COALFIRE

WHITE PAPER

Menlo Security Secure Enterprise Browser Solution

Applicability for use with the HIPAA Security Rule

COALFIRE OPINION SERIES – Final

JASON WIKENCZY | CISSP, CISA, QSA

MENLO SECURITY

877-224-8077 | info@coalfire.com | **Coalfire.com**

Table of contents

Executive summary

Menlo Security has engaged Coalfire Systems, Inc. (“Coalfire”) to conduct an independent technical review of its Menlo Secure Enterprise Browser solution (“the solution”) for its efficacy in assisting organizations that use (or are considering using) the solution to access electronic protected health information (ePHI) and to meet the technical requirements of the HIPAA Security Rule.

This Product Applicability Guide (PAG) examines an entity’s adoption of the Menlo Secure Enterprise Browser solution in alignment with the Technical Safeguards of the Health Insurance Portability and Accountability Act (HIPAA) Security Rule. This PAG outlines Coalfire’s methodology for assessment and the approach used for its review, summarizes findings from Coalfire’s review of product capabilities, provides context for the use of these capabilities, and states an opinion as to how the Menlo Secure Enterprise Browser solution’s security capabilities, functions, and features can assist organizations with supporting HIPAA Security Rule Technical Safeguards.

Coalfire PAGs provide a specific Coalfire opinion of a product’s applicability to standards, frameworks, and mandates, through the “eyes of the assessor” and should not be construed as a specific endorsement. PAGs are provided as an element of Coalfire’s product guidance services and are authored solely to inform users currently evaluating Menlo Secure Enterprise Browser and prospective customers who are interested in using the solution.

Coalfire opinion

Coalfire reviewed the Menlo Secure Enterprise Browser solution and determined that it can support HIPAA Security Rule objectives when it is properly employed by customers in covered environments. The solution provides controls necessary for securing and managing access to ePHI, including functionalities such as granular access control, data security within applications, user behavior analytics, continuous monitoring, verification, and enforcement, and additional services discussed throughout this white paper that contribute to HIPAA compliance. These functions can support numerous HIPAA Security Rule Technical Safeguards by minimizing access privileges, protecting sensitive data, and enabling detection of suspicious activity. The solution focuses on application security, establishing secure perimeters around integrated/connected applications, and reducing the attack surface.

Coalfire’s opinion depends on underlying assumptions, such as the alignment of customer configuration to HIPAA objectives, customer capabilities for supplemental and complementary controls, and alignment of HIPAA objectives across integrations with existing security tools such as identity and access management (IAM), network segmentation, and cross-domain orchestration. Within its domain, the Menlo Secure Enterprise Browser solution offers a viable foundation for supporting HIPAA Security Rule Technical Safeguards.

Purpose

The primary purpose of this PAG is to render Coalfire’s opinion and supporting observations, based on its review, of the Menlo Secure Enterprise Browser solution’s suitability to assist Menlo Security customers in meeting HIPAA Security Rule objectives. Coalfire used the following process in the development of this PAG:

- Choose possible and relevant use cases for the Menlo Secure Enterprise Browser solution.
- Identify any dependencies used for review.
- Reveal additional technical details of the solution.
- Collect artifacts, perform review, and document findings.

- Make relevant statements about the particulars of the Menlo Secure Enterprise Browser solution that can support HIPAA Security Rule objectives.
- State Coalfire's opinion of the review of the Menlo Secure Enterprise Browser solution's capacity to be used for adherence to HIPAA Security Rule objectives.

Although the opinion itself may be helpful, this PAG also contains a representative overview of many aspects of the HIPAA Security Rule, which readers may find of use. Coalfire also focused on the technical controls supporting HIPAA Security Rule objectives through use of a tenant deployment with the Menlo Cloud. Additionally, Coalfire reviewed training and administrative documents, written supporting materials, and other technical artifacts provided as part of Menlo Secure Enterprise Browser solution documentation. Coalfire did not review organizational processes, procedures, or other non-technical artifacts.

Introducing the HIPAA Security Rule

The HIPAA Security Rule is a federal regulation that mandates healthcare organizations to implement safeguards to protect electronic protected health information (ePHI). Covered entities and business associates (CE&Bs) face a constant challenge in securing ePHI from a variety of internal and external threats.

The HIPAA Security Rule is designed to be flexible and scalable, allowing covered entities to tailor their security measures to their specific size, complexity, and risk environment. The rule prioritizes technology neutrality, meaning it doesn't dictate specific technologies for implementation. Instead, CE&Bs can choose any security measures they believe are reasonable and appropriate to meet the required standards and implementation specifications (HHS, https://www.hhs.gov/hipaa/index.html).

Core requirements of the HIPAA Security Rule

The HIPAA Security Rule establishes core requirements for CE&Bs to ensure the confidentiality, integrity, and availability of ePHI. These requirements are outlined in 45 CFR § 164.306 Security standards: General rules:

- Confidentiality, integrity, and availability: CE&Bs must ensure all ePHI they create, receive, maintain, or transmit is protected against unauthorized access, modification, or loss.
- Risk management: CE&Bs must identify and protect against anticipated threats or hazards to the security of ePHI.
- Authorization: CE&Bs must implement safeguards to prevent unauthorized disclosures of PHI not permitted by HIPAA.
- Workforce compliance: CE&Bs must ensure their workforce is trained and compliant with HIPAA regulations.

45 CFR § 164.306(b): Flexibility of Approach, provides guidance for selecting security measures. The HIPAA Security Rule categorizes its requirements into different categories:

- Security standards: General rules
- Administrative safeguards
- Physical safeguards
- Technical safeguards
- Organizational requirements
- Policies and procedures and documentation requirements

Within these categories, some implementation specifications are classified as either required or addressable:

- Required: These must be fully implemented by the organization. All standards within the Security Rule are considered required.
- Addressable: Organizations have more flexibility with addressable specifications. They can choose to:
  - Implement the addressable implementation specification as defined.
  - Implement an alternative security measure that achieves the same outcome.
  - Not implement the specification or an alternative but must document the decision and justification.

This concept of addressable implementation specifications allows covered entities flexibility in how they achieve compliance, as long as the overall objectives of the rule are met.

Relationship between HIPAA Security and Privacy Rules

HIPAA mandates the Department of Health and Human Services (HHS) to develop regulations for protecting health information privacy and security. These regulations are known as the HIPAA Privacy Rule and the HIPAA Security Rule. The Office for Civil Rights (OCR) within HHS enforces these rules through compliance activities and potential civil money penalties (HHS, 2021).

- HIPAA Privacy Rule: Establishes national standards to protect individuals' health information.
- HIPAA Security Rule: Establishes national security standards for protecting ePHI.

The Security Rule complements the Privacy Rule by outlining the technical and non-technical safeguards that covered entities need to implement to secure ePHI.

Aligning with NIST Special Publication (SP) 800-161

The National Institute of Standards and Technology (NIST) Special Publication (SP) 800-161 provides a comprehensive framework for safeguarding controlled unclassified information (CUI) in nonfederal systems and organizations. While not directly focused on HIPAA, the core principles outlined in SP 800-161 can be adapted and leveraged to strengthen HIPAA compliance efforts. These core principles include:

- Least privilege access: Ensure that users and devices possess only the minimum access permissions required to perform their designated tasks, minimizing the potential exposure of ePHI in the event of a security breach.
- Continuous monitoring: Implement ongoing monitoring and analysis of all access attempts and network traffic to detect and respond to threats in real-time, safeguarding the integrity of ePHI.
- Data security: Enforce robust data security measures to protect ePHI at rest, in transit, and in use. This includes encryption, access controls, and data loss prevention (DLP) techniques.

Shifting the focus from location to identity and context

The focus of HIPAA compliance has shifted from a location-centric model to one centered around user identity, context, and data. This necessitates fine-grained security controls that can dynamically adapt to evolving threats and user behaviors while ensuring granular access control to ePHI.

While achieving a fully HIPAA-compliant environment can be a complex process, industry guidance documents such as the HIPAA Security Rule provide a roadmap for organizations to follow. By adopting a security posture that prioritizes access controls, continuous monitoring, and data security, organizations can significantly enhance their ability to safeguard ePHI and achieve HIPAA compliance.

HIPAA compliance and modern web browser use

The modern work environment, characterized by the integration of cloud-based healthcare applications and the rise of hybrid work models, necessitates robust security measures to protect electronic protected health information (ePHI) during web browsing activities. HIPAA compliance demands stringent access controls, audit controls, and data integrity to safeguard ePHI.

Browsers, now the primary interface for accessing critical healthcare applications such as electronic health records (EHR) and patient communication portals, have become potential vulnerabilities if not adequately secured. Malicious actors exploit browser weaknesses through sophisticated attacks like HTML smuggling, embedding malicious code within seemingly harmless content to bypass traditional security measures and gain unauthorized access to ePHI.

HIPAA compliance requires continuous monitoring and verification of all data flows, regardless of origin or destination. The assumption of inherent browser security is challenged, as even legitimate web content may harbor elements with malicious intent. To safeguard ePHI, organizations must move beyond perimeter defenses and endpoint security alone, adopting a comprehensive browser security approach that includes isolation, inspection, and continuous monitoring of web traffic.

Traditional web security measures like URL filtering and antivirus scanning often fall short in distinguishing between benign and malicious content in the context of HIPAA compliance. Real-time analysis of web content, combined with strong isolation techniques to contain potential threats before they reach endpoints, is crucial.

Aligning with HIPAA principles, browser security should be an integral part of an organization's overall security posture. This involves implementing layered security controls, enforcing consistent access controls and data protection policies, and enhancing visibility and audit trails for effective threat detection and response. By adopting a robust approach to browser security, organizations can mitigate the risks associated with web-based activities, fortifying their defenses against sophisticated threats and ensuring the continuous protection of sensitive ePHI.

Challenges to HIPAA compliance with web browsers

Ensuring robust security measures for web browsing activities is essential for organizations handling ePHI to achieve HIPAA compliance. Traditional security approaches, while previously sufficient, are now inadequate due to the dynamic nature of web browsing and the inherent vulnerabilities of browsers, which introduce complexities that can undermine HIPAA compliance efforts.

HIPAA compliance requires a thorough examination of every aspect of the browsing environment, from user authentication to content inspection. Achieving this level of detail can be challenging, especially with a diverse user base and complex access requirements for healthcare applications. Balancing seamless access for healthcare professionals with strict security controls necessitates careful collaboration between IT and security teams.

Browser security and exploits

Historically, browsers lack the layered security architecture necessary for environments handling ePHI. Consumer browsers prioritize privacy controls, which do not meet the granular access controls and continuous monitoring demanded by HIPAA compliance. This necessitates a shift towards solutions with robust security features, including isolation and separation principles that safeguard ePHI in line with HIPAA regulations.

Endpoint browsers are vulnerable to exploits that can bypass security controls. Common vulnerabilities like plugins, extensions, and local storage mechanisms can serve as entry points for malicious actors, leading to malware infections, data exfiltration of ePHI, and compromised accounts. These vulnerabilities undermine HIPAA compliance efforts.

Malicious actors exploit these vulnerabilities using techniques like code obfuscation, HTML smuggling, and zero-day exploits, which target weaknesses in browser security mechanisms, evading detection and jeopardizing ePHI security. This demonstrates that even organizations with robust security frameworks are vulnerable to sophisticated attacks that exploit browser weaknesses.

Administration challenges

Securing and managing traditional browsers across a diverse user base with varying devices and locations presents significant challenges in maintaining consistent security policies and ensuring continuous HIPAA compliance. Managing updates, patches, and configurations for various browser versions increases the administrative burden. Addressing these challenges requires a holistic approach to browser security that extends beyond traditional methods.

Enhancing HIPAA compliance with Menlo Security

Organizations can leverage solutions like Menlo Security to enhance their HIPAA compliance posture and mitigate the risks associated with traditional browsers. Menlo Security’s browser isolation, advanced threat detection, and secure access controls strengthen defenses against ransomware, phishing attacks, and other sophisticated threats while enabling secure and compliant web access for healthcare professionals. By adopting Menlo Security's robust browser security solutions, organizations can ensure the continuous protection of sensitive ePHI and maintain HIPAA compliance.

