COALFIRE

WHITE PAPER

Menlo Security Secure Enterprise Browser Solution

Applicability for use within a Zero Trust Architecture

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 federal agencies, state agencies, public and private sector entities, and third-party audit or assessment organizations in meeting the technical requirements of the Cybersecurity and Infrastructure Security Agency’s (CISA) Zero Trust Maturity Model version 2.0 (ZTMM 2.0). The ZTMM 2.0 was created to assist agencies in the development of zero trust strategies and implementation plans.

This Product Applicability Guide (PAG) examines an entity’s adoption of the Menlo Secure Enterprise Browser solution in alignment with the technical requirements of the ZTMM 2.0. 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 a Zero Trust architecture (ZTA).

Coalfire PAGs provide a specific Coalfire opinion of a product’s applicability to ZTMM 2.0 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 Zero Trust objectives when it is properly employed by customers in covered environments and provides controls necessary for securing and managing access to applications within a Zero Trust architecture. The Menlo Secure Enterprise Browser solution provides functionality 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 a mature ZTA. These functions can support numerous Zero Trust objectives by minimizing access privileges, protecting sensitive data, and enabling detection of suspicious activity. The solution focuses on application security, establishing micro-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 ZTA objectives, customer capabilities for supplemental and complementary controls, and alignment of Zero Trust 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 implementing Zero Trust objectives.

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 ZTMM 2.0 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 ZTMM 2.0 objectives.
- State Coalfire's opinion of the review of the Menlo Secure Enterprise Browser solution's capacity to be used for adherence to ZTMM 2.0 objectives.

Although the opinion itself may be helpful, this PAG also contains a representative overview of many aspects of ZTMM 2.0., which readers may find of use. Coalfire also focused on the technical controls supporting ZTMM 2.0 objectives through use of a trial tenant. Additionally, Coalfire reviewed training and administrative documents, written supporting materials, and other technical artifacts as part of Menlo Secure Enterprise Browser solution documentation. Coalfire did not review organizational processes, procedures, or other non-technical artifacts.

Introducing Zero Trust

Zero Trust is a strategic framework designed to address the inherent vulnerabilities and complexities of modern IT environments. At its core, Zero Trust challenges the notion of implicit trust, urging organizations to verify and authenticate every access attempt regardless of its origin or destination. This fundamental shift in mindset represents a departure from traditional security models, which often rely on perimeter defenses and implicit trust assumptions.

Zero Trust has emerged as a strategic and critical framework for protecting organizations against evolving threats. Rooted in the principle of minimizing uncertainty and enforcing precise access controls, Zero Trust challenges traditional notions of perimeter-based security, advocating for a paradigm shift towards identity, context, and data-centric approaches.

As defined by the National Institute of Standards and Technology (NIST) Special Publication (SP) 800-207, Zero Trust encompasses a collection of concepts and ideas aimed at ensuring accurate, least-privilege-per-request access decisions in the face of a compromised network. The following core tenets are central to Zero Trust:

- Verify and authenticate: Subject every access attempt to rigorous verification and authentication regardless of its source or destination.
- Least privilege access: Ensure that users and devices have access only to those resources necessary to perform their specific tasks.
- Micro-segmentation/isolation: Use micro-segmentation to compartmentalize network resources and to limit lateral movement in the event of a security breach.
- Continuous monitoring/verification: Implement continuous monitoring and analysis of network traffic to detect and respond to threats in real-time.

ZTA represents an organization's comprehensive cybersecurity plan, with Zero Trust concepts integrated into component relationships, workflow planning, and access policies. It includes not only the network infrastructure and operational policies of an organization, but also the cultural and philosophical shifts necessary to embrace a Zero Trust mindset. The overarching goal of Zero Trust, as articulated by SP 800-207, is to prevent unauthorized access to data and services while enforcing access control with granular precision. This shift in approach, from a location-centric model to one centered around identity, context, and data, necessitates fine-grained security controls that adapt dynamically to evolving threats and user behaviors. The CISA ZTMM 2.0 offers a practical roadmap for organizations to achieve those objectives by guiding them through a series of maturity stages. Together, ZTA and the ZTMM 2.0 provide organizations with the guidance and tools needed for an organization to adopt and implement Zero Trust.

The National Security Telecommunications Advisory Committee (NSTAC) further emphasizes the foundational premise of Zero Trust: that no user or asset is implicitly trusted. Instead, Zero Trust assumes that a breach has either occurred or will occur, prompting a continuous verification approach that validates the legitimacy of every access attempt. Adopting

ZTA is undeniably a non-trivial effort, requiring organizations to reevaluate their cybersecurity philosophies and cultures. However, the benefits of Zero Trust include providing the visibility and control necessary to develop, implement, enforce, and evolve robust security policies that align with the dynamic nature of modern cyber threats.

Zero Trust and modern web browser use

The evolving landscape of modern work environments, characterized by the integration of cloud-based applications and the proliferation of hybrid work models, underscores the imperative for a Zero Trust approach to cybersecurity. Within this paradigm, the traditional notion of implicit trust is discarded, and every access attempt is subject to rigorous verification, regardless of whether it originates from within or outside the network perimeter.

Browsers, once perceived as innocuous tools for web surfing, now serve as the primary interface for accessing critical business applications, including email and productivity suites. This increased reliance on browsers for daily tasks means that browsers now represent one of the most vulnerable attack surfaces within the Zero Trust model. Attackers exploit browser vulnerability through Highly Evasive and Adaptive Threat (HEAT) attacks, which leverage sophisticated techniques like Hypertext Markup Language (HTML) smuggling – hiding malicious payloads inside seemingly benign HTML files – to evade traditional security measures and gain unauthorized access to sensitive data.

In a Zero Trust framework, the inherent risks associated with browser-based activities are acknowledged and addressed through continuous monitoring and verification of all data flows, regardless of their source or destination. The assumption of inherent security within browsers is challenged in Zero Trust, which recognizes that even seemingly legitimate web content may harbor malicious intent. Rather than relying solely on perimeter defenses or endpoint security controls, Zero Trust requires organizations to adopt a holistic approach to browser security that incorporates isolation, inspection, and continuous monitoring of web traffic. Traditional web security mechanisms, such as URL filtering and antivirus scanning, fall short in the Zero Trust model, as they lack the contextual awareness necessary to distinguish between benign and malicious content. Instead, a Zero Trust approach to browser security emphasizes the need for real-time analysis of web content, coupled with robust isolation techniques to contain potential threats before they can reach endpoints.

Furthermore, in alignment with Zero Trust principles, browser security is treated as an integral component of the overall security posture, subject to the same level of scrutiny and enforcement as other critical assets within the network. This entails implementing layered security controls, maintaining consistent policy enforcement, and enhancing visibility and forensics capabilities to detect and respond to threats effectively. By adopting a Zero Trust approach to browser security, organizations can mitigate the inherent risks associated with web-based activities, fortifying their defenses against sophisticated threats while maintaining a proactive stance in safeguarding sensitive data and critical assets.

Challenges to Zero Trust implementation with web browsers

Implementing a Zero Trust architecture presents unique challenges, particularly concerning web access and the inherent vulnerabilities of traditional browsers. While Zero Trust principles advocate for continuous verification and strict access controls, the dynamic nature of web browsing introduces complexities that can undermine these efforts, as demonstrated in Figure 1 below.

