MENLO SECURITY

Browser SSE

Achieve the Goals of Security Service Edge While Closing the Browser Security Gap

Global trends, such as SaaS, cloud computing, and the explosion of generative AI, coupled with the global pandemic, have driven dramatic changes in how and where we work. The corresponding IT workspaces and workflows have changed, too, and many legacy technologies are strained and less effective because of these changes. IT teams were forced to adapt quickly, so some legacy systems were simply stuffed into the cloud.

Security Service Edge: Sideways Cloud Migration?

Security Service Edge (SSE) emerged before the most abrupt shifts of 2020, and has attempted to address some of the changes by offering cloud-based management and vendor consolidation for key network services. These services include zero trust access, cloud access security broker (CASB), and secure web gateway (SWG). Unfortunately, moving from appliances to software in the cloud doesn't really address the needs of the modern workforce. This "sideways cloud migration" proves costy to deploy and manage, and SSE is more complex than it should be. The result: IT teams struggle with long, complex SSE deployments caused by complicated network change requirements, client rollout challenges, and endless configuration tasks.

SOLUTION BRIEF

The Disadvantages of SSE

Cost and Complexity

A feeding frenzy occurred when industry analysts identified and named SSE. Larger players consumed smaller ones to build out their SSE components, leading to long and expensive journeys from acquisition to integration. The result often presented disadvantages for customers, including:

- SSE offerings seemed expensive to buyers and industry analysts alike, as vendors passed along acquisition and integration costs.
- Integration challenges resulted in SSE offerings that required multiple management consoles, sometimes with wholly different user experiences. For example, an exclusion criterion in a popular analyst piece on secure access service edge (SASE)[1] indicated that the analyst permits products with up to three consoles.

Network Integration

Imagine your company's network as a carefully constructed house of cards. You've got your public cloud over here, your private data centers over there, and all your branch offices connected by delicate WAN links. Everything is held together with things like GRE[2] tunnels (think secure pathways), carefully planned IP address ranges (CIDR[3] blocks), and your trusty firewalls and routers.

Now, you want to add cloud-based security (SSE), and suddenly, you're trying to squeeze new pieces into your house of cards. You need to:

- **Make room for new data paths —** Figure out how to punch the needed holes in your firewall and other DMZ[4] equipment to the SSE provider
- **Merge tunnels —** Combine your old secure pathways with the new ones from the SSE provider
- **Untangle security policies —** Identify and resolve conflicts between your existing security rules and those of the SSE service
- **Juggle routing tables —** Update your network's roadmap to accommodate all these changes

It's no wonder that people are constantly discussing these challenges on security forums! Bringing SSE into a complex network can be a tricky balancing act. And even given all of these challenges, SSE does not address what is acknowledged to be the primary workspace of the modern enterprise: the browser.

[1] SASE began strictly as a superset of SSE, but the vendors mentioned across the two solutions have diverged, indicating that they are different products. But while SSE is a subset, many SSE offerings include up to three management interfaces.
[2] Generic Routing Encapsulation
[3] Classless Inter-Domain Routing
[4] Demilitarized Zone: a metaphor adopted by IT globally to describe their data center edge, typically located between two firewalls, one on the "data center" side and the other on the "internet router" side.

The Browser Security Gap

SSE offerings provide defenses that can't stop attacks or data theft that target the browser. Let's look at these deficiencies by defense layer:

- SSE SWG offerings remain network security oriented. While most SWGs can, and do, fully look at each data packet for threats, attacks like HTML smuggling embed malware across multiple HTTP packets, and will skip embedding itself in packets at random to prevent discovery by devices that can aggregate multiple packets. Only a full browser, acting as an application, not at the network layer, processes the entire web session. Only browser security prevents attacks with full browser context.
- SSE CASB offerings are, like SWGs, network oriented, but they also attempt application-layer controls. That said, CASB core functionality is managing cloud access and use. While some CASBs can see and flag the download of password-protected, encrypted files, only dedicated browser security can block these files or prompt for a password, so that an encrypted file can be decrypted and inspected. Meanwhile, CASB vendors may have forgotten that every organization has vulnerable internal web applications.