The Menlo Security approach

Menlo Security offers a robust solution that addresses the challenges of securing electronic protected health information (ePHI) during web browsing activities, aligning with the core principles of HIPAA compliance. Central to this solution is the Menlo Secure Enterprise Browser, a cloud-driven enterprise browser utilizing isolation technology.

Isolation technology

The Menlo Secure Enterprise Browser isolates web content within a secure cloud environment, significantly reducing the attack surface on endpoints where ePHI might reside. This proactive approach mitigates threats before they reach user devices, decreasing reliance on traditional perimeter defenses and endpoint security measures that may have vulnerabilities. By isolating web content, Menlo Security helps organizations create a more secure browsing environment for accessing ePHI, thereby safeguarding sensitive data and enhancing their HIPAA compliance posture.

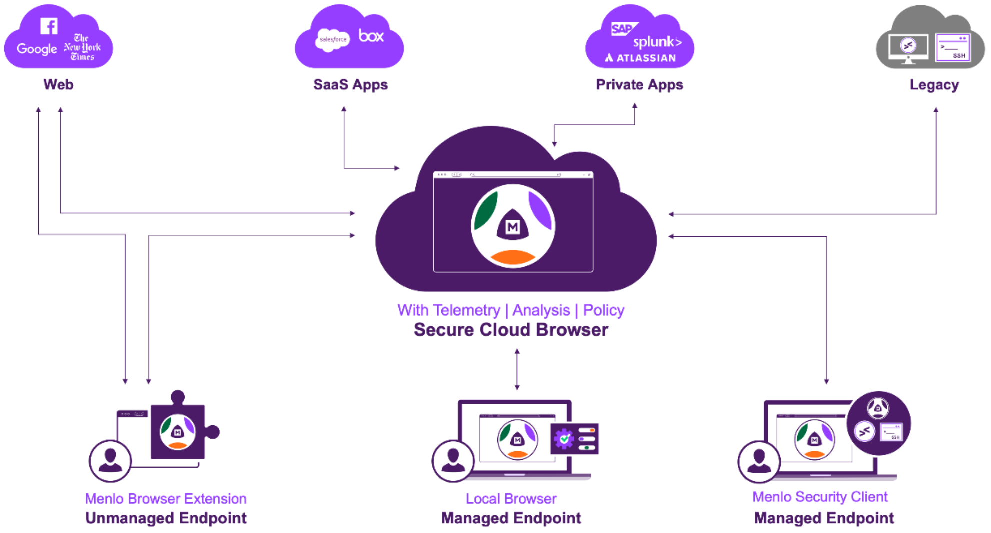


Figure 1: Menlo Secure Enterprise Browser solution architecture isolates threats from endpoints and protects applications

Cloud-native architecture

The cloud-native architecture of the Menlo Secure Enterprise Browser enables scalability and adaptability, allowing organizations to respond to evolving security threats in the healthcare landscape while maintaining user experience and operational efficiency.

Capabilities to support HIPAA compliance

The Menlo Secure Enterprise Browser encompasses capabilities to support HIPAA compliance.

Manage the browser

Menlo Security provides a unified management console for managing both local browsers and the Menlo Secure Enterprise Browser. This console streamlines policy configuration, reporting, and forensics, allowing organizations to leverage the enhanced security of the Menlo Secure Enterprise Browser while effectively managing existing browsers. This supports HIPAA principles of ongoing monitoring and access control.

Protect the user

By isolating web content and enforcing security measures off the endpoint, the Menlo Secure Enterprise Browser safeguards users from zero-hour phishing attacks, malicious files, and exploits targeting vulnerable software components on local devices. This approach mitigates the risk of unauthorized access to ePHI, adhering to HIPAA's principle of least privilege access.

Secure access and data

Menlo Security provides robust access controls and data security for software-as-a-service (SaaS) and enterprise or legacy healthcare applications. By enforcing access policies and protecting sensitive data, organizations can reduce the risk of unauthorized access and data breaches, supporting HIPAA's strict access control and data protection requirements.

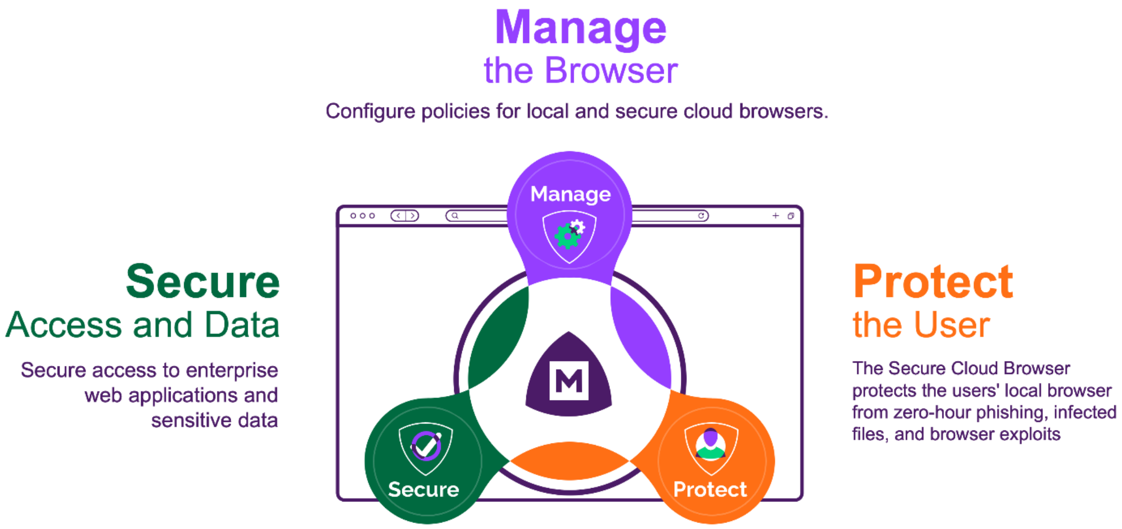

Manage
the Browser
Configure policies for local and secure cloud browsers.
Secure
Access and Data
Secure access to enterprise web applications and sensitive data
Manage
M
Secure
Protect
Protect
the User
The Secure Cloud Browser protects the users' local browser from zero-hour phishing, infected files, and browser exploits

Figure 2: Secure Enterprise Browser solution: key security capabilities

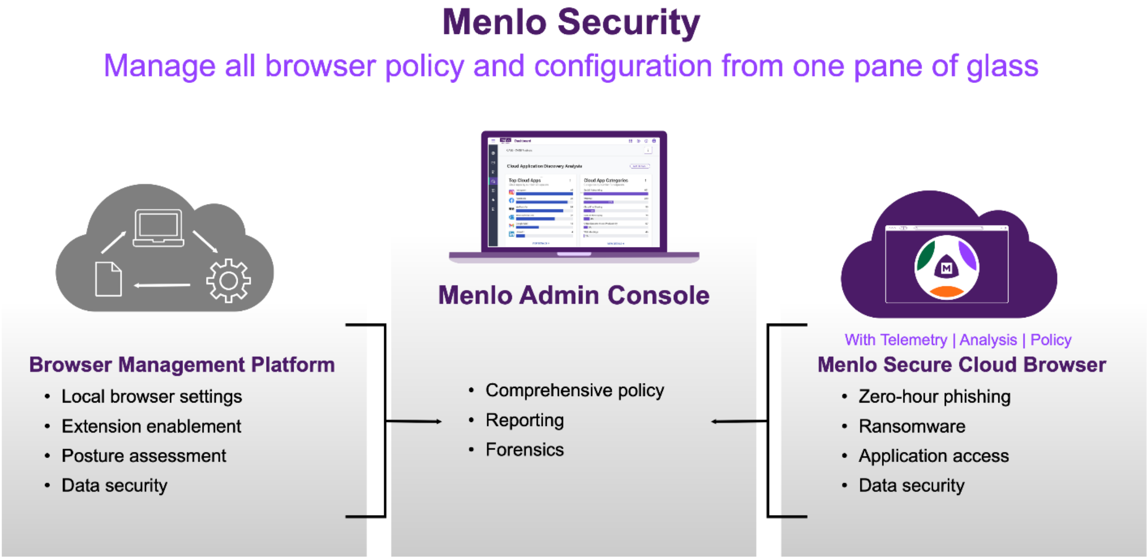
Comprehensive and unified management

The comprehensive and unified management console, combined with specialized security features and native integration options, enables organizations to minimize the attack surface on local browsers while providing enhanced security. This creates a more secure browsing environment for accessing ePHI, improving an organization's ability to achieve and maintain HIPAA compliance in a cloud-driven environment.

By leveraging Menlo Security’s advanced browser security solutions, organizations can ensure continuous protection of sensitive ePHI, mitigate sophisticated threats, and uphold stringent HIPAA compliance standards.

Menlo Secure Enterprise Browser solution

The Menlo Secure Enterprise Browser solution provides a unified solution for organizations to centrally manage and enforce security policies across both local and cloud-based browsing environments. This is achieved through a combination of technologies, including browser isolation, which ensures all web traffic is processed and rendered in a secure, isolated cloud environment, shielding user devices from potential threats.



Menlo Security

Manage all browser policy and configuration from one pane of glass

Browser Management Platform

- Local browser settings
- Extension enablement
- Posture assessment
- Data security

Menlo Admin Console

- Comprehensive policy
- Reporting
- Forensics

With Telemetry | Analysis | Policy

Menlo Secure Cloud Browser

- Zero-hour phishing
- Ransomware
- Application access
- Data security

Figure 3: Posture management subsystem – policy, reporting, and forensics

Secure cloud browsing

Browser isolation, an evolution of the Secure Cloud Browser, revolves around the principle of separating web browsing activities from the user's endpoint device. Secure Cloud Browsing, which builds upon these principles, offers more comprehensive protection than traditional Remote Browser Isolation (RBI). It ensures that potentially harmful web content never reaches the user's network or device. This is achieved by executing web browsing sessions within secure, cloud-based disposable virtual containers (DVCs) located remotely, away from the user's endpoint. When a user accesses a website, the content is rendered within the Secure Cloud Browser, and only safe rendering instructions are transmitted to the user's browser. This ensures that any malicious code or threats are contained within the isolated environment, protecting the user's device and network from compromise.

Adaptive clientless rendering (ACR) plays a critical role in this process, facilitating secure web content rendering without requiring downloads or additional plugins on the user's device. This minimizes potential attack vectors on user endpoints.

Adaptive clientless rendering

Modern browsers utilize a common framework to describe web page elements. During a typical browsing session, the content generates a document object model (DOM) and a corresponding rendering tree, instructing the browser on how to display the page for the user. Similarly, web sessions executed within the Menlo Secure Cloud Browser create their own Smart DOM and rendering tree information. ACR then optimizes and transmits this data to the user’s browser using Transport Layer Security (TLS). The user’s browser interprets this information, generating the web page view as if the content were running locally.

For a secure and transparent browsing experience, a trusted JavaScript function is delivered to the user's browser at the beginning of each session. This function establishes a secure communication channel with the Secure Cloud Browser using TLS encryption. The user's browser trusts the JavaScript function delivered by the solution. Trust is established through cryptographic verification mechanisms for authenticity and integrity of the function. The solution then trusts the user's browser to accurately render the received instructions and relay user interactions securely. This trust relationship enables the ACR system to select the most efficient encoding and transport method for different content types. Potentially dangerous content is executed securely within the isolated environment, while safe rendering instructions are delivered to the user's browser, as a high-fidelity, interactive experience. The user's browser receives non-executable, malwarefree content, protecting the user's device. Additionally, the ACR protocol securely relays user activity (keystrokes and mouse clicks) to the solution while preventing any malicious activity from reaching the user's device.