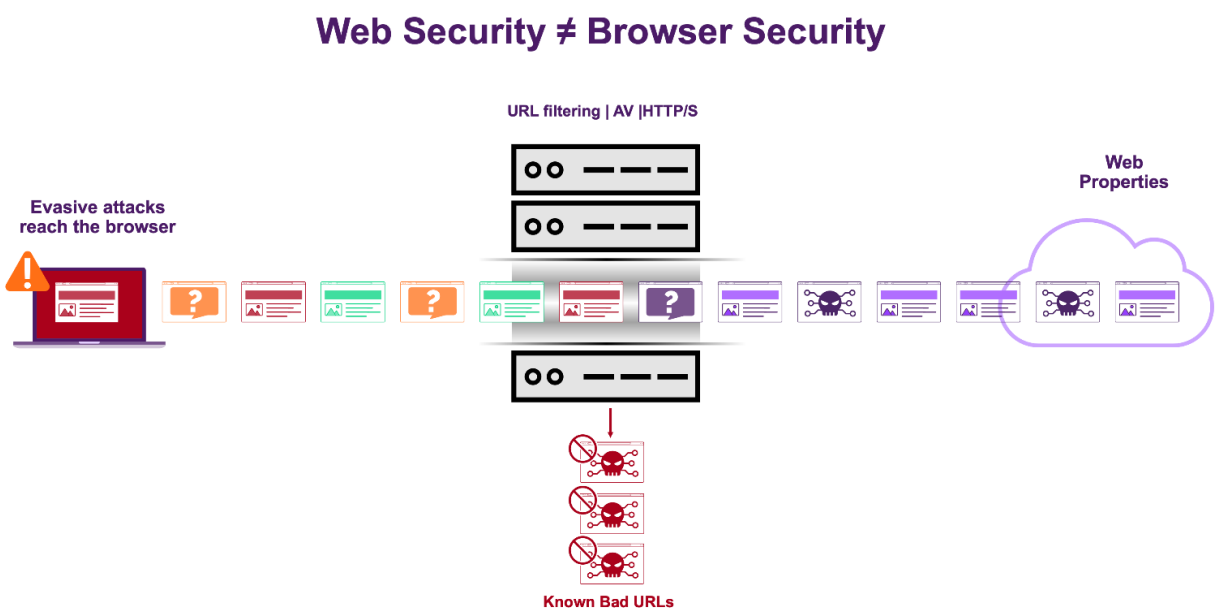

Figure 1: Web security ≠ browser security

Web access

Implementing Zero Trust principles for web access requires organizations to scrutinize every aspect of their browsing environment, from user authentication to content inspection. This level of granularity can be challenging to achieve, especially in environments with diverse user bases and complex access requirements. Moreover, ensuring seamless access to web-based applications while maintaining strict security controls demands careful planning and coordination across IT and security teams.

Browser security and security exploits

Historically, browsers, which were designed for general use on most operating systems, have lacked the layered security architecture required for enterprise environments. While some offer basic security settings, "safety-focused" consumer browsers prioritize features like privacy controls, which often fall short of the granular access controls and continuous monitoring demanded by certain security models like Zero Trust. This necessitates a shift towards solutions built with defense in depth and the isolation/separation principles that provide protection supporting Zero Trust objectives.

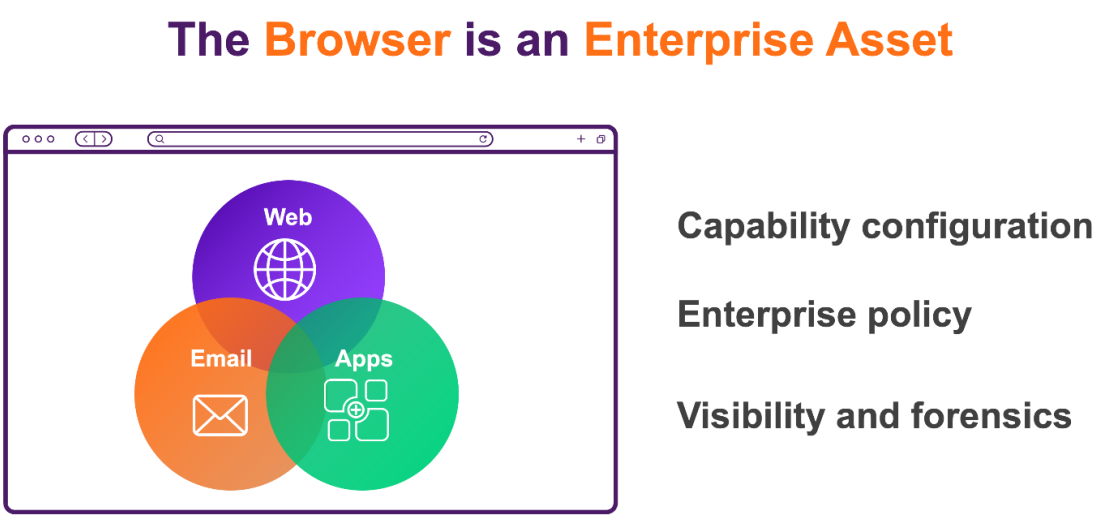

Figure 2: Layered approach to security includes the browser

Endpoint browsers are then subject to vulnerabilities that can be exploited to bypass Zero Trust controls. Common vulnerabilities include the presence of plugins, extensions, and local storage mechanisms, which can serve as entry points for malicious actors. These vulnerabilities expose organizations to a range of threats, including malware infections, data exfiltration, and account takeovers, undermining the integrity of Zero Trust architectures.

Malicious actors leverage the inherent vulnerabilities of traditional browsers on the local endpoint to circumvent Zero Trust controls and gain unauthorized access to sensitive resources. Techniques such as code obfuscation, HTML smuggling, and zero-day exploits target weaknesses in browser security mechanisms, evading detection and compromising organizational defenses. As a result, even organizations with robust Zero Trust frameworks may find themselves vulnerable to sophisticated attacks that exploit browser vulnerabilities.

Administration

Securing and managing traditional browsers across a diverse user base presents significant challenges for organizations. With employees accessing web resources from various devices and locations, maintaining consistent security policies, and ensuring compliance with Zero Trust principles becomes increasingly complex. Moreover, managing updates, patches, and configurations for disparate browser versions adds to the administrative burden, as it requires dedicated resources and infrastructure to maintain an effective security posture.

Addressing these challenges requires a holistic approach to browser security that goes beyond traditional perimeter defenses and endpoint security controls. Organizations should leverage solutions such as those offered by Menlo Security to enhance their Zero Trust architectures and mitigate the risks associated with traditional browsers. By adopting browser isolation, advanced threat detection, and secure access controls, organizations can strengthen their defenses against evasive ransomware, zero-hour phishing attacks, and other sophisticated threats, while enabling secure and productive web access for their workforce.

The Menlo Security approach to browser security

Menlo Security offers a security solution that seeks to address the above-mentioned security challenges through a proactive approach to threat mitigation, aligning closely with the principles of Zero Trust. A key component of the Menlo Security solution is the Menlo Secure Enterprise Browser, a cloud-driven enterprise browser utilizing isolation technology. To deliver a Zero Trust approach to preventing malicious attacks, the Menlo Secure Enterprise Browser solution seeks to mitigate threats before they reach endpoint devices by isolating web content in a secure cloud environment instead of

relying solely on perimeter defenses and endpoint security measures. In this way, the Menlo Secure Enterprise Browser can enhance security posture by minimizing the attack surface and protecting users from emerging threats.