SSE manages traditional network security from the cloud, but it's still infrastructure-focused network security. Modern computing is applications and application access, regardless of location and device. Menlo Browser SSE is all about applications, not the network.

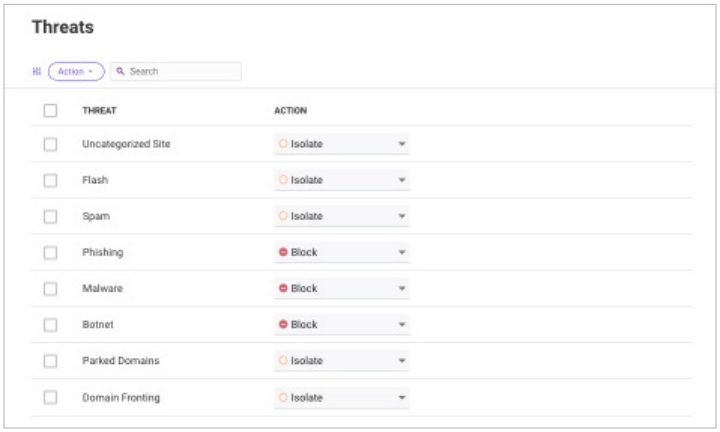
Achieve SSE Goals and Close the Browser Security Gap

Most users are accessing the majority of their applications through the web browser, which presents an enormous risk when using approaches that do not consider the browser. The Menlo Security Browser SSE solution enables you to achieve the goals of SSE, which, combined with comprehensive browser security, closes the browser security gap at scale for all users' activities in their preferred browsers.

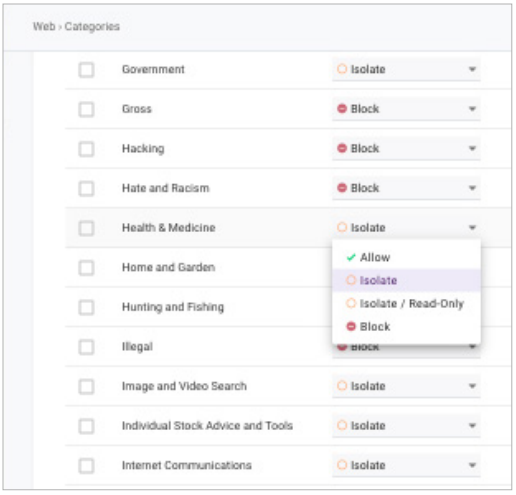
A Secure Web Gateway Cannot Close the Browser Security Gap

The mainstream SSE SWG stops known threats. In contrast, the Secure Cloud Browser at the center of Menlo Browser SSE treats all web traffic as risky, stopping zero-day phishing attempts and evasive ransomware.

The Menlo Secure Enterprise Browser solution offers full SWG functionality and much more. The core of SWG functionality includes traffic categories and URL filtering. A SWG can block some uncategorized URLs. But, as a network device, a SWG simply cannot see all of what's coming over HTTP/S. Closing the browser security gap requires application security rather than network security. With SWG defenses alone, a local browser loads a full web transaction, but can also suffer from malware embedded in that session. The Menlo Secure Cloud Browser stops the highly evasive and adaptive threats no SWG can stop, including HTML smuggling, malware in encrypted files, and LURE attacks.