The solution leverages browser isolation as a core security principle to provide enhanced security and comprehensive protection against web-based threats, as well as additional benefits noted below:

- Browser agnostic: Browser isolation delivers accurate rendering that is agnostic to both the endpoint browser in use and the web features used by the page.
- Enhanced security: By isolating web browsing activities, browser isolation effectively mitigates the risk of malware infections, phishing attacks, and other web-based threats. Even if a user inadvertently accesses a malicious website, the isolation ensures that any malicious code is contained within the isolated environment, preventing it from reaching the user's device or network.
- Transparent user experience: Browser isolation provides a seamless browsing experience for users, without impact on performance or productivity. Users can access any website without concerns about potential threats, as all web content is rendered safely within an isolated environment.
- Reduced attack surface: Browser isolation significantly reduces the attack surface for cyber threats and minimizes the risk of successful attacks targeting users' endpoints or networks, enhancing overall security posture.
- Comprehensive protection: Browser isolation protects against a wide range of web-based threats, including zero-day exploits, drive-by downloads, and phishing attacks. It serves as a proactive defense mechanism that complements traditional security controls, providing an additional layer of protection against emerging threats.

Policy management

In addition to Secure Cloud Browsing capabilities, the Menlo Secure Enterprise Browser solution offers policy management features to minimize attack surfaces and enforce security principles within the organizational browser ecosystem. Through the Secure Cloud Browser, administrators define processing filters known as web policy rules to tailor browser isolation policies to organizational needs. The Menlo Secure Enterprise Browser solution's policy management features include:

- Granular policy configuration: Administrators have considerable control over web policy configuration, including blocking access to risky sites and customizing isolation rules based on organizational needs.
- Robust policy controls: Administrators can define policies to automatically isolate high-risk websites, such as uncategorized sites and vulnerable services, while maintaining productivity.
- Traffic steering agent: Administrators can leverage the traffic steering agent to route web traffic to the Secure Cloud Browser based on pre-defined rules and user groups and ensuring consistent policy enforcement and streamlined secure browsing experiences.

Web policy rules are enforced in a hierarchical manner and cover:

- Proxy auto configuration (PAC): Determining exemptions from isolation, allowing direct user access to specified sites.
- SSL decryption exemption: Specifying actions for Hypertext Transfer Protocol Secure (HTTPS) sessions, including the determination of SSL decryption necessity.
- Web application rules: Setting standards for non-browser and unsupported browser traffic, ensuring adherence to corporate browser protocols.
- Exceptions: Crafting policy rules to accommodate specific actions typically disallowed by global policy, such as granting users access to social networking sites.

- Threat and category rules: Exerting control over website access based on threat and category classifications, prioritizing the strictest policy enforcement.
- Exception management: Allowing administrators to create policy exceptions for specific domains, file downloads, document types, and file uploads.
- Time-based policy enforcement: Permitting policy enforcement based on predefined time criteria to allow nuanced control over acceptable use policies.

Secure Application Access

Secure Application Access (SAA), part of the Menlo Secure Enterprise Browser solution, enables healthcare organizations to grant secure access to critical applications while prioritizing compliance with HIPAA regulations. Employees, partners, and guests, for example, can access critical applications without the overhead of operational mechanisms and the security challenges used with traditional VPNs. HIPAA requires strict access control for ePHI. SAA adheres to this principle by strictly verifying every access request before granting least-privileged access to specific applications. This minimizes the attack surface and ensures users only have the permissions required for their designated tasks, reducing the potential impact of a security breach.

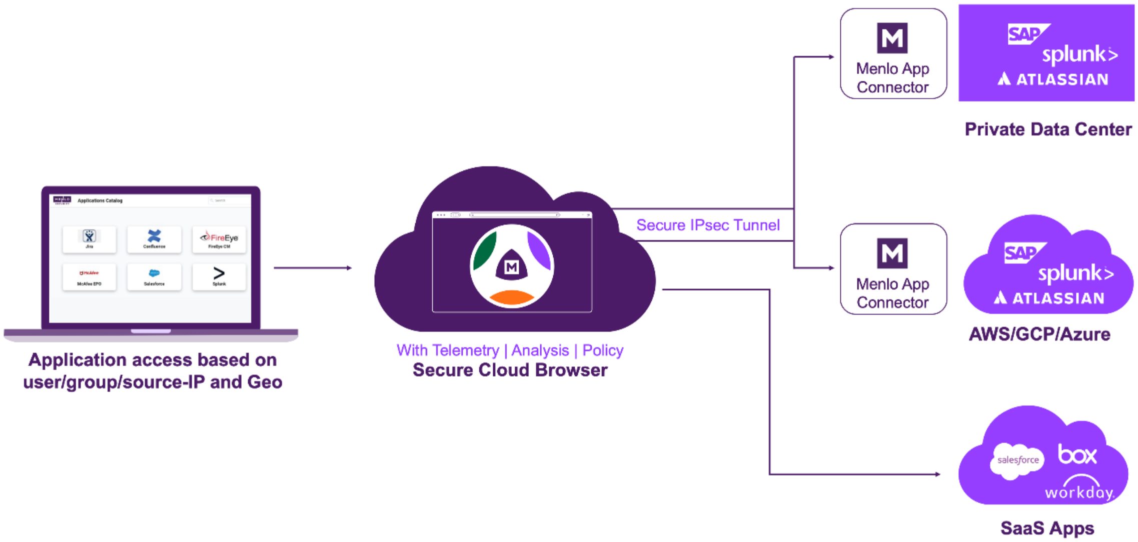


Figure 4: Access and security across application and user operating models

Secure Application Access enables organizations to make applications accessible to authorized users while they are hidden from the dangers of the public internet. Additionally, the Menlo Secure Enterprise Browser further isolates application rendering from user devices. This "air gap" prevents malware or compromised endpoints from reaching sensitive data within the application.

Secure Application Access enables administrators to define granular access policies based on user roles, groups, and specific application features. This helps ensure users are not granted unnecessary access, minimizing the risk of lateral movement within the network if a breach occurs. Streamlined user provisioning and policy configuration interfaces reduce the workload for security teams, while centralized administration provides a clear view of access controls and simplifies ongoing maintenance.

Secure Application Access offers comprehensive data-protection capabilities to safeguard sensitive ePHI. These include download/upload restrictions, data redaction for PII, watermarking, and copy/paste limitations. These controls help safeguard unauthorized data exfiltration across healthcare applications.

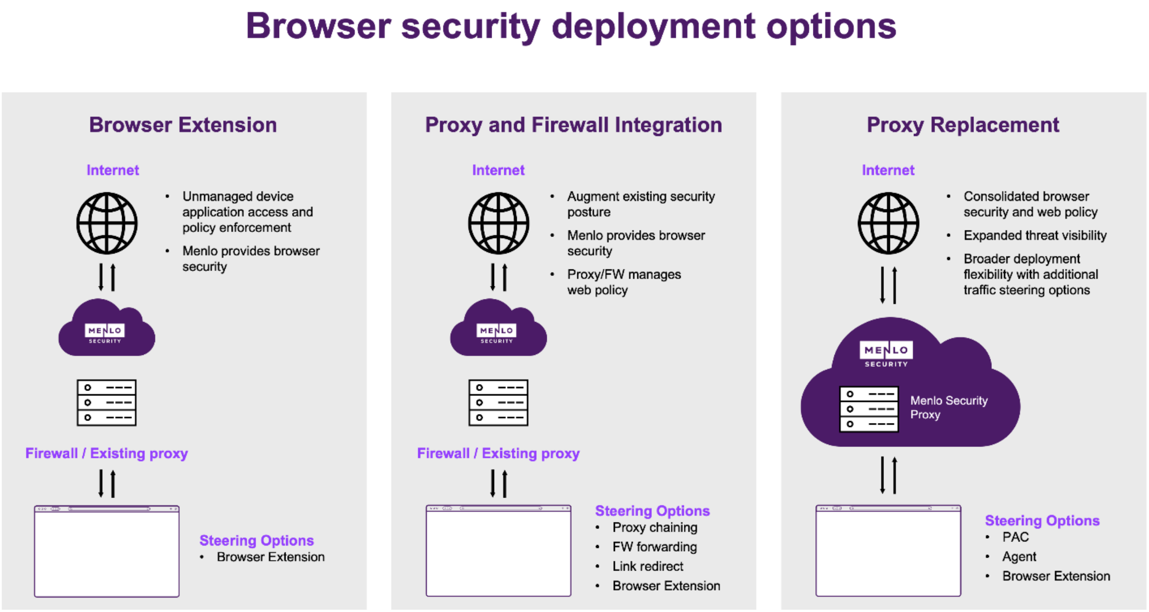

Browser security deployment options
Browser Extension
Internet
Unmanaged device application access and policy enforcement
Menlo provides browser security
Firewall / Existing proxy
Steering Options
Browser Extension
Proxy and Firewall Integration
Internet
Augment existing security posture
Menlo provides browser security
Proxy/FW manages web policy
Firewall / Existing proxy
Steering Options
Proxy chaining
FW forwarding
Link redirect
Browser Extension
Proxy Replacement
Internet
Consolidated browser security and web policy
Expanded threat visibility
Broader deployment flexibility with additional traffic steering options
Menlo Security Proxy
Steering Options
PAC
Agent
Browser Extension

Figure 5: Menlo Secure Enterprise Browser deployment flexibility and steering options

Secure Application Access caters to both private and SaaS healthcare applications through agentless and agent-based approaches. This adaptability allows organizations to integrate Secure Application Access into their existing infrastructure with minimal workflow disruption.

Key features of Secure Application Access

Key features of Secure Application Access include:

- Least-privileged access: Enforces granular permissions based on user roles and task requirements, minimizing attack surfaces and aligning with HIPAA access control mandates.
- Protection against internet threats: Shielding applications from the public internet mitigates risks like denial-of-service attacks, code injection, and Structured Query Language (SQL) injection attempts. This approach aligns with the principle of assuming untrusted external networks.
- Granular access and data security controls: Enforces download/upload restrictions, read-only/read-write permissions, watermarking, data redaction, and copy/paste limitations. This allows organizations to enforce strict access control and data protection, adhering to HIPAA requirements.
- Browser isolation: Leverages the Menlo Secure Enterprise Browser to isolate application rendering, shielding applications from content-based attacks and preventing malicious requests from reaching servers, even from compromised endpoints. This aligns with the principle of minimizing trust assumptions.

Benefits of Secure Application Access

Benefits of Secure Application Access include:

- Reduced attack surface: Hiding applications and implementing role-based access controls minimizes the attack surface and the risk of unauthorized access to ePHI.
- Protection against compromised endpoints: The Menlo Secure Enterprise Browser and sandboxing capabilities mitigate the risk of compromised endpoints accessing sensitive data.

- Enhanced data security for ePHI: Granular security controls and data protection measures safeguard the confidentiality and integrity of ePHI. These application-level controls support compliance with HIPAA regulations.
- Flexible deployment options: Supports diverse deployment options for both private and SaaS applications, allowing for zero-touch and agentless deployment for browser-based applications and agent-based deployment for non-browser applications. This flexibility caters to evolving security needs and facilitates infrastructure scaling without compromising security.
- Simplified management: Easy-to-manage policies and streamlined user provisioning/offboarding processes simplify access control management within a HIPAA-compliant framework. Providing tools for policy configuration and monitoring enables organizations to maintain robust security with minimal operational overhead.

Capabilities of Secure Application Access

Capabilities of Secure Application Access include:

- Granular access policies: Define precise access rules based on user roles, groups, and application features to enforce strict security measures.
- Intranet security: Secure access for contractors with granular controls based on user attributes and network parameters, ensuring compliance and operational security.
- Device posture assessment: Direct access through native clients enables assessment of device security posture before granting access to sensitive applications.
- Browser-based application isolation: Renders web applications within Menlo Secure Enterprise Browser, protecting applications from malicious activities originating from user devices.
- Threat detection and prevention: Utilizes sandboxing and antivirus scanning to detect and block malware attempting to exploit application vulnerabilities.
- DLP controls: Implements download/upload restrictions, redaction, watermarking, and copy/paste limitations to prevent unauthorized data exfiltration.