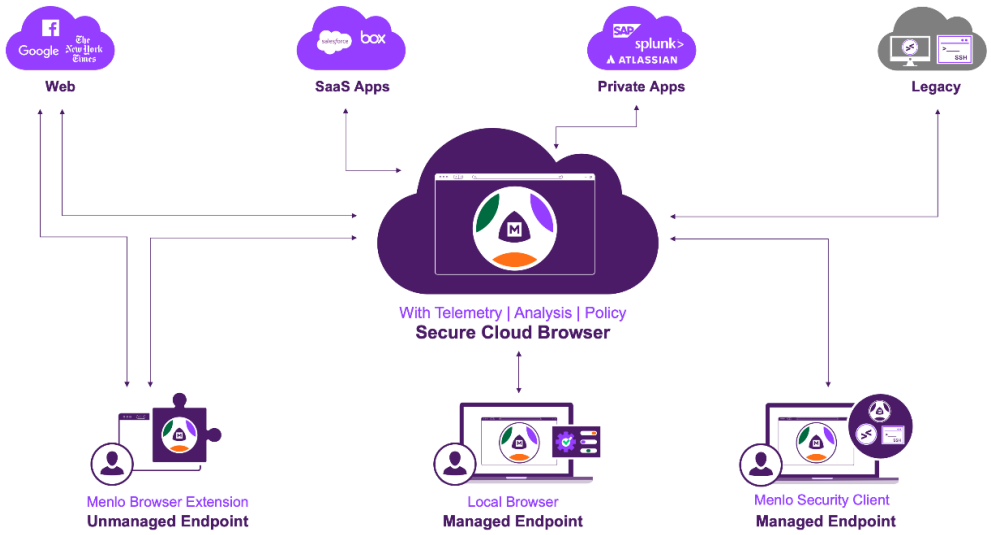

Figure 3: Menlo Secure Enterprise Browser solution architecture isolates threats from endpoints and protects applications

The Menlo Secure Enterprise Browser's cloud-native architecture enables scalability and extensibility, allowing organizations to adapt to evolving security challenges. By prioritizing user experience and operational efficiency, Menlo Security enables an effective response to dynamic threats.

The Menlo Secure Enterprise Browser solution encompasses the following capabilities:

- Manage the browser: The solution provides a unified management console for both local browsers and the Menlo Secure Enterprise Browser, streamlining policy configuration, reporting, and forensics. This approach enables organizations to effectively manage their existing browsers while benefiting from the enhanced security of the Menlo Secure Enterprise Browser, aligning with the Zero Trust principles of continuous verification and access controls.
- Protect the user: The solution safeguards users from zero-hour phishing attacks, malicious files, and exploits by enforcing security measures off the endpoint. By preventing direct interaction between local browsers and applications, the solution mitigates the risk of emerging threats targeting vulnerable software components, in line with the Zero Trust principles of least privilege access and continuous monitoring.
- Secure access and data: The solution provides robust access controls and data security for software-as-a-service (SaaS) and enterprise, or legacy, applications. By enforcing access policies and protecting sensitive data, organizations can reduce the risk of unauthorized access and data breaches, safeguarding digital transformation initiatives within the Zero Trust objectives of strict access controls and data protection.

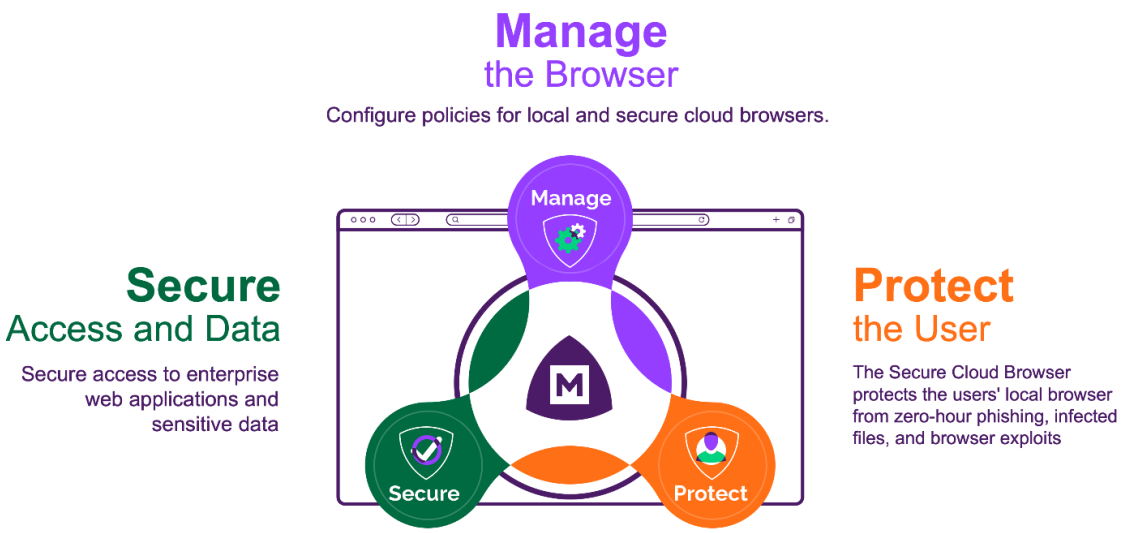

Figure 4: Secure Enterprise Browser solution: key security capabilities

The Menlo Secure Enterprise Browser's architecture, comprehensive and unified management console, specialized security capabilities, and native integration options enable organizations to minimize the attack surface on local browsers while providing enhanced security capabilities, improving organization's ability to implement cloud-driven security that aligns with the principles of Zero Trust.

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.

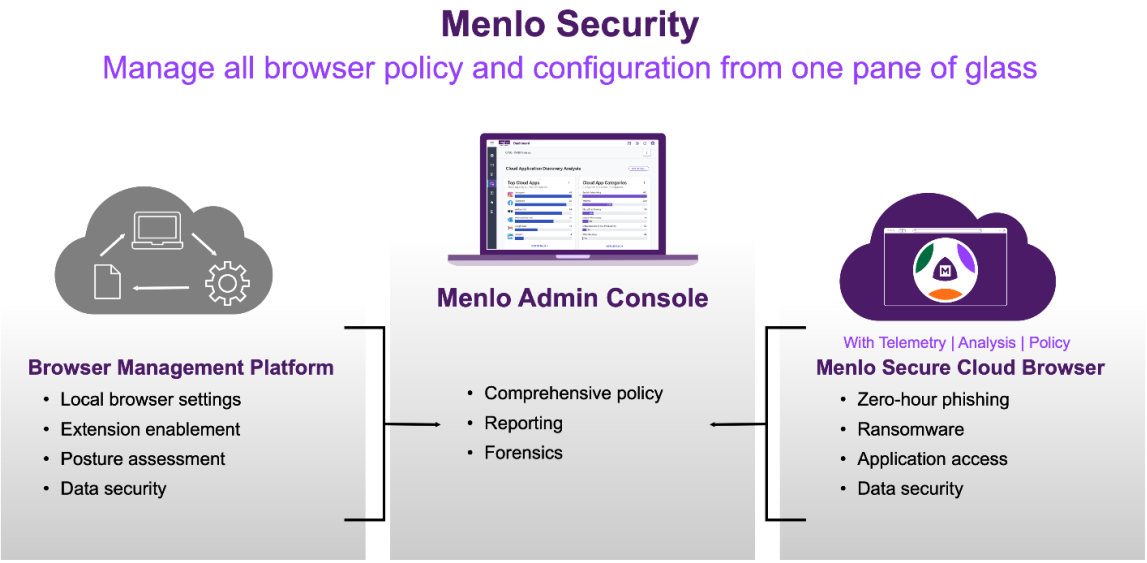

Figure 5: Posture management subsystem – policy, reporting, and forensics

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 creating a trust relationship. The user's browser trusts the JavaScript function delivered by the solution. This trust is established through cryptographic verification mechanisms for authenticity and integrity of the function. The solution 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, malware-free 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 its browser isolation 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.

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.

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.

Cloud access security broker

The solution's cloud access security broker (CASB) capability provides visibility and control over sanctioned and unsanctioned cloud applications accessed by users. As a single pane of glass for unified security management, 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.
- Integration with third-party CASB solutions: Integrates with existing CASB deployments for a unified view of cloud security.

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. This aligns with Zero Trust by ensuring the strictest security measures are applied consistently.

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).

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.

Secure Application Access

Secure Application Access (SAA), part of the Menlo Secure Enterprise Browser solution, offers a Zero Trust-aligned solution that prioritizes security while enabling access to enterprise applications for employees and partners. Employees, partners, and guests, for example, can access critical applications without the overhead of operational mechanisms and the security challenges used with traditional VPNs. In a Zero Trust environment, every access request undergoes strict verification. Menlo Secure Access adheres to Zero Trust principles by examining each request before granting least-privileged access to the specific application a user needs. This minimizes the attack surface and ensures users have only the permissions required for their tasks.