Your SWG cannot isolate threats



Your SWG cannot isolate web sessions

SaaS Governance

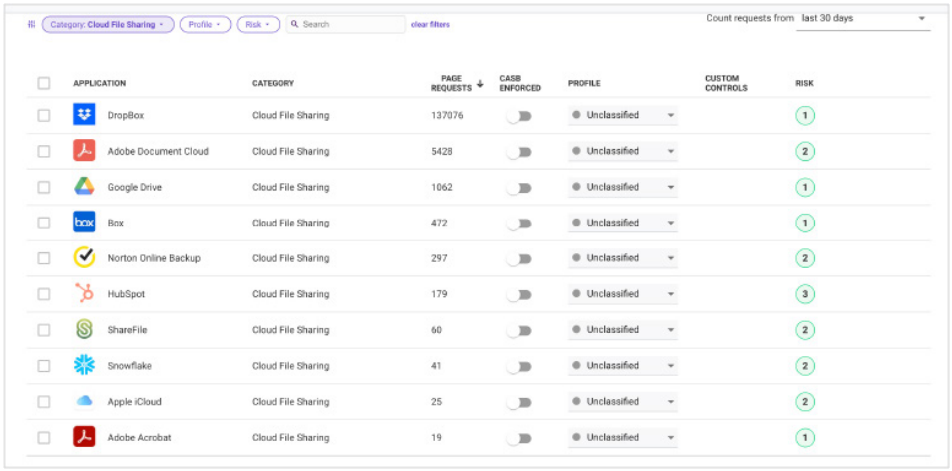
The mainstream SSE CASB controls which users are permitted and which SaaS sites are allowed. In addition to those controls, SSE CASBs may include attempts at data loss prevention, but they are often insufficient.

SaaS governance provided by the Menlo Browser SSE solution offers CASB-equivalent controls, leveraging an intuitive administrative workflow and a user-friendly experience.

Menlo SaaS governance begins with a curated list of thousands of known web applications, a number that is frequently increasing.

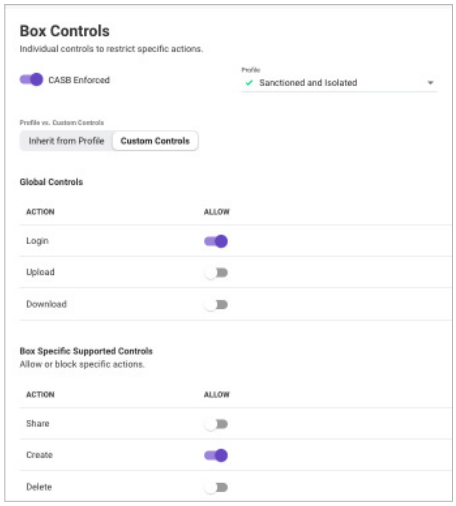
Intuitive, Fast SaaS Governance Workflow

Cloud application discovery gives you the information you need to manage SaaS consumption in your organization.



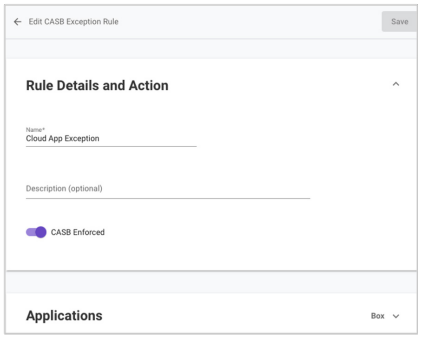
In this illustration, Cloud Application Discovery has been filtered on an important data security and DLP category: Cloud File Sharing

Rules give you the unique combination of security and flexibility. You can assign rules on a per-application basis. Here is an example of rule management for Box.com, which no CASB could replicate. Menlo can isolate browser sessions to sanitize HTML, and apply machine learning to stop phishing attacks.

