into templates, and both single dictionaries and templates of dictionaries can be bound to DLP rules. In addition, Menlo prevents downloads (Protect) or uploads (Secure) of files or archives that contain malware, by default.

Menlo DLP Operation with Menlo Protect

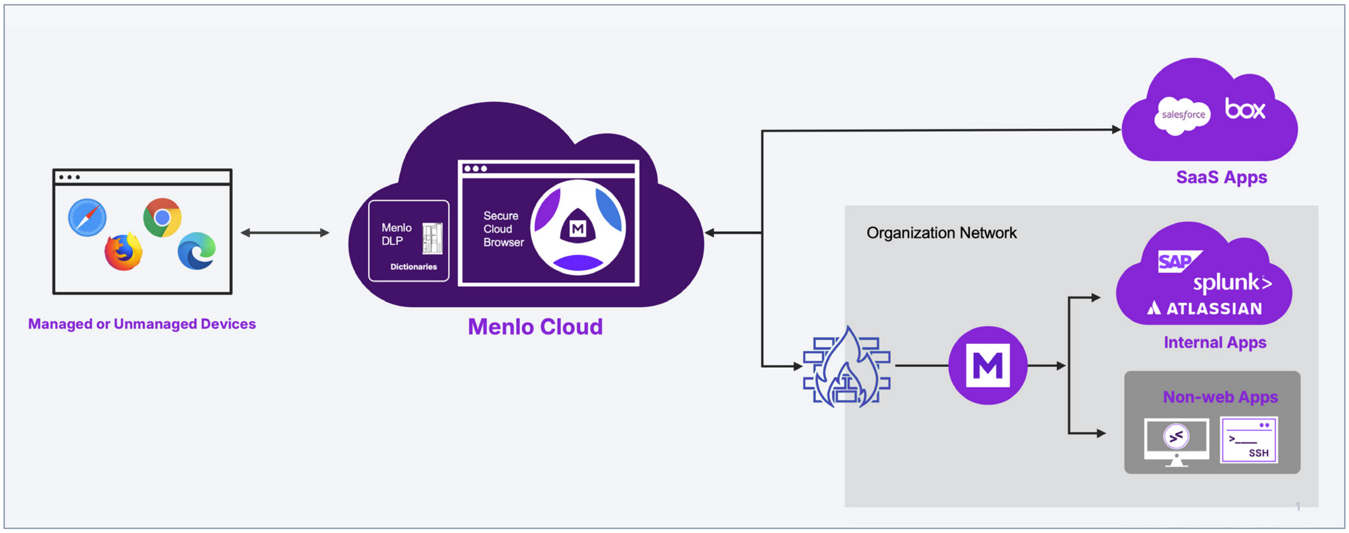
Menlo Protect is the first line of defense against the continuously evolving class of browser-borne attacks. The defense is provided by the Menlo Secure Cloud Browser, which delivers cloud-based browser security, separating the user's browser from web traffic. In addition, Menlo DLP examines every file passing through the Secure Cloud Browser, ensuring that sensitive data is prevented from being **uploaded to the internet**.



Menlo DLP with Menlo Protect

Menlo DLP Operation with Menlo Secure

Menlo Secure allows organizations to provide zero trust access to applications needed by the hybrid workforce. Users are granted access only to the applications required to do their jobs and nothing more. All applications provided by Menlo Secure Application Access are protected by the Menlo Secure Cloud Browser. And Menlo DLP examines every file passing through the Secure Cloud Browser, ensuring that sensitive data is prevented from being **downloaded to users' devices**.



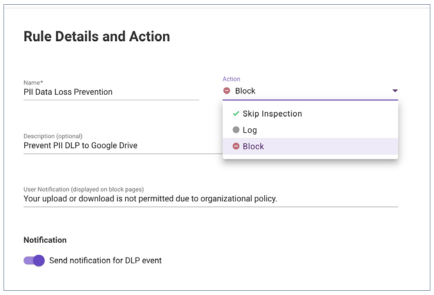
Menlo DLP with Menlo Secure

A few notes about the diagram above:

- In the organizational network, no VPN concentrator is visible, and there is no VPN client visible for the managed or unmanaged devices. The Menlo Secure Cloud Browser can deliver DLP and zero trust security with enhanced, least-privileged access superior to any legacy VPN.
- Menlo DLP controls prevent loss from the internal applications in the Organization Network portion of the diagram.
- Importantly, the Secure Cloud Browser offers security not typically available with VPNs or Cloud Access Security Brokers: a file with malware detected is blocked from upload or download. Beyond DLP, this by-default blocking protects the organizational network from infection and, with browser context, prevents applications behind web servers from infection.