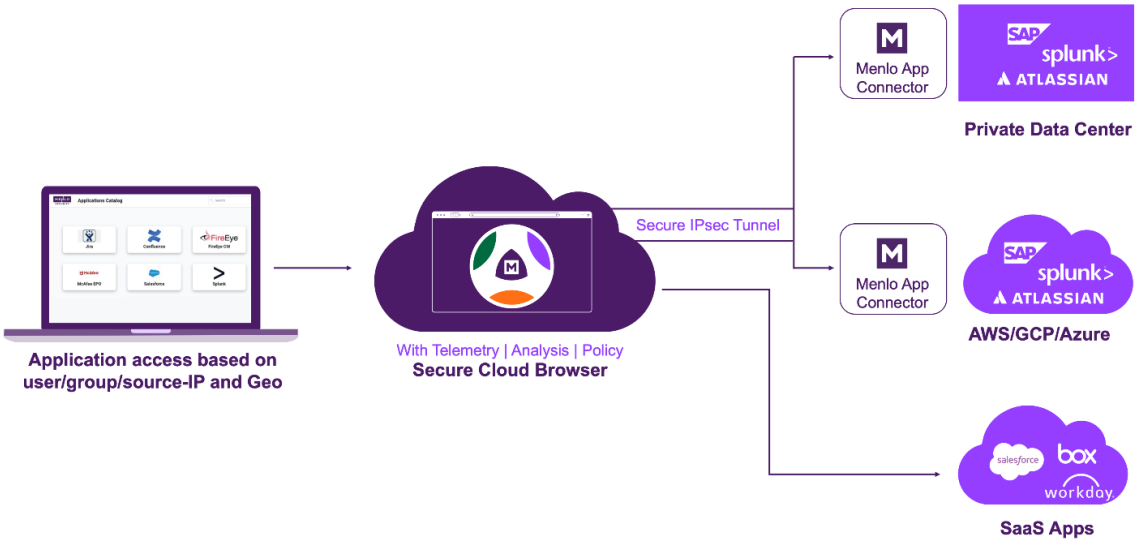

Figure 6: Access and security across application and user operating models

Secure Application Access acts as a secure gateway, shielding applications from the dangers of the public internet. By keeping these applications hidden, they become invisible, eliminating them as targets for malicious actors. Additionally, the Menlo Secure Enterprise Browser further isolates application rendering from user devices. This creates an air gap that prevents malware or compromised endpoints from reaching sensitive data within the application.

Secure Application Access provides organizations with granular control. Administrators can define access policies, tailoring permissions based on user roles, groups, and application features. This helps ensure that users are not granted unnecessary access, minimizing the risk of lateral movement within the network should a breach occur. Interfaces for policy configuration and streamlined user provisioning processes reduce the burden on security teams. Centralized administration provides a clear view of access controls and simplifies ongoing maintenance.

Secure Application Access offers comprehensive data-protection capabilities, including download/upload restrictions, redaction of sensitive data/PII, watermarking, and copy/paste limitations. These controls help safeguard sensitive information and prevent unauthorized data exfiltration across enterprise applications.

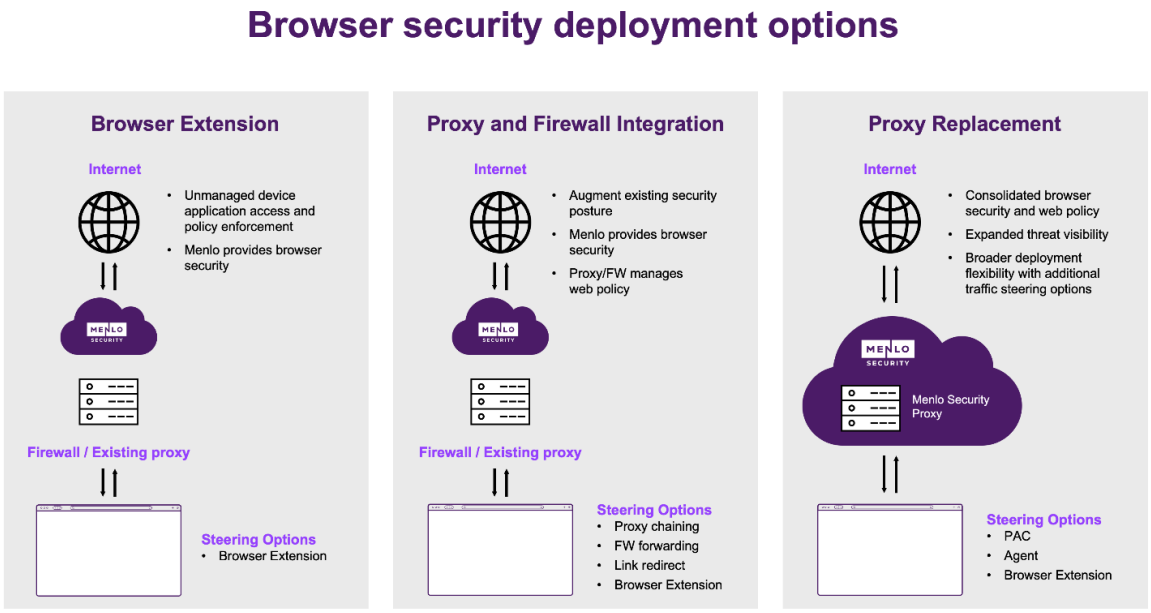

Figure 7: Menlo Secure Enterprise Browser deployment flexibility and steering options

Deployment options cater to both private and SaaS applications, with agentless and agent-based approaches depending on the application type. This adaptability enables organizations to integrate Secure Application Access into their existing infrastructure.

Key features of Secure Application Access

The key features of Secure Application Access include:

- Least-privileged access: Enforcement of a least-privilege access model, granting granular permissions based on specific resources that users require for their job functions. This aligns with Zero Trust by minimizing attack surfaces and access privileges.
- Protection against internet threats: By keeping private applications hidden from the public internet, applications are better shielded from internet-born threats like denial-of-service (DDoS) attacks, code injection, and Structured Query Language (SQL) injection. This proactive approach aligns with the Zero Trust principle of assuming untrusted external networks and implementing controls to mitigate risks.
- Granular security controls: Granular security controls help safeguard application access and data. These controls include 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, aligning with Zero Trust principles.
- Menlo Secure Enterprise Browser: Instead of direct endpoint access, the Menlo Secure Enterprise Browser is leveraged to isolate application rendering. This shields applications from content-based attacks and ensures that malicious requests cannot reach the server, even from compromised endpoints. This isolation aligns with Zero Trust principles of segmentation and minimizing trust assumptions.

Benefits of Secure Application Access

The key features of Secure Application Access include:

- Reduced attack surface: Hiding applications and enforcing role-based access controls reduces the attack surface and minimizes the risk of unauthorized access or lateral movement within the network. This aligns with Zero Trust ’s core tenets of continuous verification and strict access control.
- Protection against compromised endpoints: The Menlo Secure Enterprise Browser and sandboxing capabilities mitigate the risk of compromised endpoints accessing sensitive data. Even with a compromised endpoint, threat actors cannot directly access application data, preventing unauthorized access and breaches. This aligns with Zero Trust by minimizing trust in endpoints.
- Enhanced data security: Granular security controls and data protection measures, such as watermarking and data redaction, help organizations maintain data confidentiality and integrity. Applying these controls at the application-access-level helps achieve compliance with regulations and uphold Zero Trust data protection principles.
- Flexible deployment options: Deployment options for both private and SaaS applications support both zero-touch and agentless deployment for browser-based applications and agent-based deployment for non-browser-based applications. This flexibility allows organizations to adapt to evolving security needs and scale their access infrastructure without compromising security.
- Simplified management: Easy-to-manage policies and streamlined onboarding/offboarding processes simplify application access control management within a Zero Trust framework. Providing tools for policy configuration and monitoring enables organizations to maintain robust security with minimal operational overhead.