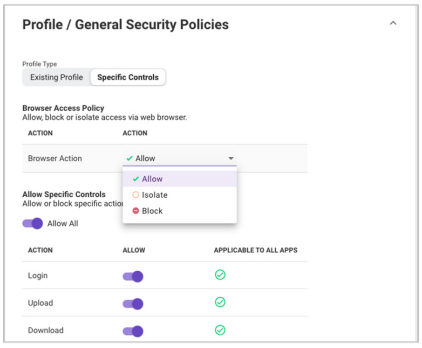


With Menlo, you can assign rules by application

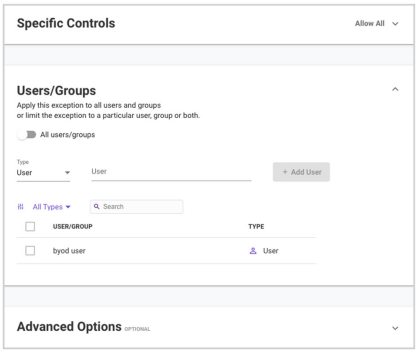
Exceptions: Least-privileged access requires that default rules for web properties apply to all users and groups at all times. But Menlo Cloud Governance, like all Menlo policies, provide exceptions to default rules with the same level of specificity. The illustrations below show some of the attributes of a Cloud Governance exception. In addition, as users log into the service, the comprehensive Menlo integrations with all leading third-party authentication providers offer both time- and location-based controls on login permission.



This exception pertains to box.com



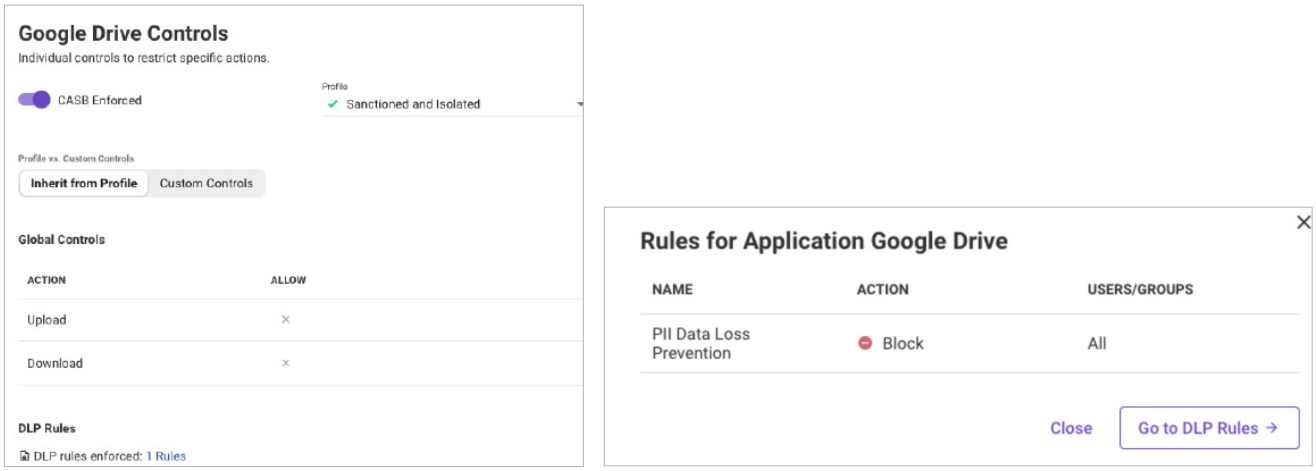
This exception permits file uploads or downloads, which was not allowed by the default rules for the web site.



Here, we have assigned the exception to a single user.

