MENLO SECURITY

Data Sheet

Menlo Security Browsing Forensics

Shine a light on browser activities

Security and IT professionals have always required visibility into enterprise events to provide appropriate defenses. This need for visibility has led to an array of security tools and platforms. Firewalls historically provided perimeter-level security, while secure web gateways (SWGs) delivered network security and filtering in accordance with policy and data loss prevention (DLP) protections tracked intellectual-property assets.

These technologies have different central purposes, but they all have one thing in common: to provide the vital intelligence that enables enterprise security teams to lock down the network, endpoints, and applications. The downside is that as security controls have tightened around the network and the endpoint, attackers have had to look for other, less secure assets to infiltrate the enterprise. And they've found this blind spot in an unexpected place: the browser.

Three things to know:

Organizational attack surfaces have expanded enormously in recent years. This growth has been driven notably by accelerated adoption of SaaS, expanding digital supply chains, increased corporate presence on social media, custom application development, remote working, and internet-based customer interaction.[1]

Web browsers are the most widely used enterprise applications, and they represent a massive blind spot for enterprise security.

Researchers discovered a 198% increase in browser-based phishing attacks in the second half of 2023 compared to the first half of the year.[2]

1 Gartner Top Trends in Cybersecurity for 2024

2 State of Browser Security: Defending browsers against zero-hour phishing attacks, Menlo Security

The blind spot created by the browser has spawned a new category of threat. Known as Highly Evasive Adaptive Threats (HEAT), these exploits target the browser to penetrate the enterprise "under the radar." As organizations have adopted the SaaS model, vital enterprise apps have become increasingly accessible by the browser. Users no longer need to open specific apps to get the resources they need because the browser enables access to everything. The browser, as the universal client for both consumer and enterprise applications, has emerged as the new, unmanaged, and vulnerable attack surface. Enterprises need visibility and control over browsers to reduce the new risk.Along with browser isolation, Menlo Security converges all secure web gateway capabilities into a single cloud-native platform—including CASB, DLP, RBI, Proxy, FWaaS, and Private Access—to provide extensible APIs and a single interface for policy management, reporting, and threat analytics.

Network or endpoint-based security platforms provide a plethora of information, but even the most sophisticated of these tools simply cannot provide meaningful visibility into users' browser sessions. Security and IT teams may be able to tell that a DLP event has happened, for example, but they cannot easily trace exactly how the event occurred.

In the case of an incident response, teams are left trying to piece together fragmented information, tracking malicious actions by the clues these actions leave rather than viewing the actions themselves. In a search for clarity, teams sometimes have to interview users themselves, asking people to review specific actions they took hours or weeks in the past.

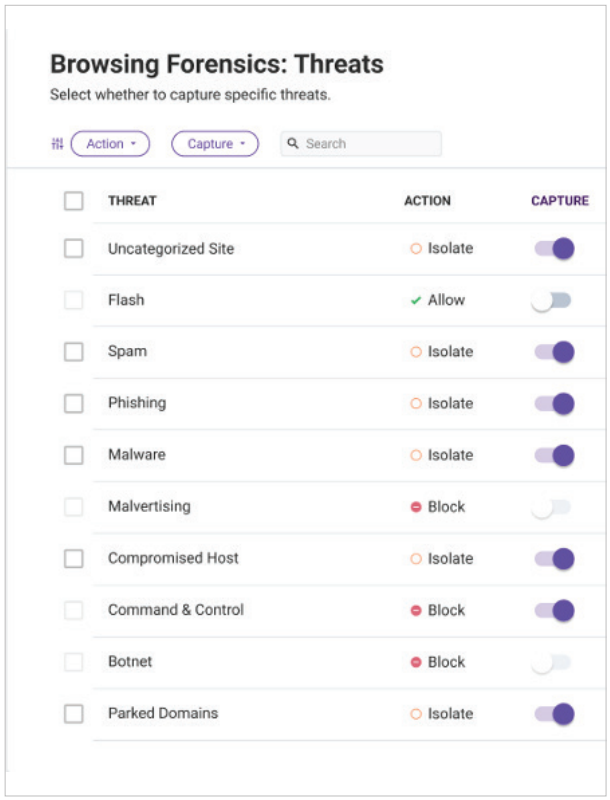
Using traditional security capabilities to solve a breach is like trying to crack a burglary case by measuring footprints rather than checking security cameras.

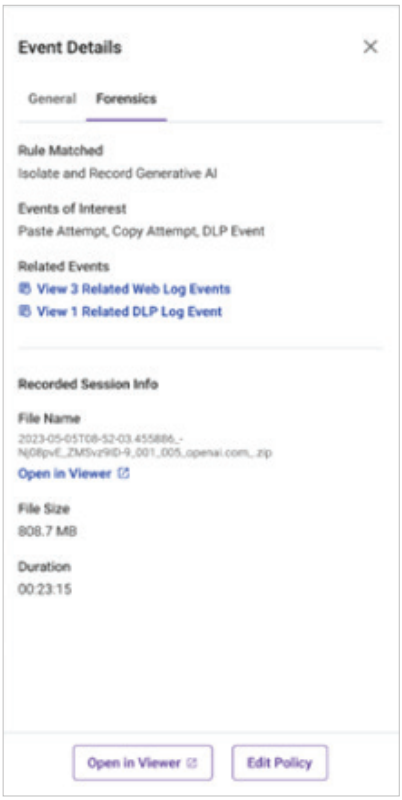
Not only does this method of incident response yield ambiguous results, but it is also time-consuming. Extra time and staff focus, two elements in short supply in most enterprises, are required to carry out investigations. Dedicated threat hunters are likewise hamstrung by a lack of visibility into browser sessions. As with any other security incident, the time required to determine the details of an organization's exposure multiplies the possibility that an initial exploit can have severe repercussions.