Zero Trust capabilities of Secure Application Access

The capabilities of Secure Application Access relative to Zero Trust include:

- Defining granular access policies for users/groups to access specific applications.
- Securing intranet access for contractors, granting read-only access with granular controls based on user/group, source internet protocol (IP) address, and location.
- Directing access from a native client to provide device posture assessment.
- Replacing web application rendering on the user device with rendering in the Secure Cloud Browser, protecting applications from malicious activity and user errors.
- Threat detection and prevention employs sandboxing and anti-virus (AV) scanning to identify and block malware or other threats attempting to exploit applications through user interactions.
- DLP granular controls like download/upload restrictions, redaction, file- and page watermarking, and copy/paste limitations.
- Flexible deployment options for agentless, client-based, and browser extension deployments.
- Simplified management of policies and centralized administration streamline access control and configuration.

Secure Application Access aligns with Zero Trust principles by enabling least-privileged access, protecting against internet-born threats, enforcing granular security controls, and leveraging Menlo Secure Enterprise Browser.

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.

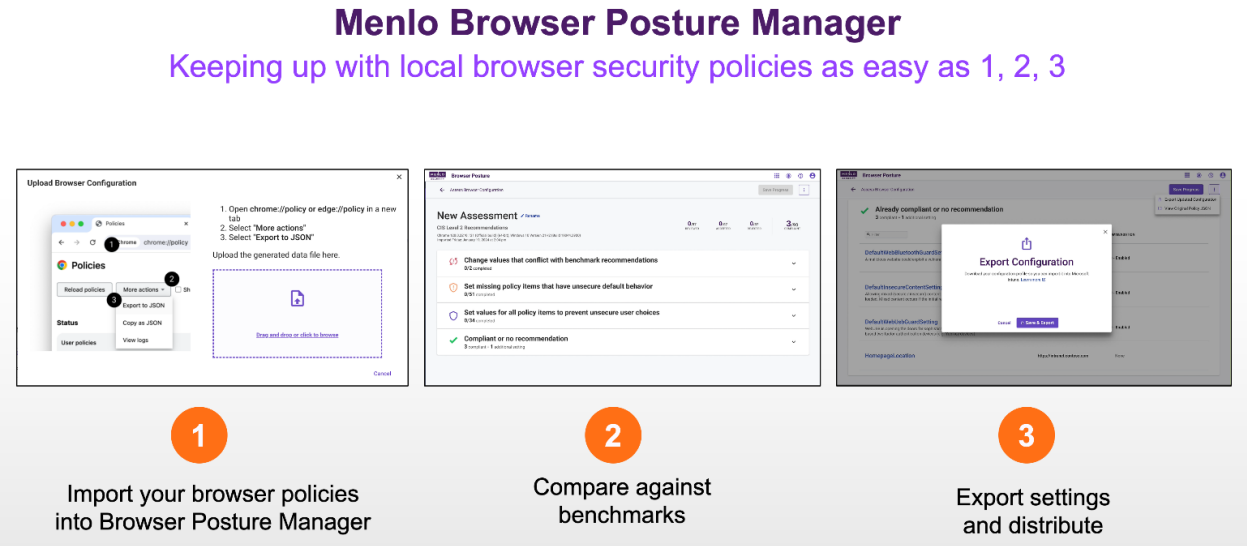

Figure 8: Centralized management and policy enforcement for browsers

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.

Browser Forensics

Browser 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, Browser 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.

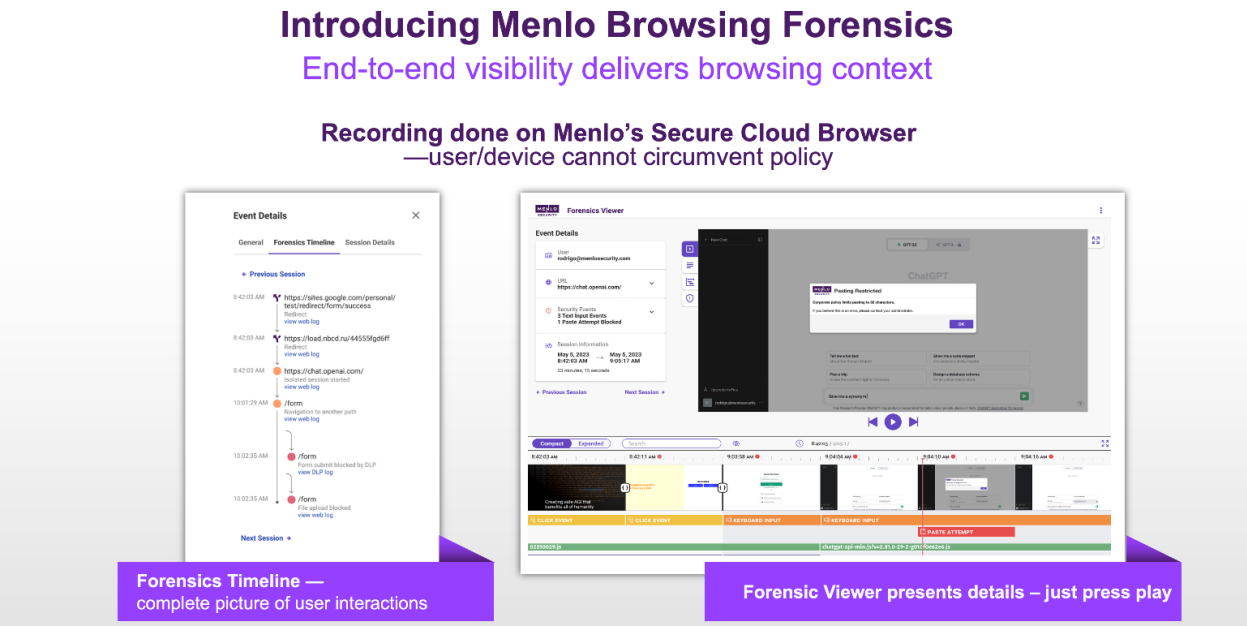

Figure 9: Browser Forensics features

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 pre-defined 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

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.

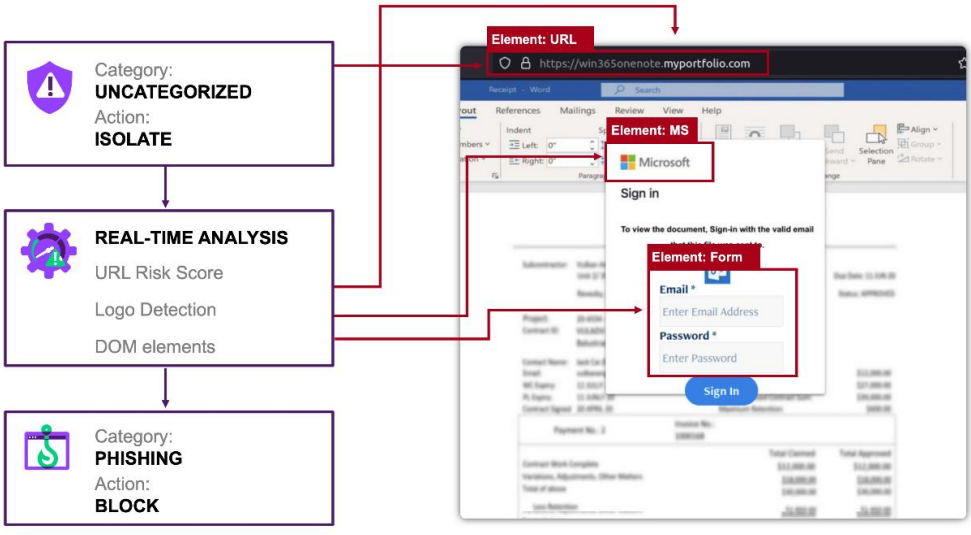

Figure 10: Real-time protection against sophisticated, evasive phishing attacks and threats

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 preventing users from entering sensitive information while still allowing them to view the content.
- Log access attempts for further investigation.

Aligned with the principles of Zero Trust security, 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 logs 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.