Aligning with HIPAA principles

Secure Application Access aligns with core HIPAA principles by ensuring:

- Least-privileged access: Restricts access to ePHI based on user roles and tasks, minimizing exposure and ensuring data confidentiality.
- Protection against internet threats: Shields healthcare applications from external threats, maintaining operational continuity and data integrity.
- Granular access controls: Enforces detailed access policies to protect sensitive ePHI, mitigating risks associated with unauthorized access and data breaches.
- Browser isolation for enhanced security: Utilizes browser isolation to minimize trust assumptions and prevent malicious activities from compromising application security.

By implementing Menlo Secure Application Access, healthcare organizations can enhance their security posture, achieve compliance with HIPAA regulations, and ensure secure access to critical applications without compromising operational efficiency.

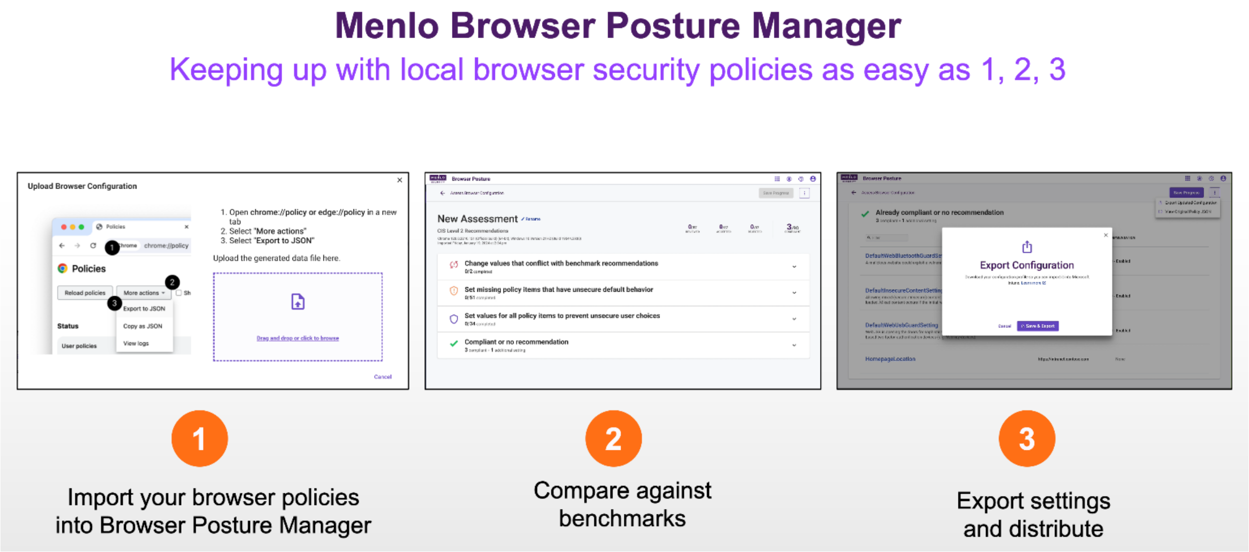
Browser Posture Manager

Browser Posture Manager serves to enhance browser security and shield organizations from web-based threats. Browser Posture Manager works to maintain the integrity of browser configurations, thus protecting against malware, phishing attacks, and breaches originating from compromised browsers.

By providing a centralized solution for managing and enforcing security policies across all web browsers, Browser Posture Manager simplifies the administration of browser security. This helps ensure consistent protection and adherence to compliance standards. Moreover, Browser Posture Manager allows organizations to define and enforce specific security policies based on user role, device type, and threat intelligence. This tailored approach helps mitigate the risks associated with web-based threats.

Additionally, the Browser Posture Manager takes proactive measures to strengthen browser configurations, such as automatically applying security patches and restricting insecure features to reduce vulnerabilities and enhance resilience against exploitation attempts. The Browser Posture Manager integrates real-time threat intelligence feeds to bolster its ability to detect and mitigate potential risks. The Browser Posture Manager offers:

- Benchmarked policies: Browser Posture Manager employs industry-recognized benchmarked policies as a standard for evaluating browser security configurations. By continuously analyzing and monitoring these policies, security controls are based on strict policy enforcement rather than implicit trust.
- Continuous validation: Browser Posture Manager continuously validates browser configurations against benchmarked policies. This proactive approach enables organizations to identify and remediate security gaps in real-time.
- Management of Chrome and Edge policies: Browser Posture Manager supports the management of policies for both Google Chrome and Microsoft Edge browsers.


Menlo Browser Posture Manager

Keeping up with local browser security policies as easy as 1, 2, 3

Upload Browser Configuration

1. Open chrome://policy or edge://policy in a new tab
2. Select "More actions"
3. Select "Export to JSON"

Upload the generated data file here.

New Assessment

CIS Level 2 Recommendations

Change values that conflict with benchmark recommendations 0/2 completed

Set missing policy items that have unsecure default behavior 0/51 completed

Set values for all policy items to prevent unsecure user choices 0/34 completed

Compliant or no recommendation 3 compliant · 1 additional setting

Already compliant or no recommendation 3 compliant · 1 additional setting

Export Configuration

1 Import your browser policies into Browser Posture Manager

2 Compare against benchmarks

3 Export settings and distribute

Figure 6: Centralized management and policy enforcement for browsers

Browser Posture Manager offers comprehensive visibility into browser usage and compliance posture through centralized dashboards and reporting tools, including Browser Forensics. This enables organizations to monitor and analyze their security stance effectively.

Document and archive isolation

The Secure Enterprise Browser document isolation feature takes a layered approach to safely viewing documents while minimizing risk to devices or networks. Documents downloaded from the web are opened in an isolated space where the file is examined. Any active content, which could potentially be malicious, is neutralized. The result is that the document is safely rendered in a secure document viewer. The clean version is then presented for viewing. Depending on the organization's defined policies, users have the option to download either the original document (once it has been scanned by multiple content inspection engines and determined "clean") or a safe version that retains original formatting.

In cases where password-protected documents are encountered, the Menlo Secure Enterprise Browser can handle user-provided passwords within the isolated environment. This ensures that passwords are never transmitted to the user's device or network unencrypted, further enhancing security.

The Menlo Secure Enterprise Browser solution also allows the establishment of granular access policies to restrict document access based on file type and individual user, ensuring that only authorized personnel can access sensitive documents and further strengthening security posture.

The solution's document isolation allows a wide range of document types to be securely viewed within its web-based viewer, as well as permitting the viewing of archive files (even within nested archives) and the ability to allow safe access to encrypted archives.

Firewall-as-a-Service

The Menlo Secure Enterprise Browser Firewall-as-a-service (FWaaS) solution offers cloud-based network security solutions to protect organizations from cyber threats. It enables administrators to enforce network access control policies, monitor traffic flows, and detect and block malicious activities targeting distributed and mobile users to safeguard remote infrastructure and assets. FWaaS reduces the need for traditional, on-premise firewalls and can reduce deployment and management processes. By leveraging cloud-based infrastructure, organizations can achieve agility and scalability while preserving application performance for authorized traffic.

FWaaS allows administrators to create rules governing non-web traffic, such as File Transfer Protocol (FTP), Secure Shell Protocol (SSH), and Domain Name System (DNS). This capability allows consistent policy enforcement, control and visibility over network traffic, and mitigation of risks including:

- Unauthorized access: FWaaS enforces strict access controls and scrutinizes outbound traffic to prevent unauthorized communication with malicious entities.
- Data exfiltration: By regulating non-web traffic and implementing stringent policies, FWaaS helps prevent data exfiltration attempts, safeguarding sensitive information.
- Lateral movement: FWaaS thwarts lateral movement within the network by monitoring and controlling outbound traffic, limiting the spread of cyber threats.

FWaaS operates on the principle of least privilege access, enabling administrators to establish precise rules that dictate users' specific actions on outbound connections. Granular access controls minimize the damage caused by excessive permissions or compromised accounts, reducing the attack surface, and enhancing security posture. Organizations gain granular control over outbound connections, defining rules based on criteria such as source and destination IP addresses, ports, and protocols.

Key functionality and benefits of FWaaS include:

- Continuous verification and monitoring: FWaaS continuously verifies the trustworthiness of outbound traffic in real-time, adapting network security policies based on threat intelligence and contextual information.
- Microsegmentation: FWaaS facilitates network segmentation, isolating critical resources and user groups to limit lateral movement capabilities of attackers. Even if a single device is compromised, segmentation contains potential breaches, enhancing overall security resilience.
- Object management and customizable services: FWaaS allows rule creation and policy enforcement through reusable IP address objects, helping ensure consistent access controls. Additionally, it allows customization of services for specific organizational needs and regulatory requirements.
- Logging and user/group targeting: FWaaS provides continuous visibility into network activity through logging and monitoring capabilities. Security teams can identify suspicious behavior and potential security incidents in real-time, applying granular access controls to specific users or groups to minimize the risk of insider threats.
- Isolation of web traffic: Web traffic is routed through the Menlo Cloud Proxy for inspection, isolating potential threats within a secure environment. This prevents malicious content from reaching end-user devices, reducing the risk of malware infections and data breaches.
- Protection against lateral movement: FWaaS limits an attacker's ability to move laterally within the network by enforcing network segmentation.
- Centralized policy management: Centralized policy management ensures consistent enforcement across locations and users, eliminating policy gaps and enhancing security governance.

FWaaS dashboard

The FWaaS dashboard offers real-time insights into network traffic patterns and potential security risks. Security teams can identify unauthorized outbound traffic, monitor network health, and continuously improve security policies based on observed traffic patterns, helping mitigate emerging threats.

Key dashboard insights include:

- Blocked traffic: Provides insights into potential policy violations or unauthorized outbound attempts, helping identify and stop unauthorized activity.
- Top protocols and actions: Highlights potential risks associated with specific protocols or actions, enabling security teams to prioritize mitigation efforts and strengthen enforcement.
- Top sources and destinations: Helps identify unusual network communication patterns that might indicate compromised devices or malicious actors, aiding in threat detection and response.

Last-Mile Data Protection

Last-Mile Data Protection extends DLP capabilities beyond the network perimeter and to the user's endpoint, helping ensure sensitive information remains secure even when using the latest AI-powered tools. It strengthens security posture by safeguarding sensitive information from both accidental and malicious exfiltration attempts and provides granular control over user data to enforce consistent security policies, including control over copy/paste functionality.

Network separation

Last-Mile Data Protection focuses on preventing data exfiltration at the final stage of transmission. It creates an “air gap” between users and the internet, facilitating inspection of file uploads and user input. This isolation-driven approach enables comprehensive monitoring and control over data transmission, helping ensure that sensitive information remains confidential and inaccessible to unauthorized entities. Last-Mile Data Protection also integrates with existing DLP solutions, both on-premises and cloud-based, for a layered defense strategy, enhancing data protection and compliance.

User traffic undergoes deep inspection for potential leaks as it travels through the solution. Globally enforced policies identify and potentially block sensitive data uploads or submissions in web forms. DLP controls help ensure proactive threat mitigation, compliance management, and user awareness:

- Global dictionaries: Pre-configured dictionaries recognize various sensitive data types, streamlining policy creation and reducing configuration complexity.
- Customizable detection: Tailors DLP rules to identify organization-specific sensitive data, ensuring a tailored approach to data protection.
- Context-aware rules: Considers context to minimize false positives and enable accurate detection of suspicious activities.
- Granular visibility: Offers visibility into user activities and file uploads, enabling organizations to detect and prevent potential data breaches in real-time.
- Actionable insights: Detailed logs and alerts provide visibility into potential leaks, guiding remediation efforts and enhancing security posture.
- User education: Customizable notifications educate users about potential policy violations and best practices for data handling.
- Detailed logging and reporting: Permits insights into DLP violations through comprehensive logs and reports, enabling proactive threat mitigation and compliance management.