Product Overview

Menlo Security Browsing Forensics records policy-defined browser sessions to support customer teams with the investigation of security, audit / compliance, HR and other necessary events. The recordings are based on policy triggers, such as Heat Shield detections or users accessing private or sensitive applications.

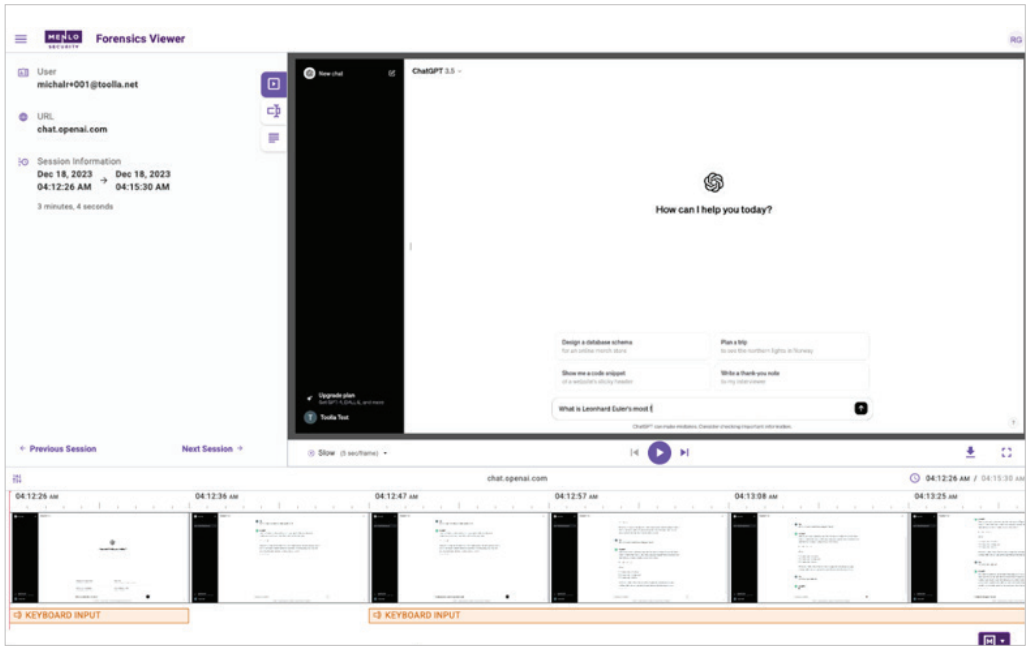
Each recorded session has a Menlo Forensics Log entry that includes supporting data of the event and one-click access to the recording. The Forensics log data, available in near real time, includes a link to the associated recording. The recorded sessions are transferred to a customer's defined location for secure, access-controlled storage. Browsing Forensics supports both AWS and Azure storage options.





The Menlo Security Browsing Forensics Viewer presents the rich content of the recording, enabling analysts to reach substantiated conclusions quickly and easily.

Menlo Logs provide customers with all the traditional details of the user sessions, including actions such as DLP or Copy/Paste and the results of virus scanning and sandboxes. Additionally, Menlo Browsing Forensics Logs adds a summary of the critical events and any corresponding logs that may be of interest. For example, the researcher may be investigating an internal threat and the Browsing Forensics Logs contain the link to DLP Log for a complete picture of the exposure and intent.



A summary of the Browsing Forensics recording is included in logs with a link to the recording. With one click the researcher is viewing the browsing session data, significantly reducing the time required to complete an investigation.

Some of the use cases for Browsing Forensics include:

- Phishing Incident Response
- Data Security
- Threat Hunting
- Generative AI sites & ChatGPT
- Copy/Paste
- Security Research
- Insider threat
- Audit and compliance

Benefits

Get information you can use, not data you have to parse

With Menlo Security, you can finally connect the dots between a triggering security event and the details of the incident. Menlo Browsing Forensics automatically preserves a comprehensive record of web sessions and user interactions, so you can access the complete history of any browser session. Records are automatically stored in the location of your choice and can be sent to your SIEM.

Resolve security incidents quickly

Every hour that a security incident goes unresolved amplifies the potential exposure for an organization. Menlo Security Browsing Forensics enables you to visualize the missing browser-based information you need to determine exactly how an incident unfolded. With the ability to see user actions, you can decide if a user's actions were inadvertent or possibly malicious.

Maintain privacy – for your organization and your users

While Menlo Security enables visibility, the system does not keep the record of user browsing, nor does operations involve Menlo staff viewing these sessions. Content is sent directly to the AWS or Azure storage that you choose and logs can be ported to your SIEM at your direction.

Manage the browser with Menlo Security

Menlo Security secures all the browsers used in the enterprise. Menlo protects your users, and secures access to applications and associated enterprise data, providing a complete enterprise browser security solution. 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, with Menlo Security.

MENLO SECURITY

To find out more, contact us:

menlosecurity.com

(650) 695-0695

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.