Figure 11: Proactive threat detection with evasive threat intelligence

Utilizing continuous, offline analysis of recent web logs, HEAT Visibility uncovers evasive threats that may have slipped past initial detection mechanisms. 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 web logs 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

Multiple options are available that enable secure user access to corporate resources and accommodate organizations' varying connectivity requirements and security postures.

Menlo Security Client

Menlo Security Client (MSC) is a lightweight application for user devices. The MSC enforces consistent security policies for all traffic, regardless of location (in-office, remote, roaming). It enables users to connect to Wi-Fi networks in public places by automatically handling captive portals (e.g., airports, hotels). MSC automatically adjusts proxy settings, minimizing disruptions to user workflows. With built-in location awareness, MSC dynamically adapts to different connectivity environments, determining a user's location and applying appropriate proxy settings based on placement within a corporate network or elsewhere. It creates an encrypted tunnel between the client and the Menlo cloud, ensuring data privacy and integrity.

This solution allows administrators to monitor and apply security policies for non-web traffic, including those originating from roaming users who might bypass traditional on-premises firewalls. Additionally, user identification within this internet traffic enables granular policy enforcement based on various user attributes. The MSC offers centralized configuration through the Menlo admin portal and includes tamper protection mechanisms to maintain intended security posture. When configured in SAA mode, the MSC facilitates secure access to private and enterprise applications based on Zero Trust principles. Application access controls can be defined based on user roles, group memberships, source IP addresses, geo-location, and device posture checks.

Clientless Web Access

For scenarios where agent deployment is impractical, Menlo Security offers a clientless web portal approach for secure access to browser-based private and enterprise applications. This zero-touch deployment eliminates the need for installing agents on user devices, importing certificates, or managing public DNS records for private applications. Users log in to a secure portal where they can access a list of provisioned applications. This approach provides a convenient way for organizations to grant access to applications from unmanaged devices for employees, partners, and contractors.

Browser Extension

Further extending access flexibility, Menlo Security offers a lightweight browser extension that mirrors the functionalities of the clientless web portal. This extension allows users to seamlessly access applications even outside the dedicated portal. Links received through emails, messages, or other applications can be automatically redirected to the appropriate application through the extension.

Menlo Connect

Menlo Connect is a lightweight application that provides organizations with secure endpoint connectivity and the ability to access corporate resources from anywhere, supporting remote work and enhanced security. It manages system proxy settings and handles issues like captive portals and restricted network access. By requiring the use of the PAC file and preventing unauthorized changes, Menlo Connect protects endpoints from malicious activities. It also offers centralized control and configuration capabilities for administrators. Using the Menlo Connect interface, administrators can deploy, configure, and monitor Menlo Connect agents across endpoints, ensuring consistent security policies.

Menlo Secure Enterprise Browser solution support for Zero Trust architecture

Zero Trust Maturity Model 2.0

ZTMM 2.0 provides a structured approach for organizations to assess and advance their implementation of ZTA. Comprising five distinct pillars (Identity, Devices, Networks, Applications and Workloads, and Data) and three cross-cutting capabilities, the ZTMM 2.0 outlines an iterative process, allowing organizations to make incremental advancements over time towards optimization. At the core of the ZTMM 2.0 are seven key tenets of Zero Trust, as defined in SP 800-207, which emphasize principles such as securing all data repositories and communications regardless of network location, granting access on a per-session basis, and continuously monitoring the security posture of assets.

While the ZTMM 2.0 standard itself does not explicitly call out browser security as a ZTA pillar, it is a critical vulnerability area that agencies and organizations must consider when planning and implementing their ZTA strategy. Web browsers are a common attack vector for cybercriminals and securing them is essential for an organization's overall ZTA posture.

As organizations transition towards optimal Zero Trust implementations, associated solutions increasingly rely on automated processes and systems that integrate across pillars and dynamically enforce policy decisions. Each pillar can progress independently, but cross-pillar coordination becomes essential as maturity advances. The journey through the ZTMM comprises multiple stages (Traditional, Initial, Advanced, and Optimal), each demanding greater levels of protection, detail, and complexity for adoption. Guiding criteria for each stage enable organizations to evaluate maturity across Zero Trust technology pillars consistently.

While the ZTMM 2.0 focuses on critical cybersecurity aspects for federal enterprises, it does not encompass all cybersecurity activities, such as incident response or specifics for logging and monitoring. Additionally, it does not address challenges specific to operational technologies or emerging technologies, such as machine learning and AI, within Zero Trust solutions. The model also does not encompass challenges related to operational technologies, certain Internet of Things (IoT) devices, or emerging technologies.

Agencies should carefully plan ZTA implementation based on factors such as risk, mission, federal requirements, and operating constraints. External partnerships and service providers should also be considered in ZTA planning to ensure comprehensive security measures. The ZTMM 2.0 serves as a guide to help organizations navigate their journey towards Zero Trust implementation and enhance their overall cybersecurity posture, adapting and evolving over time to meet evolving threats and operational needs.

This section evaluates how the Menlo Secure Enterprise Browser solution assists customers in aligning with each ZTMM 2.0 pillar, and associated functions, and identifies customer considerations essential for maximizing effectiveness within a ZTA.

Identity pillar

This pillar focuses on establishing strong authentication and authorization mechanisms to verify a user’s identity and access rights. The subsections below detail how specific Menlo Secure Enterprise Browser solution components contribute to the identity pillar, categorized by corresponding ZTMM 2.0 function and maturity stage.

Complementary customer controls

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. Typically, this includes an in-

depth approach that leverages other, specialized technologies and security controls. In support of optimizing cross-cutting functions, customers should consider complementary, and often required, responsibilities supporting ZTMM 2.0 identity functions, including:

- Customers are responsible for establishing user provisioning processes, managing user identities throughout their life cycle (creation, activation, deactivation, deletion), and enforcing strong password policies.
- Integrating the Menlo Secure Enterprise Browser solution with existing directory services (e.g., Active Directory, Lightweight Directory Access Protocol [LDAP]) for user authentication and authorization.
- Defining and enforcing specific multi-factor authentication (MFA) requirements (e.g., types of MFA acceptable, risk-based MFA enforcement).

Solution support

The following details how specific Menlo Secure Enterprise Browser solution components contribute, categorized by corresponding ZTMM 2.0 function and maturity stage.

Function	Maturity Alignment	Maturity Stage	Supporting Elements
Authentication	Advanced	Agency begins to authenticate all identity using phishing-resistant MFA and attributes, including initial implementation of passwordless MFA via FIDO2 or PIV.	• MFA support: Integrates with various MFA solutions, enabling strong authentication beyond basic passwords. Integration with advanced MFA solutions can provide phishing resistance. • Risk-based access control: Allows for policy configuration based on user attributes and risk scores, promoting context-aware access decisions.
Identity stores	Advanced	Agency begins to securely consolidate and integrate some self-managed and hosted identity stores.	• Identity provider (IdP) integration: Relies on existing customer-managed Identity stores (e.g., Active Directory, Azure AD) for user authentication and streamlined access management. • Leveraging identity store risk scores: Can leverage risk assessments from integrated providers to inform access control decisions.
Risk assessments	Advanced	Agency determines identity risk with some automated analysis and dynamic rules to inform access decisions and response activities.	• Leveraging external assessments: Integrates with IdPs and SIEM systems for potential leverage of risk scores to influence access control decisions.
Access management	Optimal	Agency uses automation to authorize just-in-time and just-enough access tailored to individual actions and individual resource needs.	• Policy-based access control: Allows for granular access control decisions based on numerous factors like user, device, application, and risk. • Context-aware access: Policy configuration can consider context-aware factors for access control, potentially including location or unusual activity detection. • Integration with IdPs: Integrates with existing IdPs for authentication and authorization data.