Watermarking

The Menlo Secure Enterprise Browser solution’s watermarking feature augments its Last-Mile Data Protection capabilities. Watermarking enables organizations to embed tamper-proof watermarks on isolated web pages and safe document downloads accessed through the solution. This is because the watermarks are applied within the Secure Cloud Browser, whereas conventional browser watermarking can typically be manipulated on the local device. The solution allows customization of watermark appearance and content. Organizations can define the watermark text, its position within the document, and its visibility (visible or invisible). This flexibility ensures watermarks are both informative and unobtrusive, maintaining user experience while enhancing data security.

Watermarking strengthens DLP strategy through:

- Deterrence: Visible watermarks serve as a visual deterrent, reminding users that downloaded documents or screenshots contain traceable information. This can discourage unauthorized sharing of sensitive content.
- Attribution: In the event of a data breach, watermarks can help identify the source of the leak by embedding user or device-specific information within the watermark. This facilitates faster investigation and potential disciplinary actions.
- Authentication: Watermarks can be used for internal verification purposes. By embedding department names or project codes, organizations can verify the legitimacy of downloaded documents and identify potential misuse of sensitive information.

Watermarking integrates with existing Last-Mile Data Protection functionality. Watermarks can be applied in conjunction with content inspection, policy enforcement, and user behavior monitoring to create a multi-layered approach to DLP. This feature strengthens data security posture and enables organizations to manage sensitive information more effectively.

DLP rules for file downloads

In the context of Secure Application Access, the solution provides additional control over sensitive data through its ability to apply DLP rules to file downloads. This enables administrators to define granular download restrictions based on file type, content, or application source. DLP rules for file downloads can enhance data security through:

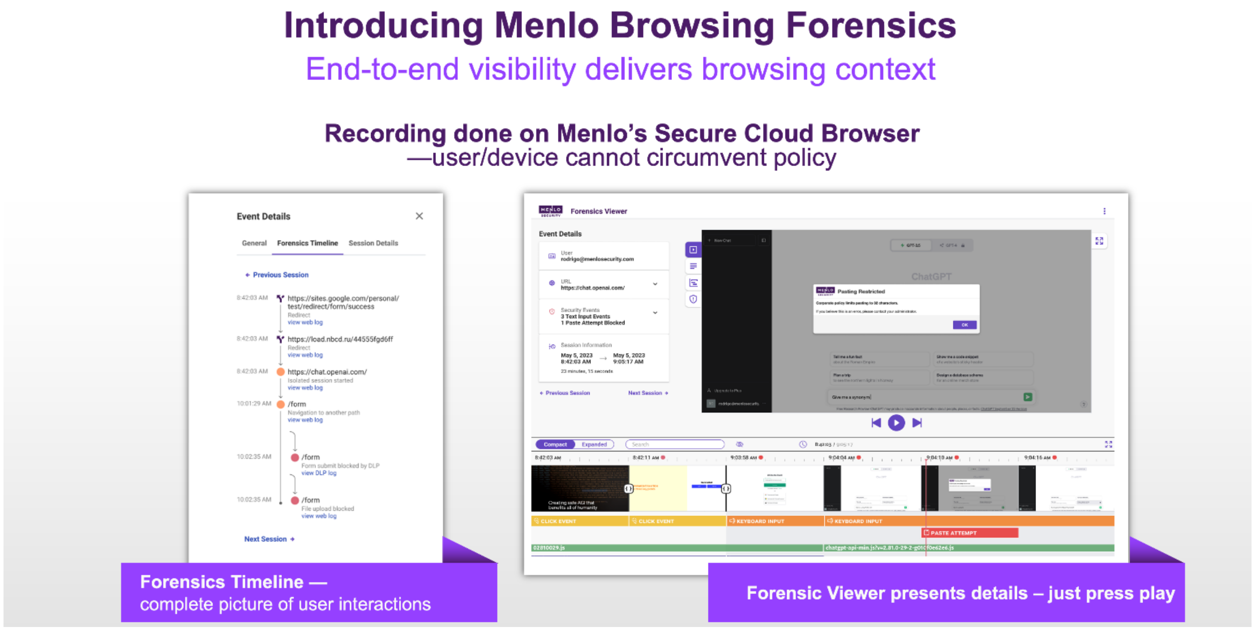
- Comprehensive download control: Administrators can create rules to block downloads of specific file types (e.g., executables, compressed archives) or files containing sensitive keywords or patterns. This helps prevent unauthorized downloads of potentially malicious or confidential information.
- Application-level enforcement: DLP rules can be applied not only to web downloads but also to downloads from CASB-integrated applications and even specific internal applications to ensure consistent data protection across various access points.
- Reduced risk of data exfiltration: By restricting downloads based on predefined rules, organizations can significantly reduce the risk of sensitive data being exfiltrated from the organization through unauthorized file transfers.

DLP rules for downloads integrate with existing Last-Mile Data Protection functionality. Administrators can leverage content inspection, user behavior monitoring, and other features, alongside download restrictions, to create a comprehensive DLP strategy. Additionally, the Menlo Secure Enterprise Browser solution offers flexibility in defining rule parameters, allowing for granular control tailored to specific organizational needs.

Last-Mile Data Protection offers broad visibility into user browser sessions, thorough data inspection, and the reduction of the blind spots often present in traditional DLP solutions. A vast library of sensitive data categories is recognized for compliance with regional regulations, addressing data privacy concerns and facilitating adherence to data protection standards like GDPR, PCI DSS, and HIPAA.

Browser Forensics

Browsing Forensics provides visibility into browser-based security incidents, facilitates forensic investigations, and enhances threat analysis capabilities. By capturing detailed telemetry data, including web requests, file downloads, and browser activities, Browsing Forensics enables security analysts to reconstruct the sequence of events leading up to a security incident, identify the attack vector, determine the extent of the compromise, and implement proactive security measures to mitigate future risks.



Introducing Menlo Browsing Forensics

End-to-end visibility delivers browsing context

Recording done on Menlo's Secure Cloud Browser
—user/device cannot circumvent policy

Event Details

General | Forensics Timeline | Session Details

← Previous Session

8:42:03 AM https://sites.google.com/personal/test/redirect/form/success
Redirect
view web log

8:42:03 AM https://load.nbcd.ru/44555fgd6ff
Redirect
view web log

8:42:03 AM https://chat.openai.com/
Isolated session started
view web log

10:01:29 AM /form
Navigation to another path
view web log

10:02:35 AM /form
Form submit blocked by DLP
view DLP log

10:02:35 AM /form
File upload blocked
view web log

Next Session →

Forensics Timeline —
complete picture of user interactions

Forensics Viewer

Event Details

User
rodrigo@menlosecurity.com

URL
https://chat.openai.com/

Security Events
3 Text Input Events
1 Paste Attempt Blocked

Session Information
May 5, 2023 8:42:03 AM → May 5, 2023 9:05:17 AM
23 minutes, 15 seconds

← Previous Session | Next Session →

Pasting Restricted
Corporate policy limits pasting to 32 characters.
If you believe this is an error, please contact your administrator.
OK

Forensic Viewer presents details – just press play

Figure 7: Browser Forensics features

Forensic evidence related to browser-based security incidents is collected and preserved. By capturing forensic artifacts such as Hypertext Transfer Protocol (HTTP) headers, browser cookies, and user session data, Browser Forensics enables security teams to maintain a chain of custody for digital evidence, adhere to legal and regulatory requirements, and support law enforcement investigations when necessary.

Integration with threat intelligence feeds and security analytics platforms enrich forensic data with contextual information about known threats, indicators of compromise (IOCs), and attack patterns. Browser Forensics correlates forensic data with external threat intelligence sources to enhance the accuracy and relevance of threat detection, enabling security teams to identify emerging threats and take proactive countermeasures to defend against them.

Offered analysis and visualization tools help security teams interpret and analyze forensic data. By leveraging interactive dashboards, timeline views, and search capabilities, Browser Forensics enables security analysts to identify anomalous behavior, detect patterns of malicious activity, and uncover hidden threats within browser-related telemetry data. Browser Forensics includes the following capabilities:

- Policy-defined session recording: Browser Forensics records browser sessions based on policy triggers, such as advanced threat detections or user access to private or sensitive applications. This approach captures potentially suspicious activities and provides organizations with visibility into browser-based threats. Browser Forensics captures activity based on predefined security policies, helping minimize unnecessary data collection.
- Secure storage and access controls: For data privacy, recordings are stored in designated secure cloud storage (e.g., Amazon Web Services [AWS] or Microsoft Azure).
- No user browsing history tracking: The system does not maintain a record of overall user browsing history, protecting user privacy while providing insights for security investigations.
- Forensics logs: Each recorded session includes a detailed forensics log entry, containing critical event summaries and links to associated recordings. Browser Forensics consolidates traditional session details with browser-specific insights, such as DLP violations or copy/paste actions, enabling security teams to conduct investigations and make decisions.

- Enhancing threat detection: Browser Forensics provides visual evidence to support security investigations, enabling analysts to identify malicious intent or accidental exposure of sensitive data.
- Rich content viewer: The Browser Forensics Viewer presents a comprehensive view of the recorded session, allowing analysts to reach substantiated conclusions and facilitating decision-making and incident resolution.

Continuous monitoring and alerting capabilities enable detection and response to suspicious browser activities in real-time. By configuring custom alerting rules based on predefined thresholds, behavioral patterns, or IOC matches, Browser Forensics enables security teams to receive timely notifications of potential security incidents, investigate them promptly, and mitigate risks before they escalate.

HEAT Shield capabilities

The browser is the primary entry point for internet borne attacks, resulting in data exfiltration, credential theft, and account takeover. Traditional tools often fail to stop these attacks, because they rely on signature and or pattern matching of known attacks to detect and block such threats. Additionally, they lack visibility into specific browser signals. Security teams need a solution that provides end-to-end visibility and that is as dynamic as the threats targeting users. An emerging industry term, HEAT refers to Highly Evasive, Adaptive Threats. Menlo Security HEAT Shield and HEAT Visibility work together to defend against evasive threats and provide comprehensive threat intelligence.

HEAT Shield

HEAT Shield offers proactive protection against zero-hour phishing attacks. Its threat prevention technologies and policy controls enable security teams to proactively prevent phishing threats in real-time, reducing the risk of data breaches and financial losses.

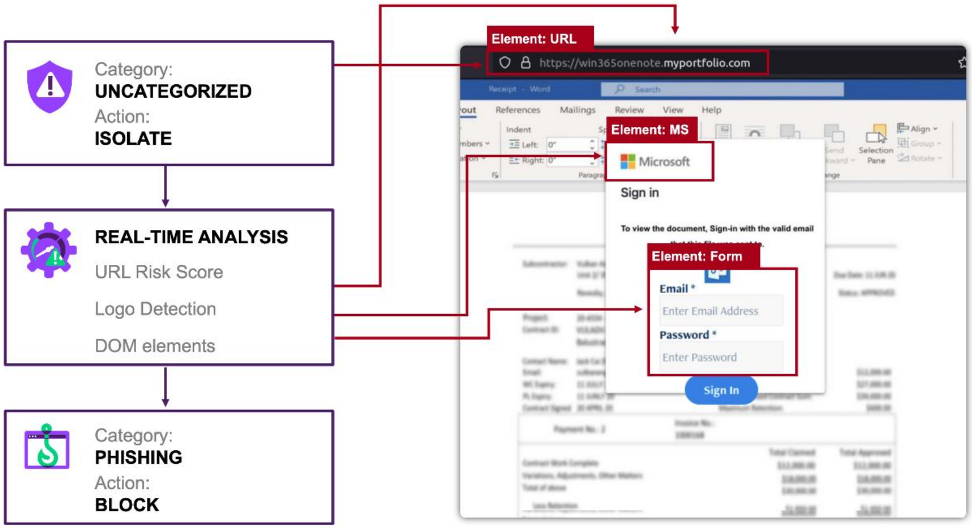


Figure 8: Real-time protection against sophisticated, evasive phishing attacks and threats

HEAT Shield dynamically analyzes each web session, examining both what the user sees and cannot see, applying artificial intelligence (AI) / machine learning (ML) detection models within the context of the Secure Cloud Browser, to detect and block previously unseen phishing sites that attempt to steal user credentials and sensitive data.

