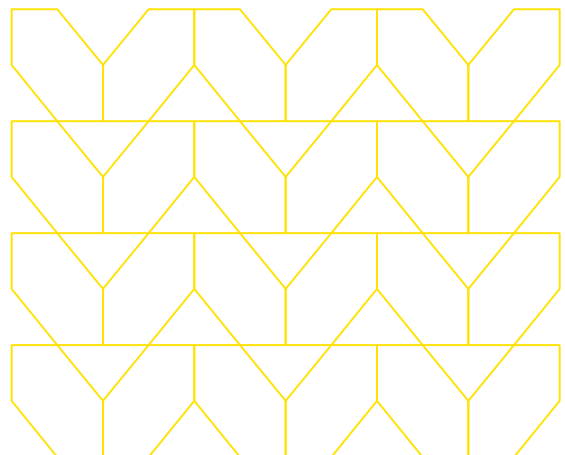
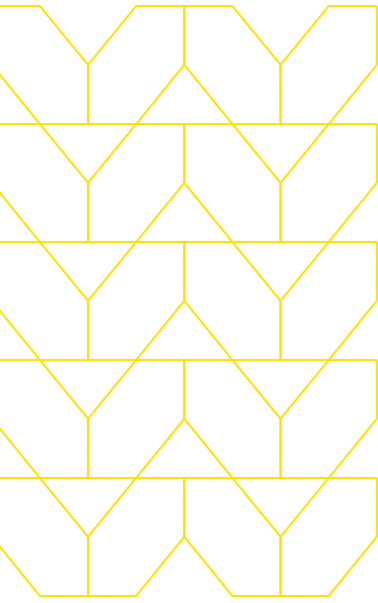


Browsing Forensics with HEAT Shield

Get visibility into the most dangerous threats targeting the browser and stop them cold

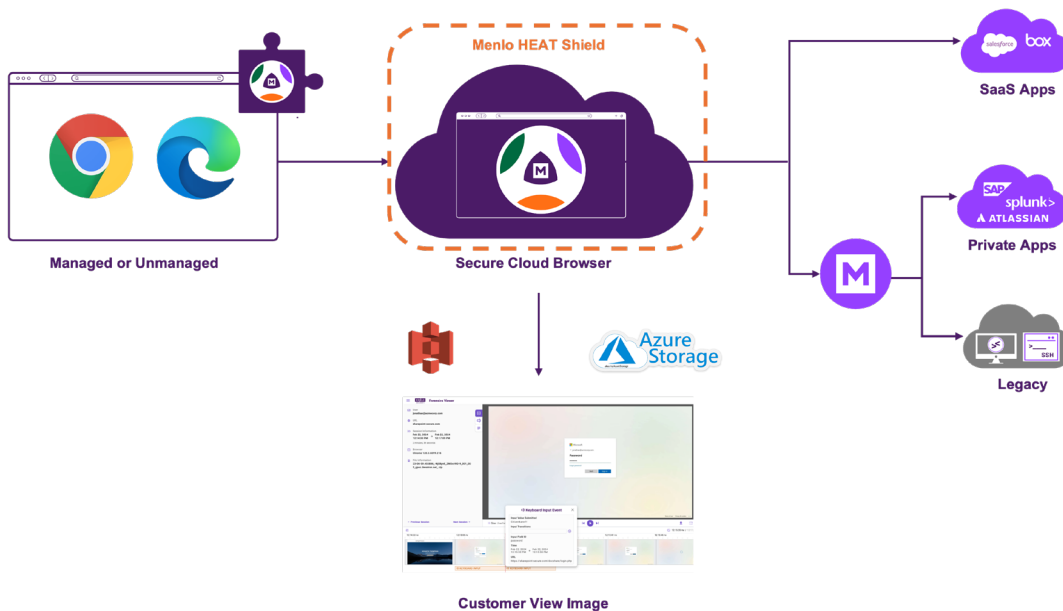


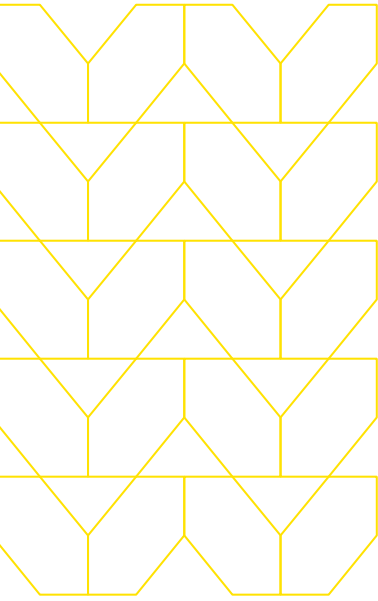
Solution Brief



As enterprise applications have moved to the cloud and hybrid /remote work has become the norm, users have come to rely on the browser as their primary method to access the apps and data that they need to do their jobs. As a result, the browser has become the central workspace in the enterprise, replacing many traditional desktop apps. While this move has created great opportunities, it has also served to exacerbate an existing issue – visibility. Because browser traffic has been designed to punch through network-level defenses, activities within user sessions have historically been opaque to security and IT teams. The explosive growth of threats like phishing and other browser-based attacks have naturally followed suit.