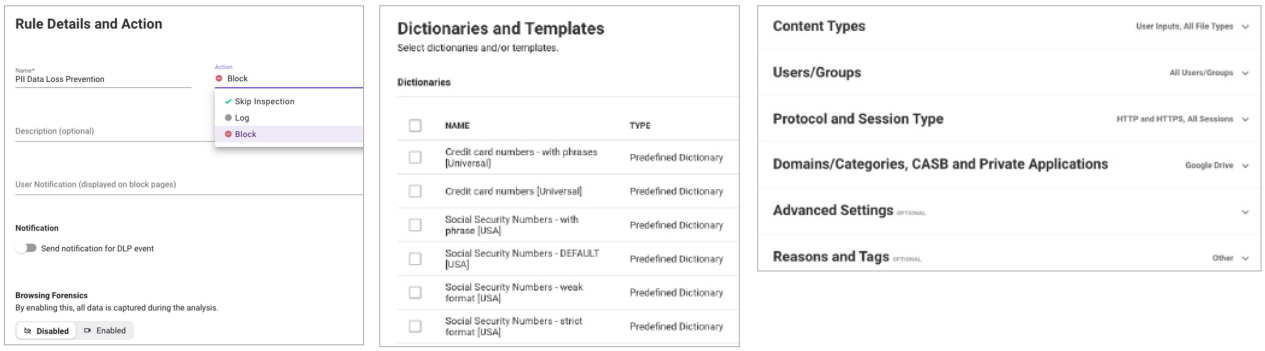
Data Loss Prevention

Menlo SaaS governance offers powerful, browser-centric data loss prevention (DLP) controls, with almost 400 built-in DLP dictionaries and the flexibility to add more based on customer requirements. Dictionaries may be gathered into templates, and either single dictionaries or templates of dictionaries can be bound to DLP rules. After DLP rules are created, they can be bound to SaaS governance profiles.



Above, you can see that the DLP rule for Google Drive is intended to prevent loss of personally identifiable information (PII)

Below, you can see an example of DLP rule details. The left pane shows high-level rule attributes, as well as whether Menlo Browsing Forensics should capture web sessions associated with the DLP rule. The middle pane shows that this rule includes six DLP dictionaries. The right pane shows six additional, expandable rule attributes, which are presented in an intuitive order.



Even with the most stringent controls and carefully considered policy exceptions, accidents or nefarious behavior can happen in any large organization. Menlo Security Browsing Forensics enables accelerated resolution of detected incidents, because SOC personnel have immediate access to recorded web sessions. Menlo Browsing Forensics is integrated with Menlo SaaS governance, as seen above in the definition of a DLP rule attached to a SaaS application.

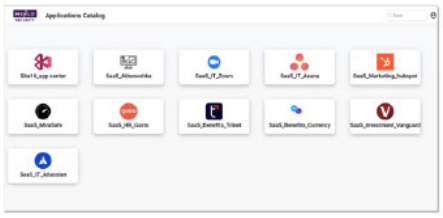
Menlo SaaS governance offers simple workflows and easy-to-manage controls over the use of a curated list of almost 3,000 SaaS applications. With browser-centric DLP and Menlo Browsing Forensics, Menlo Browser SSE brings your SaaS applications under control and closes the browser security gap.

Zero Trust Access

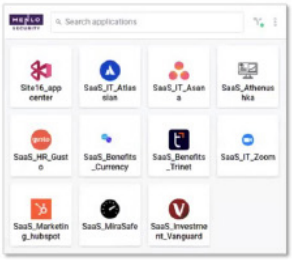
The core principles of zero trust include user and device verification and authentication, least-privileged access, and continuous monitoring and verification. Many of these principles were first implemented in the network as zero trust network access (ZTNA). But we live now in an application-centric world, in which ZTNA has evolved to become zero trust access (ZTA). Unfortunately, most zero trust offerings cannot close the browser security gap.

Menlo Browser SSE offers zero trust access through Menlo Secure Application Access, which is fast to deploy and easy to manage from a single console. Menlo Secure Application Access, combined with the Menlo Secure Cloud Browser, delivers comprehensive zero trust access.

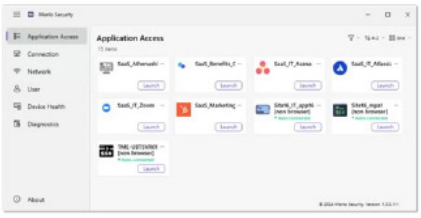
Mainstream SSE zero trust network access is almost universally provided via clients, which requires more desktop software to deploy and manage. In contrast, Menlo zero trust access delivers access to internal and external web properties through users' web browsers. Clientless access is ideal for multiple use cases, such as contractors, guests, and BYOD.



Secure Application Access
Web Portal View



Secure Application Access
Browser Extension View



Secure Application Access
Menlo Security Client View

Browser-focused ZTA delivers secure and least-privileged access to permitted internal and SaaS applications. And with data secured through the Secure Cloud Browser, legacy VPNs can be decommissioned, eliminating traffic backhauls.