HEAT Shield combines:

- Computer vision applied as real-time object detection to identify brand logos on web pages - including frequently impersonated brands like Microsoft and Adobe.

- An ML-weighted risk score model that analyzes the full URL path – assigning each URL ‘feature’ a score which is then combined into a final value determining its maliciousness.
- DOM Analyzer - HEAT Shield also examines what the user cannot see, the underlying DOM Layers from which the page is constructed, including JavaScript and CSS resources.

Security policies are dynamically enforced based on real-time analysis and contextual information such as user roles and organizational risk tolerance. HEAT Shield determines appropriate response actions, such as blocking access to malicious websites or forcing web sessions into read-only mode. Enforcement actions include:

- Blocking malicious websites in real-time.
- Read-only mode, which prevents users from entering sensitive information while still allowing them to view the content.
- Log access attempts for further investigation.

HEAT Shield minimizes trust in web content and dynamically assesses the risk associated with accessed URLs. This reduces the likelihood of successful phishing attacks and strengthens defenses against cyber threats.

HEAT Shield builds on the existing Secure Cloud Browser, providing seamless deployment and management, supporting diverse browser environments without the need for additional endpoint software. With globally available coverage and scalability, organizations can deploy HEAT Shield across distributed environments, helping ensure consistent protection against evolving threats.

Additionally, seamless integration with the Browser Forensics capability enables security teams to quickly investigate attempted phishing attacks. All session data / browser artifacts are captured including screenshots, keyboard inputs, page resources, HTTP headers, cookies, and user session data.

HEAT Visibility

HEAT Visibility equips organizations with threat detection capabilities and actionable intelligence. By analyzing web telemetry and employing advanced algorithms, HEAT Visibility helps security teams identify elusive threats in their environment, receive timely alerts, and gain deeper insights into malicious activity, strengthening security posture and resilience against cyber threats.

HEAT Visibility: Evasive Threat Intel for Security Teams

Menlo Security identifies evasive threats targeting YOUR organization

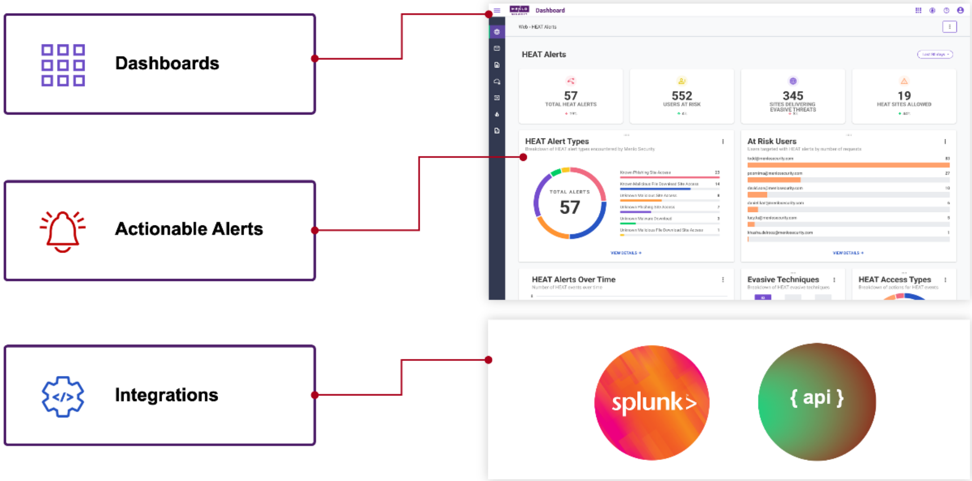

Dashboards
Actionable Alerts
Integrations
Dashboard
Web › HEAT Alerts
HEAT Alerts
57
TOTAL HEAT ALERTS
552
USERS AT RISK
345
SITES DELIVERING EVASIVE THREATS
19
HEAT SITES ALLOWED
HEAT Alert Types
Breakdown of HEAT alert types encountered by Menlo Security
TOTAL ALERTS
57
Known Phishing Site Access 23
Known Malicious File Download Site Access 14
Unknown Malicious Site Access 8
Unknown Phishing Site Access 7
Unknown Malware Download 3
Unknown Malicious File Download Site Access 1
VIEW DETAILS
At Risk Users
Users targeted with HEAT alerts by number of requests
VIEW DETAILS
HEAT Alerts Over Time
Number of HEAT events over time
Evasive Techniques
Breakdown of HEAT evasive techniques
HEAT Access Types
Breakdown of actions for HEAT events
splunk>
{ api }

Figure 9: Proactive threat detection with evasive threat intelligence

By scrutinizing web traffic patterns, user behaviors, and access trends, it identifies anomalous activities indicative of potential security incidents or malicious behavior, enabling proactive threat detection and response.

HEAT Visibility employs advanced algorithms and behavioral analysis techniques to detect various evasive tactics employed by cybercriminals, ranging from stealthy malware infections to sophisticated phishing campaigns. By analyzing telemetry for signs of malicious activity, it helps security teams stay ahead of emerging threats and effectively mitigate risks.

Upon detecting suspicious activities or security events, HEAT Visibility generates actionable alerts, providing security teams with timely notifications and insights into potential threats. By prioritizing alerts based on severity, impact, and relevance to organizational risk, HEAT Visibility facilitates timely and informed decision-making, enabling proactive threat mitigation and incident response.

HEAT Visibility allows security administrators to define policy-driven response actions based on detected threats or suspicious behaviors. By aligning alert types with predefined policies, such as isolation, blocking, or further investigation, it ensures consistent enforcement of security controls and adherence to organizational policies.

Through comprehensive threat intelligence dashboards and customizable queries, HEAT Visibility provides security teams with insights into threat activity and attack trends. By analyzing historical data, correlating events, and identifying patterns of malicious behavior, it provides security teams with the knowledge needed to understand evolving threats and make informed decisions to protect critical assets.

HEAT Visibility integrates with existing security information and event management (SIEM) and security orchestration, automation, and response (SOAR) tools, enabling a holistic security posture as well.

Secure Web Gateway

Menlo offers Secure Web Gateway (SWG) capabilities that merge advanced threat detection capabilities with precise policy controls to help ensure users and devices navigate the web safely, shielded from malicious content, phishing attacks, and data breaches and fostering a secure and productive browsing environment.

Employing a multi-layered defense approach, SWG integrates URL filtering, content inspection, and threat intelligence to combat both known and unknown web threats. Through real-time analysis of web traffic and utilization of threat intelligence feeds, SWG identifies and blocks malicious URLs, phishing sites, malware downloads, and other security risks.

SWG allows organizations to establish granular policies governing web access and to enforce security controls tailored to user roles, groups, and content categories. Administrators can configure policies to restrict access to inappropriate or high-risk websites, manage file transfers, and uphold encryption standards such as AES-256 for safeguarding sensitive data during transit, to help ensure compliance with regulatory mandates and internal security protocols.

SWG enhances its threat detection and response capabilities by drawing from multiple threat intelligence sources, including commercial vendors, open-source repositories, and proprietary research. By correlating threat indicators with real-time web traffic, SWG identifies emerging threats, zero-day vulnerabilities, and advanced persistent threats (APTs) to enable proactive threat mitigation and incident response strategies.

Built on a cloud-native architecture, SWG offers organizations the ability to scale their web security infrastructure dynamically and to adapt to evolving security needs. SWG leverages cloud-based deployment models to deliver flexibility, scalability, and resilience for protection against web-based threats across dispersed environments and remote users.

Key features of SWG include:

- Centralized proxy configuration: Proxy configuration is managed via Active Directory (AD). Group Policy Objects enable organization-wide configuration for consistent settings and minimal administrative overhead.
- Proxy chaining: Allows organizations to selectively forward requests through the solution. User validation can occur in anonymous or authenticated mode to accommodate different deployment scenarios.
- Fixed egress IP routing: Organizations can control the source IP address for traffic originating from selected services, providing a known source IP address for authentication purposes, ensure compliance with access requirements and maintain compatibility with protected web services
- Mobile device web steering: Multiple methods for steering connections from mobile devices are offered, including URL prepend, email transformed URLs, proxy chaining, and Mobile Device Management (MDM)-managed PAC settings to enable organizations to enforce consistent security policies across all devices and maintain a unified security posture.
- Menlo Secure Enterprise Browser: Isolates web content execution within the cloud, minimizing the attack surface on user devices and reducing the potential impact of vulnerabilities.
- ACR: Delivers only safe, rendered content to user devices, eliminating the risk of malicious code execution.
- Threat rule and category mapping: Provides granular control over web traffic access based on website characteristics and user roles.
- Automatic policy enforcement: Enforces security policies in real-time, blocking access to malicious websites and content.

Traffic steering options

Menlo Security offers a variety of access methods that enable healthcare organizations to grant secure and compliant user access to ePHI and corporate resources while accommodating diverse connectivity needs and security postures.

Menlo Security Client

The Menlo Security Client (MSC) is a lightweight application for user devices that enforces consistent security policies for all traffic, regardless of location. This is essential for HIPAA compliance, as it ensures that ePHI is protected even when users access data from public Wi-Fi networks or while roaming.

Key features of MSC supporting HIPAA compliance include:

- Captive portal handling: The MSC automatically handles captive portals encountered in public Wi-Fi environments like airports or hotels. This eliminates the need for manual logins, potentially exposing ePHI, and streamlines the user experience.
- Dynamic proxy settings: The MSC automatically adjusts proxy settings based on location awareness. This ensures that user traffic adheres to appropriate security policies within the corporate network or elsewhere, safeguarding ePHI data.
- Encrypted tunneling: The MSC creates an encrypted tunnel between the user device and the Menlo cloud, ensuring data privacy and integrity during transit. This mitigates the risk of unauthorized access to ePHI, especially on public networks.
- Non-web traffic monitoring: The solution allows administrators to monitor and enforce security policies for all traffic types, including non-web traffic. This is particularly relevant for healthcare organizations, as it enables monitoring of potential security risks associated with roaming users who might bypass traditional on-premises firewalls, potentially carrying ePHI data.
- Granular policy enforcement: User identification within internet traffic enables administrators to define granular security policies based on user attributes like role, department, or location. This allows for a more nuanced approach to access control, safeguarding ePHI based on specific user permissions.
- Centralized management and tamper protection: The MSC offers centralized configuration through the Menlo admin portal for simplified policy management. Additionally, tamper protection mechanisms ensure that the intended security posture is maintained, preventing unauthorized modifications that could compromise ePHI.

Secure access for unmanaged devices: clientless web access and browser extension

For scenarios where deploying software agents on user devices might be impractical, Menlo Security provides alternative access methods suitable for HIPAA compliance:

- Clientless web portal: This approach offers a zero-touch deployment, eliminating the need for installing software on user devices or managing certificates. Users simply log in to a secure portal and access a list of provisioned applications. This facilitates secure access to ePHI for employees, partners, and authorized users working from unmanaged devices, as long as they can access the portal.
- Browser extension: A lightweight browser extension provides functionalities similar to the clientless web portal. Users can seamlessly access applications directly within their web browser, even outside the dedicated portal. This offers additional flexibility for accessing ePHI while maintaining a secure connection.

Menlo Connect

Menlo Connect is a lightweight application that ensures secure endpoint connectivity for remote workers accessing healthcare resources. It manages system proxy settings, handles captive portals, and restricts unauthorized network access changes through the use of a PAC file. This helps to safeguard ePHI data on remote endpoints. Additionally, Menlo Connect offers centralized control and configuration capabilities for administrators, enabling consistent policy enforcement across the organization.

Email isolation dashboard

Email remains a significant vector for cyber threats, including phishing, malware distribution, and credential theft. Email isolation complements browser isolation to provide organizations with comprehensive protection against such threats. While browser isolation focuses on securing browsing activities, email isolation extends these principles to safeguard email communications.