Function	Maturity Alignment	Maturity Stage	Supporting Elements
Visibility and Analytics Capability	Advanced	Agency performs automated analysis across some user and entity activity log types and augments collection to address gaps in visibility.	• ACR: The protocol carries user activity (keystrokes and mouse clicks) to the Secure Cloud Browser and prevents malicious activity from flowing in the upstream direction. • MSC: Allows for improved visibility over traffic from user activity for stricter control and customization of policy enforcement. • Browser Forensics: Provides captures of user activity. • Menlo Insights: Provides insights into user activity related to data access attempts. • SAA: All user activity that takes place on pages accessed via SAA is logged.
Automation and Orchestration Capability	Client-driven	Client-driven	• Policy engine allows for automated access control decisions and responses based on configured policies.
Governance Capability	Client-driven	Client-driven	• Client-driven

Table 1: Solution support for ZTMM 2.0 identity functions

Devices pillar

This pillar emphasizes managing and securing devices that access organizational resources. The following subsections detail how specific solution components contribute to this pillar, categorized by corresponding ZTMM 2.0 function and maturity stage.

Complementary customer controls

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. Typically, this includes an in-depth approach that leverages other specialized technologies and security controls. In support of optimizing cross-cutting functions, the customer should consider complementary, and often required, responsibilities supporting ZTMM 2.0 devices functions, including:

- Implementing and maintaining endpoint security solutions on user devices to complement the Menlo Secure Enterprise Browser solution's focus on application access control.
- Defining and enforcing device posture requirements (e.g., anti-virus software, operating system updates) to ensure devices meet security standards before granting access.
- Defining device enrollment processes and managing device configurations according to security policies.

Solution support

The following details how specific Menlo Secure Enterprise Browser solution components contribute, categorized by corresponding ZTMM function and maturity stage.

Function	Maturity Alignment	Maturity Stage	Supporting Elements
Policy Enforcement & Compliance Monitoring	Advanced	Agency has verified insights (i.e., an administrator can inspect and verify the data on device) on initial access to device and enforces compliance for most devices and virtual assets. Agency uses automated methods to manage devices and virtual assets, approve software, and identify vulnerabilities and install patches.	• Policy-based access control: Leverages device posture for access control decisions and offers security functionality that can improve device hygiene. • Traffic Steering Agent: Consistent policy enforcement regardless of the device being used by the user. • Web Policy Management: Granular web browsing policies can restrict access to risky websites, enforce isolation rules, and control exemptions for specific users or situations. • Document and Archive Isolation: Documents examined within an isolated environment minimize the risk of malware or other threats infecting the user's device through downloaded files. • Last-Mile Data Protection: Deep content inspection, policy enforcement on data uploads and submissions, and copy/paste controls. • Secure Web Gateway: Role in overall device security by filtering web traffic, identifying and blocking malicious URLs and downloads, reducing risk of malware and other threats reaching the user's device.
Asset & Supply Chain Risk Management	Client-driven	Client-driven	• SAA enables third-party suppliers on unmanaged devices to securely access company apps. • External integration potential: Integration with SIEM solutions can offer asset discovery features. • The Menlo Secure Enterprise Browser solution's primary functionality targets runtime security for devices rather than pre-deployment asset discovery, inventory, or supply chain risk assessments.
Resource Access	Optimal	Agency's resource access considers real-time risk analytics within devices and virtual assets.	• Policy-based access control that can consider device health, application risk, and user identity as factors. • Zero Trust approach that grants access based on context, not just device type.
Device Threat Protection	Advanced	Agency begins to consolidate threat protection capabilities to centralized solutions for devices and virtual assets and integrates most of these capabilities with policy enforcement and compliance monitoring.	• Browser Isolation: Prevents malicious code from reaching the user's device endpoint. • ACR: Minimizes the attack surface on the user's device by rendering web content within the secure cloud environment and transmitting only safe rendering instructions to the user's browser. • Secure Download Environment: Scans downloaded files for malware before allowing them to reach the user's device. • SAA: Reduces attack surface for vulnerabilities related to third-party software in the form of plugins or extensions. • Integration with SIEM solutions can provide broader threat visibility.

Function	Maturity Alignment	Maturity Stage	Supporting Elements
Visibility and Analytics Capability	Client-driven	Client-driven	• Enhanced Visibility: Insights into user behavior and potential security risks that can be integrated with existing SIEM systems for a more holistic view of the security landscape. • User activity monitoring: Supports user activity monitoring within the secure browsing session, identifying suspicious behaviors or attempts to bypass security controls.
Automation and Orchestration Capability	Client-driven	Client-driven	• Menlo Secure Enterprise Browser solution examines vulnerable services on a website when a user visits it and can isolate the session to keep the user's browser clean and unexposed to threats which may exist.
Governance Capability	Client-driven	Client-driven	• Client-driven.

Table 2: Solution support for ZTMM 2.0 device functions

Networks pillar

This pillar highlights the importance of segmenting networks and controlling network traffic to limit lateral movement of threats. The following details how specific solution components contribute to this pillar, categorized by corresponding ZTMM 2.0 function and maturity stage.

Complementary customer controls

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. Typically, this includes an in-depth approach that leverages other specialized technologies and security controls. In support of optimizing cross-cutting functions, the customer should consider complementary, and often required, responsibilities supporting ZTMM networks functions, including:

- Designing and implementing network segmentation strategies to isolate sensitive resources and limit lateral movement within the network (may require additional network security tools).
- Leveraging network traffic inspection tools to monitor network activity, detect suspicious behavior, and potentially integrate with the Menlo Secure Enterprise Browser solution for a more holistic view.

Solution support

The following details how specific solution components contribute, categorized by corresponding ZTMM 2.0 function and maturity stage.

Function	Maturity Alignment	Maturity Stage	Supporting Elements
Network Segmentation	Optimal	Agency network architecture consists of fully distributed ingress/egress micro-perimeters and extensive micro-segmentation based	• FWaaS for application-level security focuses on Zero Trust principles rather than traditional network segmentation between internal resources. It demonstrates a move towards a more advanced

Function	Maturity Alignment	Maturity Stage	Supporting Elements
		around application profiles with dynamic just-in-time and just-enough connectivity for service-specific interconnections.	approach to segmentation by focusing on application security and context-aware access control. • For Optimal alignment, the solution would ideally offer functionality for true micro-segmentation within the network itself, creating isolated security zones at a more granular level.
Network Traffic Management	Optimal	Agency implements dynamic network rules and configurations that continuously evolve to meet application profile needs and reprioritize applications based on mission criticality, risk, etc.	• Zero Trust principles inherently promote traffic inspection and control based on identity, device, and application. • FWaaS provides functionality for traffic filtering and policy enforcement based on security requirements. • For Optimal maturity, the solution provides advanced analytics and dynamic traffic-shaping capabilities.
Traffic Encryption	Optimal	Agency ensures encryption for all applicable internal and external traffic protocols, manages issuance and rotation of keys and certificates, and begins to incorporate best practices for cryptographic agility.	• TLS inspection secures connections. • For Optimal maturity, the solution would ideally offer functionality to encrypt all traffic by default across the entire network infrastructure. It would also need robust key management capabilities to ensure secure handling of encryption keys.
Network Resilience	Optimal	Agency integrates holistic delivery and awareness in adapting to changes in availability demands for all workloads and provides proportionate resilience.	• Global infrastructure with automatic failover mechanisms: Leverages geographically distributed data centers with automatic traffic rerouting in case of failure at any location. • Redundant components within each data center further enhance solution resilience. • Zero Trust principles inherently promote least-privilege access and segmentation, which can limit the blast radius of potential attacks. • Sandboxing technology can isolate threats and prevent them from spreading across the network. • Denial-of-service (DoS) mitigation through policy enforcement.
Visibility and Analytics Capability	Advanced	Agency deploys anomaly-based network detection capabilities to develop situational awareness across all environments, begins to correlate telemetry from multiple sources for analysis, and incorporates automated processes for robust threat hunting activities.	• Zero Trust approach and FWaaS: Provides network traffic visibility through connection inspection for security purposes. • Integration with SIEM solutions for broader network visibility and analytics. • HEAT Visibility with HEAT Shield threat detection capabilities: HEAT Visibility offers insights into zero-day threats and suspicious application behavior.