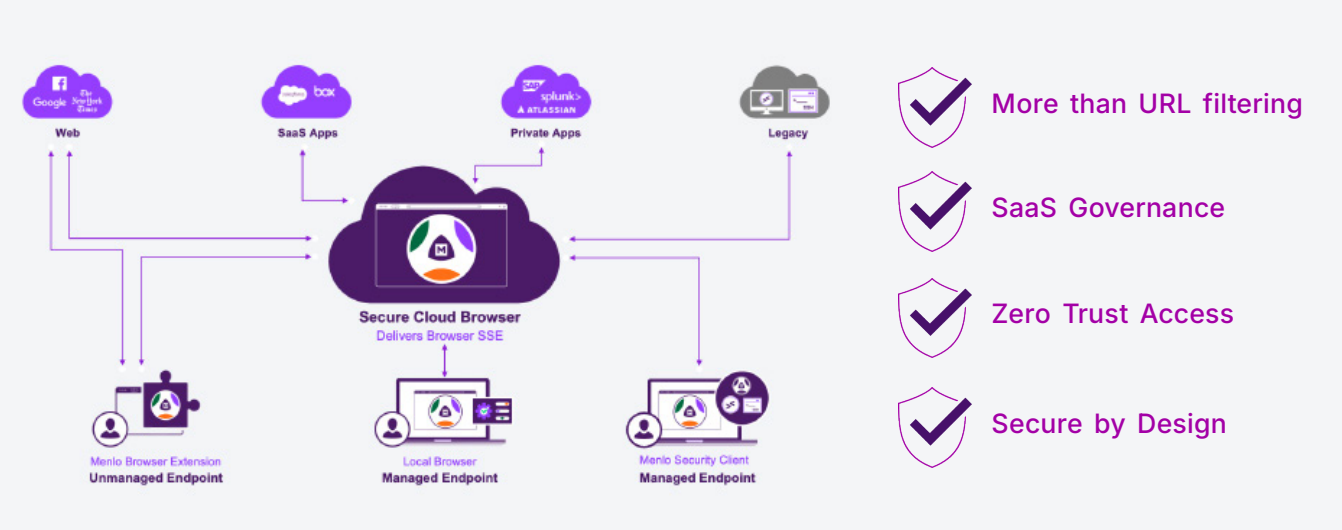
To understand the benefits of Menlo Data Loss Prevention for zero trust access, it is important to understand two forms of data risk:

- **Downloading** content from internal web sites is a crucial data loss vector. Menlo policies can prevent users from downloading files or archives from internal web applications outright, or downloads may be permitted with Menlo DLP scanning them to ensure that they do not contain unpermitted content.
- **Uploading** content to the internet is another critical data loss vector. Menlo policies can prevent users from uploading files or archives to specific websites, or can block uploads outright. Or, users may be permitted to upload files or archives after Menlo DLP scans them for unpermitted content. In addition, Menlo enforces policies on pasting, which can close another significant data loss vector.

As with Menlo SaaS governance, Menlo Browsing Forensics is integrated with Menlo Secure Application Access. The combination ensures that permitted users access only required content, and that there is complete visibility into their actions during any browsing session. Least-privileged access and full visibility are two essential steps in the journey to zero trust.

In Summary

The web browser is the most widely used app in the modern enterprise, the place where work gets done. With this reliance on the browser, and the continued migration of apps to the cloud, it is imperative to close the browser security gap, a problem that can't be solved by other SSE offerings. Menlo Security Browser SSE enables you to achieve your SSE goals, while closing the browser security gap using one management console, not two or three. Users continue to work with the browser they love, with cloud-based security that scales to billions of protected web sessions per month. Menlo Browser SSE delivers the security, visibility, and incident response assistance that the modern organization requires for zero trust.



Menlo Security Browser SSE: built into the Secure Enterprise Browser solution

To learn more about securing the ways people 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.