Email isolation works by isolating links and attachments within a secure environment, preventing malicious code from reaching end users' devices and minimizing the risk of cyber threats infiltrating organizational networks or compromising user data. By rendering email content in read-only mode or blocking access to high-risk links, organizations can prevent inadvertent data breaches and maintain a secure communication environment. Email isolation effectively addresses various threats posed by malicious email links, including:

- Malware infection: Prevents malicious code from compromising users' systems when accessing linked sites via email.
- Credential and data loss: Users are safeguarded against inadvertently providing sensitive information to illegitimate sites, reducing the risk of credential theft and data loss.

In addition to providing isolation for email links, the Menlo Secure Enterprise Browser solution offers several advanced features, including:

- Risk score calculation: Links in emails undergo risk score calculation to differentiate between known malicious sites and other links. Administrators can configure policies to block high-risk links while allowing controlled access to others, including options for full isolation or read-only access to prevent credential theft.
- Attachment isolation: Email attachment isolation enhances security by selectively blocking or isolating email attachments based on policy configurations. Attachments can be scanned, allowed, blocked, or isolated for safe viewing, with options to attach Safe Portable Document Format (PDF) versions for additional security.
- Configurable workflow: Administrators can define workflows to train users on appropriate responses to emails that contain links and attachments. This includes providing users with information about the clicked link and the resulting site to facilitate informed decision-making.
  - Basic mode: Displays a customizable message at the top of the page and loads the page in isolated, read-write mode.
  - Educate mode: Provides additional information about why the page is opened in a certain mode and usually loads the page in isolated, read-only mode.
  - Coach mode: Offers comprehensive training with pop-up windows explaining the risk factors associated with the clicked link.

Policy management

Email isolation provides administrators with customizable policies and granular controls to tailor security measures to organizational needs. From defining isolation rules based on risk scores to configuring attachment-handling policies, administrators can enforce security measures to specific users or groups and in alignment with business objectives and requirements. This includes managing sender and recipient lists, configuring uniform resource locator (URL) transformation rules, and defining attachment isolation policies. The granular level of control helps ensure that security measures remain adaptive and effective in mitigating evolving email threats.

Email isolation dashboard

In addition to proactive threat prevention, email isolation enhances incident response and threat intelligence capabilities. By logging and analyzing email interactions, organizations can gain valuable insights into emerging threats and user behavior. This visibility enables security teams to identify patterns, detect anomalies, and respond promptly to potential security incidents. The solution's email isolation dashboard offers insights into email link activity, user interactions, and link processing via customizable widgets:

- Risk score clicks: Tracks the total count and timestamps of URL clicks based on the risk score, dynamically assessing link risks.
- Threat type clicks: Monitors the total count and timestamps of URL clicks categorized by threat type, facilitating proactive threat mitigation.
- Link processing summary: Provides an overview of the number of email links processed within a specified timeframe, supporting continuous monitoring and enforcement of policies.
- Top user clicks: Highlights users with the highest count of clicks leading to transformed URLs, aiding in user-centric security awareness training.
- Exit mode behavior: Analyzes URL links based on exit mode behavior, including "read-write" and "connect direct" actions, for consistent enforcement of access controls.
- Emails processed: Records the total count and processing dates of all emails processed through isolation, facilitating compliance audit trails.
- Errors and error actions: Tracks errors encountered during email isolation processes, including rejected or aborted actions, providing insights for troubleshooting and continuous improvement of email security measures.

Cloud access security broker

The solution's cloud access security broker (CASB) capability enables SaaS governance, providing visibility and control over sanctioned and unsanctioned cloud applications accessed by users. Menlo CASB allows administrators to configure policies, monitor activities, and respond to threats from a centralized console. CASB access control capabilities can enforce adaptive access policies based on user context and risk levels. By integrating user identity, device posture, and behavior analytics, access to cloud services can be granted or denied based on dynamic risk assessment.

CASB helps mitigate risks associated with data loss, unauthorized access, and compliance violations through functionality including:

- Cloud application discovery and visibility: Identifies and visualizes cloud applications accessed by users, including unsanctioned applications (shadow IT), and provides detailed reporting on cloud app usage patterns and associated risks. Supports over 1,000 cloud applications and services.
- Cloud application control: Blocks or limits specific functions within sanctioned applications (login, share, upload, download). Enforces access to unsanctioned applications through isolation, preventing direct interaction with potentially risky services.

- Threat protection: Identifies and blocks malware within SaaS applications, safeguarding against malicious threats targeting cloud environments, as well as isolating document downloads from cloud apps, preventing potential data breaches and ensuring data integrity.
- Continuous risk monitoring: Analyzes cloud usage patterns, user activities, and security events, to help identify emerging threats and vulnerabilities.
- Compliance management: Monitors cloud app usage for compliance with regulations such as General Data Protection Regulation (GDPR), Health Insurance Portability and Accountability Act of 1996 (HIPAA), and Payment Card Industry Data Security Standard (PCI DSS). Provides insights into cloud app security posture and associated certifications.

Policy management

Inline CASB inspects traffic inline, acting as an intermediary between users and cloud applications. Inline CASB policies take precedence over existing access controls. It consolidates security policy enforcement, enabling organizations to apply granular controls over user interaction and file sharing and governing data protection with precision.

CASB dashboard

The CASB dashboard provides a centralized view of key CASB metrics such as top cloud applications used, application categories accessed, user activity on unsanctioned apps, and data loss prevention (DLP) violations. It provides information about cloud application usage and security metrics, including:

- Cloud application discovery: Provides a list of discovered applications with details like category, access count, risk score, and associated CASB profile.
- App insights: Offers risk scores for each application based on factors like security posture, compliance certifications, and vulnerabilities.
- App details: Displays information about individual applications, including security controls supported, compliance certifications, reputation scores, and associated domains.
- CASB profiles: Allows creation of predefined sets of access controls applicable to multiple applications or categories.
- Cloud application rules: Enables granular control over specific user actions within each application category (e.g., file upload, download).

Applicability to the HIPAA Security Rule

This section describes Coalfire’s compliance findings and the corresponding customer requirements and responsibilities for the Menlo Secure Enterprise Browser solution as it was reviewed in Coalfire’s analysis.

The narratives that follow detail HIPAA Security Rule Technical Safeguards that the Menlo Secure Enterprise Browser solution has applicability to address or support. This applicability applies either as a customer configurable item or as a native and default capability to address or support the safeguard. Menlo customers are also referred to as a CE&B. The findings assume that the Menlo Secure Enterprise Browser solution is used in conjunction with workloads that contain ePHI. Therefore, the Menlo Secure Enterprise Browser solution is considered in scope for application of the CE&B HIPAA-compliant security program.

It is crucial to understand that HIPAA Security Rule compliance requires a coordinated effort to first secure ePHI applications and then to augment the health care data platforms with technology that maintains secure access to those applications. The Menlo Secure Enterprise Browser falls into the non-ePHI application category and may only be used to maintain secure access. The Menlo Secure Enterprise Browser can only provide enablement and support for HIPAA Security Rule compliance, as its primary function supports other elements of a compliance program.

Successful implementation of any technology relies on the supporting control environment and the applied use of the technology in accordance with defined policies, processes, standards, and procedures. Complementary customer controls are responsibilities and dependencies that customers should address to ensure the efficacy of the Menlo Secure Enterprise Browser solution in supporting HIPAA Technical Safeguards. Typically, this includes an in-depth approach that leverages other, specialized technologies and security controls.

Capabilities supporting the HIPAA Security Rule

The Menlo Secure Enterprise Browser integrates a variety of components that collectively support the HIPAA Security Rule Technical Safeguards. These components ensure comprehensive protection of ePHI through access control, audit controls, data integrity, transmission security, and user authentication mechanisms.

Below is a summary of how solution components support the specific technical safeguards mandated by HIPAA.

Access Control (§ 164.312(a))

Standard: Implement technical policies and procedures for electronic information systems that maintain electronic protected health information to allow access only to those persons or software programs that have been granted access rights as specified in § 164.308(a)(4) [Information Access Management].

Four implementation specifications are associated with the Access Control standard:

(i) *Unique user identification (required):*

- *A CE&BA must determine the best user identification strategy based on their workforce and operations.*

(ii) *Emergency access procedure (required)*

- *CE&BAs must determine the types of situations that would require emergency access to an information system or application that contains ePHI.*

(iii) *Automatic logoff (addressable):*

- *The CE&BA must implement electronic procedures that terminate an electronic session after a predetermined time of inactivity.*

(iv) *Encryption and decryption (addressable):*

- *The CE&BA must implement a mechanism to encrypt and decrypt ePHI.*

The Menlo Secure Enterprise Browser supports compliance with the Technical Safeguards through the following:

Secure Web Gateway:

- Granular policy controls: Enforces policies through URL filtering and content inspection, restricting access to high-risk websites to ensure only authorized personnel can access ePHI.

Menlo Security Client and Secure Access Methods:

- Unique user identification: Assigns unique identifiers to users and enforces access policies across devices to ensure only authenticated users can access ePHI.
- State handling: Prevents active content from reaching the client by executing it within the Isolation Container, ensuring only sanitized resources are sent to the client.
- Dynamic proxy settings: Handles captive portals and adjusts settings based on location awareness, facilitating emergency access to ePHI.
- Immediate access to forensic data: Provides detailed forensic data and logs to support emergency access procedures.
- Session management: Implements automatic logoff procedures after periods of inactivity to prevent unauthorized access.
- State handling: Ensures that all other state information is destroyed immediately, enhancing security and compliance.

Browser Posture Manager:

- Security policy enforcement: Enforces security policies across all web browsers, ensuring adherence to standardized configurations for accessing ePHI.
- Strict communication protocol: Ensures the client accepts only allowed DOM instructions, and the server ignores non-protocol events, enhancing security.

Browser Forensics:

- Immediate access to forensic data: Provides immediate access to detailed forensic data and logs to support emergency access procedures.

Cloud Access Security Broker:

- Granular access policies: Defines and enforces access policies for cloud applications based on user roles and contextual attributes.
- Session management: Enforces automatic logoff mechanisms for cloud sessions after inactivity.

HEAT Shield:

- Blocking malicious websites: Detects and blocks access to malicious websites and phishing sites in real-time.

Firewall-as-a-Service:

- Centralized firewall management: Enforces security policies across network perimeters.

Audit Controls (§ 164.312(b))

Standard: Implement hardware, software, and/or procedural mechanisms that record and examine activity in information systems that contain or use electronic protected health information.

The Menlo Secure Enterprise Browser supports compliance with the Technical Safeguards through the following:

Browser Forensics:

- Detailed logging: Captures and logs comprehensive telemetry data, including web requests, file downloads, and browser activities related to ePHI.

Secure Web Gateway:

- Logging and monitoring: Records web traffic activities and security events, providing comprehensive audit trails.

Menlo Security Client and Secure Access Methods:

- Activity monitoring: Logs and monitors all traffic, including non-web traffic, ensuring comprehensive audit controls over user activities accessing ePHI.
- Isolation Container monitoring: Uses the MSIP monitor.js to observe changes and ensure isolation from the page's own JS.

Browser Posture Manager:

- Audit trail: Logs and monitors browser configurations and security events.

HEAT Visibility:

- Activity monitoring: Continuously monitors web logs and analyzes traffic patterns, recording activities within information systems containing ePHI.

Cloud Access Security Broker:

- Activity monitoring: Tracks user activities and data transactions in cloud environments, facilitating audit trails.

Integrity (§ 164.312(c))

Standard: Implement policies and procedures to protect electronic protected health information from improper alteration or destruction.

Implementation specification: Mechanism to authenticate electronic protected health information (addressable). Implement electronic mechanisms to corroborate that electronic protected health information has not been altered or destroyed in an unauthorized manner.

The Menlo Secure Enterprise Browser supports compliance with the Technical Safeguards through the following:

Browser Forensics:

- Detection of unauthorized alterations: Identifies and documents unauthorized alterations or manipulations of ePHI within browser sessions.

Secure Web Gateway:

- Content inspection: Uses threat intelligence feeds to detect and block malicious content, maintaining the integrity of web sessions.