Convenient, Intuitive DLP Workflows

What follows is an overview of Menlo dictionary-based DLP workflows. Rule creation occurs in a single screen, broken up here for visibility:



Rule Details and Action

Name*: PII Data Loss Prevention

Action: Block
- ✓ Skip Inspection
- ● Log
- ⊖ Block

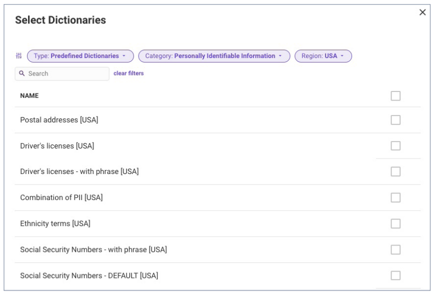
Description (optional): Prevent PII DLP to Google Drive

User Notification (displayed on block pages): Your upload or download is not permitted due to organizational policy.

Notification

● Send notification for DLP event

DLP Rule Creation Including Action



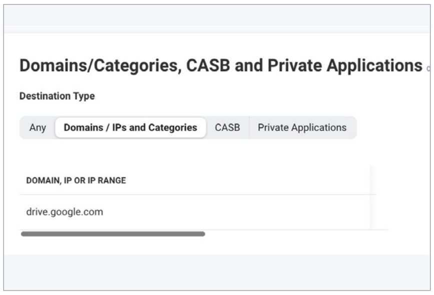
Select Dictionaries

Type: Predefined Dictionaries · Category: Personally Identifiable Information · Region: USA

Search · clear filters

NAME	□
Postal addresses [USA]	□
Driver's licenses [USA]	□
Driver's licenses - with phrase [USA]	□
Combination of PII [USA]	□
Ethnicity terms [USA]	□
Social Security Numbers - with phrase [USA]	□
Social Security Numbers - DEFAULT [USA]	□

DLP Dictionary Selection Criteria



Domains/Categories, CASB and Private Applications

Destination Type: Any | **Domains / IPs and Categories** | CASB | Private Applications

DOMAIN, IP OR IP RANGE
drive.google.com

DLP Destination: Google Drive

The portion of DLP rule creation illustrating exceptions based on users or groups is not shown. But as with the entire Menlo platform, DLP exceptions or enforcement can be specific to users or groups.

DLP for the Modern Workspace Requires Browser Context

With the web browser at the center of the modern workspace, data loss prevention requires browser context to prevent data loss through web pages as well as files carried using web protocols. Network-based solutions cannot control web page forms or see entire files carried with HTTP and HTTPS, nor can they cover the crucial security gap posed by password-protected files and archives. Data loss prevention features provided by the Menlo Secure Enterprise Browser solution bring crucial browser context to DLP. As importantly, users continue to work with the browser they prefer, with cloud-based browser security that scales to hundreds of billions of protected web sessions every year.

To learn more about securing the ways that modern users work, visit menlosecurity.com or email us at ask@menlosecurity.com

About Menlo Security

Menlo Security eliminates evasive threats and protects productivity with the Menlo Secure Cloud Browser. Menlo delivers on the promise of cloud-based security—enabling zero trust access that is simple to deploy. The Menlo Secure Cloud Browser prevents attacks and makes cyber defenses invisible to end users while they work online, reducing the operational burden on security teams.

Menlo protects your users and secures access to applications, providing a complete enterprise browser solution. With Menlo, you can deploy browser security policies in a single click, secure SaaS and private application access, and protect enterprise data down to the last mile. Secure your digital transformation with trusted and proven cyber defenses, on any browser.

Work without worry and move business forward with Menlo Security.

MENLO SECURITY

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