The ability to dig into the source of these browser-based attacks have eluded security and incident response professionals for years. These teams have had to painstakingly piece together information from network security tools, secure web gateways, other cloud security platforms, and endpoint detection and response (EDR) tools, as well as inspecting the user's device itself. Unfortunately, at the end of the day, response teams are left to infer a conclusion, because they have no definitive proof. Threat hunters are presented with a similarly difficult job, as the sites from which an attack begins don't remain live for long – by design.





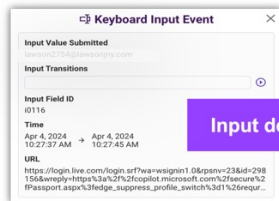
Browsing Forensics has the answers you need

Browsing Forensics from Menlo Security solves the visibility problem. When traffic passes through the Menlo Secure Cloud Browser, Browsing Forensics can be configured to capture sessions as specified by website category, threat, user, or group. The recorded packages are then immediately sent to the customer's choice of storage location.

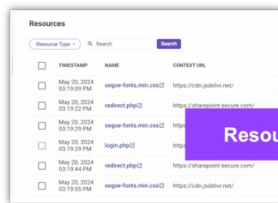
End investigations with details, not guesswork

Browsing Forensics presents a wealth of detail in just a few clicks, with no need to reassemble files, interview users, or inspect the endpoint to reconstruct an event. With Browsing Forensics, you just press "Play," and you are presented with screen captures of exactly where the user went, and what they did while they were there.

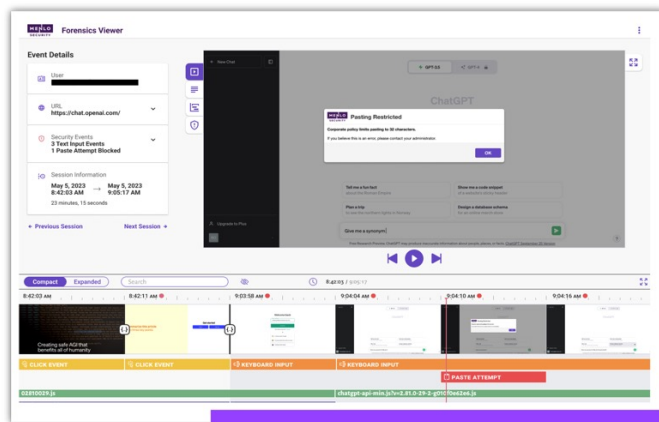
Not only can you see the screens that the user interacted with, but there is also a record of the user inputs, so in the case of a phishing site you'll know if credentials were entered. Browsing forensics also captures the page resources themselves, so threat hunters can learn about attackers' methods even if the site itself is no longer live.



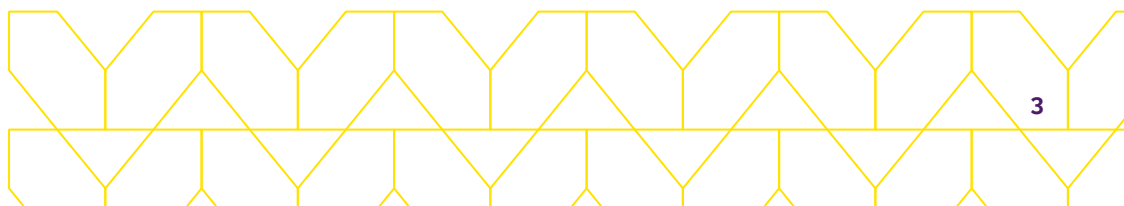
Input details



Resources



Forensic Viewer presents details – just press play





HEAT Shield stop these threats in their tracks

These techniques are particularly important as they relate to Highly Evasive and Adaptive Threat (HEAT) attacks, which are often used to establish a beachhead in the enterprise that is later used in ransomware or extortion attacks. HEAT Shield from Menlo will capture the attack and stop it cold; with Browsing Forensics, security teams can also get the details that they need to warn users or be on the lookout for similar techniques. Menlo DLP controls can protect against leakage of sensitive information. Finally, in the case of an incident, Browsing Forensics provides invaluable data needed to comply with regulations.

Browsing Forensics is also a companion to Menlo Secure Application Access. Whether you seek to optimize VDI deployment or replace VPNs, Secure Application Access makes the process simple, while Browsing Forensics delivers the user session details that you need.

Find out more about HEAT Shield here: <https://www.menlosecurity.com/product/protect/heat-shield>

Find out more about Browsing Forensics here: <https://www.menlosecurity.com/product/manage/browsing-forensics>



To find out more, contact us:

[menlosecurity.com](https://www.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.

© 2024 Menlo Security, All Rights Reserved.