Browser Posture Manager:

- Browser configuration integrity: Ensures adherence to standardized security policies and benchmarks to prevent unauthorized changes to browser settings.

HEAT Visibility:

- Detection of anomalous behavior: Uses advanced algorithms to identify potential threats and suspicious behaviors.

Cloud Access Security Broker:

- Data loss prevention: Enforces policies to detect and block unauthorized sharing or leakage of ePHI stored in cloud applications.

Person or Entity Authentication (§ 164.312(d))

Standard: Implement procedures to verify that a person or entity seeking access to electronic protected health information is the one claimed.

The Menlo Secure Enterprise Browser supports compliance with the Technical Safeguards through the following:

Secure Web Gateway:

- User authentication: Integrates with identity management systems for centralized authentication.

Menlo Security Client and Secure Access Methods:

- Unique user identification: Assigns unique identifiers to users and enforces access policies across devices.
- No foreign active content: The Content Security Policy (CSP) ensures that foreign scripts are not executed, enhancing security.

Browser Forensics:

- User identification and authentication: Correlates browser activities with user identities and authentication events.

Browser Posture Manager:

- Authentication mechanisms: Integrates with centralized authentication methods to verify user identities.

HEAT Visibility:

- Verification of identity: Supports authentication procedures by verifying user identities.

Cloud Access Security Broker:

- Multi-factor authentication: Supports strong authentication mechanisms for cloud application access.

Transmission Security (§ 164.312(e))

Standard: Implement technical security measures to guard against unauthorized access to electronic protected health information that is being transmitted over an electronic communications network.

Implementation specifications:

(i) Integrity controls (addressable):

- *Implement security measures to ensure that electronically transmitted electronic protected health information is not improperly modified without detection until disposed of.*

(ii) Encryption (addressable):

- *Implement a mechanism to encrypt electronic protected health information whenever deemed appropriate.*

The Menlo Secure Enterprise Browser supports compliance with the Technical Safeguards through the following:

Secure Web Gateway:

- HTTPS inspection: Ensures secure web access and enforces encryption standards like AES-256 for data transmitted over electronic communications networks.

Menlo Security Client and Secure Access Methods:

- Encrypted tunneling: Establishes encrypted tunnels for data transmission, ensuring the confidentiality and integrity of ePHI during transit.
- WebSocket communication: Utilizes WebSocket channels over TLS for secure communication between the client and Isolation Container.

Browser Forensics:

- Monitoring data transfers: Monitors data transfers within browser sessions, including encrypted transmissions and potential vulnerabilities.

Browser Posture Manager:

- HTTPS enforcement: Enforces HTTPS protocols and secure communication standards within browsers.

HEAT Visibility:

- Monitoring and alerting: Monitors networks for unauthorized access attempts and provides real-time alerts.

Cloud Access Security Broker:

- Encryption: Enforces encryption policies for data transmitted to and from cloud applications.

Secure Application Access:

- Encrypted data transmission: Ensures encrypted data transmission between applications and user devices.

Last-Mile Data Protection:

- Endpoint data protection: Ensures data protection at the endpoint and during transmission, preventing unauthorized alterations.

Firewall-as-a-Service:

- Secure communication channels: Implements encryption and secure communication for data transmission.

These components collectively establish a strong framework for securing ePHI, detecting security incidents, and maintaining compliance with the HIPAA Security Rule Technical Safeguards. By leveraging these capabilities, Menlo Secure Enterprise Browser addresses the specific security and compliance needs of healthcare environments effectively.

Complementary customer controls

Healthcare entities (Covered Entities and Business Associates) cannot achieve comprehensive HIPAA compliance solely by focusing on HIPAA's requirements. While HIPAA outlines required outcomes for Privacy and Security Rules compliance, it lacks specific technical guidance. To address this, entities should adopt a comprehensive cybersecurity framework, such as NIST SP 800-53 or ISO/IEC 27001, to inform their approach. The following summarizes customer responsibilities to ensure compliance with HIPAA standards and how they can complement the Menlo Secure Enterprise Browser solution.

- Choose a comprehensive framework like NIST SP 800-53 or ISO/IEC 27001 to guide technical controls not specified by HIPAA.
- Actively manage and update policies to ensure alignment with HIPAA requirements, preventing unauthorized access and modifications.
- Enforce encryption policies to ensure all ePHI transmissions are secure.
- Define policies within the Menlo Secure Browser that mandate the use of unique identifiers and secure protocols for all users accessing ePHI.
- Train users on the secure use of the solution, the importance of unique user identification, and adherence to organizational policies.
- Educate personnel on emergency access procedures using the solution to ensure readiness during critical situations.
- Use training modules that emphasize the proper use of unique identifiers and secure browsing practices to reduce accidental or intentional ePHI alterations.
- Assign unique names or numbers to each user to ensure they are uniquely identified.
- Maintain integration with systems like Active Directory for consistent user identity management.
- Regularly review user access rights and privileges to ensure only authorized individuals have access to ePHI.
- Integrate with directory services (e.g., LDAP) for user authentication and authorization, and enforce strong password policies and multi-factor authentication (MFA).
- Evaluate potential risks to ePHI and business continuity and implement actions to support HIPAA security mandates.
- Develop and maintain an incident response plan to address integrity breaches, authentication failures, and transmission security incidents.
- Utilize the solution’s audit logs and real-time monitoring capabilities to detect and respond to unauthorized access attempts and security incidents effectively.
- Regularly review audit logs generated by the solution to detect unauthorized access attempts, suspicious activities, or potential security incidents involving ePHI.
- Use SIEM systems to correlate audit events from the solution with other systems to gain a comprehensive view of the security posture.
- Implement auditing and monitoring processes within the solution to track user activities and maintain compliance with HIPAA’s audit control requirements.
- Ensure all ePHI transmitted over networks is encrypted using up-to-date cipher suites and secure protocols.
- Conduct regular audits of transmission security measures and configurations to identify and mitigate potential risks.
- Leverage the solution’s support for HTTPS and AES-256 encryption standards to ensure secure data transmission.

- Implement solutions like digital signatures or message authentication codes (MAC) to verify data authenticity and detect unauthorized modifications.
- Conduct regular audits of solution usage and configurations to identify and mitigate risks related to ePHI integrity.
- Use the solution's content inspection and threat intelligence feeds to maintain the integrity of web sessions and ePHI.
- Define and enforce session timeout policies based on risk assessments and operational needs.
- Regularly test the effectiveness of automatic logoff procedures to prevent unauthorized access due to idle sessions.
- Configure the solution to implement automatic logoff after periods of inactivity, ensuring compliance with HIPAA's access control requirements.

By implementing these complementary controls, organizations can enhance the effectiveness of the Menlo Secure Enterprise Browser solution in supporting the HIPAA Security Rule Technical Safeguards. These measures ensure robust protection of ePHI, efficient detection and response to security incidents, and overall compliance with regulatory requirements.

Conclusion

Coalfire has determined that the Menlo Security Secure Enterprise Browser solution aligns with the core requirements of the HIPAA Security Rule Technical Safeguards. Its strengths lie in access control, user behavior monitoring, and application security. The solution's comprehensive approach, which includes CASB, DLP, and FWaaS functionality, demonstrates a robust capability for protecting electronic protected health information (ePHI) and ensuring secure data transmission.

Achieving optimal HIPAA compliance requires a comprehensive strategy that extends beyond the capabilities of any single solution. This white paper explored how the Menlo Security Secure Enterprise Browser solution supports the HIPAA Security Rule Technical Safeguards and highlighted the customer responsibilities that are crucial for successful implementation.

By understanding these alignments and responsibilities, healthcare organizations can leverage the Menlo Secure Enterprise Browser solution's strengths while implementing additional security controls and processes to achieve a comprehensive HIPAA compliance posture. This layered approach, combining solution capabilities with a commitment to best practices and compliance requirements, provides organizations the ability to ensure the confidentiality, integrity, and availability of ePHI, mitigate risks, and continuously improve their security posture.

Legal disclaimer

This white paper is provided by Coalfire Systems, Inc., or its subsidiaries (“Coalfire”) for informational purposes only. This white paper is the property of Coalfire and is protected by U.S. and international copyright laws. Unauthorized use, reproduction, or distribution of this white paper, in whole or in part, is strictly prohibited. Factual information included in this white paper has been taken from sources that Coalfire believes to be reliable, but its accuracy, completeness, or interpretation cannot be guaranteed. Information is current as of the date of this white paper only and is subject to change without notice. This white paper is provided “as-is” with no warranties, including any warranty of merchantability, fitness for a particular purpose, and non-infringement. Coalfire expressly disclaims all liability arising from or relating to the use of any information or material included in this white paper for any purpose, including any actions taken or not taken based on the contents of this white paper. You are solely responsible for making your own independent assessment of the information in this white paper and for the development, implementation, and execution of your information security program. For questions regarding any legal or compliance matters referenced in this white paper, you should consult your legal counsel, security advisor, or the relevant standard authority.

Additional information, resources, and references

HIPAA resources

- U.S. Department of Health and Human Services (HHS) HIPAA Guidance: Provides comprehensive guidance on the HIPAA Privacy, Security, and Breach Notification Rules.
  - https://www.hhs.gov/hipaa/for-professionals/security/guidance/index.html
- HIPAA Security Rule Crosswalk to NIST Cybersecurity Framework: Aligns the HIPAA Security Rule to the NIST Cybersecurity Framework to help healthcare organizations manage cybersecurity risks.
  - https://www.hhs.gov/guidance/document/hipaa-security-rule-crosswalk-nist-cybersecurity-framework
- National Institute of Standards and Technology (NIST) Special Publication 800-66 Revision 1: Provides an implementation guide for the HIPAA Security Rule.
  - https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-66r1.pdf
- HHS Office for Civil Rights (OCR) Cybersecurity Guidance: Offers resources and guidance on cybersecurity best practices for HIPAA-covered entities.
  - https://www.hhs.gov/hipaa/for-professionals/security/guidance/cybersecurity/index.html
- HealthIT.gov HIPAA Security Risk Assessment Tool: An interactive tool to assist small to medium-sized healthcare practices in conducting security risk assessments as required by the HIPAA Security Rule.
  - https://www.healthit.gov/topic/privacy-security-and-hipaa/security-risk-assessment

Menlo Security resources

- Menlo Security’s website provides an overview of Menlo Security solutions and resources:
  - https://www.menlosecurity.com/
- Menlo Security’s blog features articles and insights on various security topics relevant to HIPAA:
  - https://www.menlosecurity.com/blog
- Menlo Security’s white papers offer additional information on specific Menlo Security solutions and use cases:
  - https://resources.menlosecurity.com/white-paper

Coalfire resources

- The Coalfire corporate payment card references and the Solutions Engineering offerings may be found at the following links:
  - https://www.coalfire.com/industries/payments
  - https://www.coalfire.com/solutions/cyber-engineering
- Coalfire corporate information is available at the following link:
  - https://www.coalfire.com/about

About the author

Jason Wikenczy | *Principal, Payments Advisory & Product Guidance*

Leveraging his experience in financial audit, cloud security, and business information technology, Jason employs a security-centric approach to assurance and compliance initiatives across a diverse set of industries. From government and energy to healthcare, insurance, and retail, Jason has an established record of helping clients achieve their business objectives while upholding strong security standards.

About Coalfire

The world's leading technology infrastructure providers, SaaS companies, and enterprises – including the top 5 cloud service providers and 8 of the top 10 SaaS businesses – rely on Coalfire to strengthen their security posture and secure their digital transformations. As the largest firm dedicated to cybersecurity, Coalfire delivers a comprehensive suite of advisory and managed services, spanning cyber strategy and risk, cloud security, threat and vulnerability management, application security, privacy, and compliance management. A proven leader in cybersecurity for the past 20 years, Coalfire combines extensive cloud expertise, advanced technology, and innovative approaches that fuel success. For more information, visit **Coalfire.com**.

WP_MENLO_HIPAA_2024