Function	Maturity Alignment	Maturity Stage	Supporting Elements
Automation and Orchestration Capability	Client-driven	Client-driven	• Policy engine allows for automated access control decisions and responses based on configured policies.
Governance Capability	Client-driven	Client-driven	• Client-driven

Table 3: Solution support for ZTMM 2.0 network functions

Applications and workloads pillar

This pillar focuses on securing applications and workloads to prevent unauthorized access or exploitation. The following provides details of how specific solution components contribute, categorized by corresponding ZTMM 2.0 function and maturity stage.

Complementary customer controls

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. Typically, this includes an in-depth approach that leverages other specialized technologies and security controls. In support of optimizing cross-cutting functions, the customer should consider complementary, and often required, responsibilities supporting ZTMM 2.0 applications and workloads functions, including:

- Maintaining a comprehensive inventory of applications and workloads within their environment. This includes conducting risk assessments to identify potential vulnerabilities within applications that the Menlo Secure Enterprise Browser solution might not directly address.
- Implementing a vulnerability management program to identify and patch vulnerabilities within applications and workloads, independent of the Menlo Secure Enterprise Browser solution's focus on access control.
- Integrating application security testing tools to proactively identify and address vulnerabilities within applications before deployment.

Solution support

The following details how specific solution components contribute, categorized by corresponding ZTMM 2.0 function and maturity stage.

Function	Maturity Alignment	Maturity Stage	Supporting Elements
Application Access	Optimal	Agency continuously authorizes application access, incorporating real-time risk analytics and factors such as behavior or usage patterns.	• Zero Trust approach: At its core, the Menlo Secure Enterprise Browser solution is built on Zero Trust principles. This inherently promotes least privilege access control for applications, ensuring users only access the specific resources they need for their job functions. • Browser isolation: The Menlo Secure Enterprise Browser solution's technology isolates web browsing sessions, preventing malware or malicious code within applications from reaching the user's device or the corporate network.

Function	Maturity Alignment	Maturity Stage	Supporting Elements
			• Access control granularity: The solution allows for granular access control based on numerous factors such as user identity, device posture, application risk level, and more. • Support for various applications: The Menlo Secure Enterprise Browser solution caters to securing access to web applications, SaaS applications, and private or internal applications.
Application Threat Protections	Optimal	Agency integrates advanced threat protections into all application workflows, offering real-time visibility and content-aware protections against sophisticated attacks tailored to applications.	• Browser isolation: Prevents malicious code from reaching and infecting web applications addressing risk of web-based attacks compromising applications and exploiting vulnerabilities within them. • Threat detection/prevention: Advanced threat detection techniques identify and neutralize malicious content within web pages and applications accessed through the browser. • ACR: Minimizes attack surface of web applications by rendering web content within the secure cloud environment. • Last-Mile Data Protection: DLP policies can prevent sensitive data from being leaked or exfiltrated through web applications. • Least privilege access: Potential to integrate with existing IAM systems to enforce least privilege access principles for web applications. • Integration with security tools: Can integrate with existing SIEM solutions for broader threat intelligence and provide actionable alerting for quicker incident response.
Accessible Applications	Optimal	Agency makes all applicable applications available over open public networks to authorized users and devices, where appropriate, as needed.	• Support for various applications: Caters to securing access to web applications, SaaS applications, and private or internal applications.
Secure Application Development and Deployment Workflow	Client-driven	Client-driven	• Client-driven
Application Security Testing	Client-driven	Client-driven	• Client-driven
Visibility and Analytics Capability	Optimal	Agency performs continuous and dynamic monitoring across all applications to maintain	• HEAT Visibility: Provides insights into application access patterns, potential security risks within web browsing sessions, and user behavior.

Function	Maturity Alignment	Maturity Stage	Supporting Elements
		enterprise-wide comprehensive visibility.	• User behavior analytics: HEAT Visibility can identify anomalous user behavior within applications, which could indicate compromised accounts or attempts to breach application security. • Application access patterns: Provides insights into how users access applications that can help identify risky access patterns or potential shadow IT usage. • Threat detection: Correlating application access data with threat intelligence might aid in identifying and responding to application-borne threats.
Automation and Orchestration Capability	Client-driven	Client-driven	• Policy engine allows for automated access control decisions and responses based on configured policies.
Governance Capability	Client-driven	Client-driven	• Client-driven

Table 4: Solution support for ZTMM 2.0 application and workload functions

Data pillar

This pillar emphasizes protecting data at rest, in transit, and in use. The following details how specific solution components contribute, categorized by corresponding ZTMM 2.0 function and maturity stage.

Complementary customer controls

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. Typically, this includes an in-depth approach that leverages other specialized technologies and security controls. In support of optimizing cross-cutting functions, the customer should consider complementary, and often required, responsibilities supporting ZTMM 2.0 data functions, including:

- Classifying and labeling sensitive data across various data stores to facilitate data loss prevention and access control decisions.
- Implementing data encryption solutions beyond the Menlo Secure Enterprise Browser solution's capabilities to protect data at rest within storage systems.

Solution support

The following provides a breakdown of how specific solution components contribute, categorized by corresponding ZTMM 2.0 function and maturity stage.

Function	Maturity Alignment	Maturity Stage	Supporting Elements
Data Inventory Management	Client-driven	Client-driven	• Client-driven

Function	Maturity Alignment	Maturity Stage	Supporting Elements
Data Categorization	Client-driven	Client-driven	• Data classification: The Menlo Secure Enterprise Browser can integrate with data classification solutions like MIP. • Data visibility: The Menlo Secure Enterprise Browser solution might provide visibility into the types of data being accessed through applications. This data visibility, in some cases, could be relevant for categorization (e.g., identifying PII or financial data). • DLP rules and dictionaries apply bi-directionally, to uploads and downloads. • DLP integration: If integrated with DLP solutions, the Menlo Secure Enterprise Browser solution might leverage pre-defined data classifications within the DLP tool to identify and protect sensitive data during transit.
Data Availability	Client-driven	Client-driven	• Client-driven
Data Access	Optimal	Agency automates dynamic just-in-time, and just-enough data access controls enterprise-wide with continuous review of permissions.	• Zero Trust approach: The Menlo Secure Enterprise Browser solution core philosophy aligns with Zero Trust principles, which require continuous verification for all data access attempts, regardless of user identity or location. • Enhanced security: SSO integration can enforce centralized authentication policies and leveraging MFA for added protection. • Simplified Administration: IdP integration for application access, including the Secure Enterprise Browser. • Policy-based access control: The solution allows for defining granular access control policies based on user attributes, device posture, application risk level, and other factors. This ensures that only authorized users can access specific data. • Data isolation: The Menlo Secure Enterprise Browser solution isolates user sessions and data within a secure execution environment, further restricting unauthorized access to sensitive information.
Data Encryption	Client-driven	Client-driven	• Client-driven
Visibility and Analytics Capability	Advanced	Agency maintains data visibility in a more comprehensive, enterprise-wide manner with automated analysis and correlation and begins to employ predictive analytics.	• User Access Monitoring: The Menlo Secure Enterprise Browser solution can potentially provide insights into user activity related to data access attempts. This includes information about users, applications accessed, and data types involved. • Threat detection and prevention: The solution's analytics can identify suspicious data access patterns or potential malware activity that could indicate data security threats. • Browser forensics provides advanced investigative and analytical capabilities for historical data and user behavior.

Function	Maturity Alignment	Maturity Stage	Supporting Elements
Automation and Orchestration Capability	Client-driven	Client-driven	• Policy engine allows for automated access control decisions and responses based on configured policies.
Governance Capability	Client-driven	Client-driven	• Client-driven

Table 5: Solution support for ZTMM 2.0 data functions

Cross-cutting functions

Three additional capabilities cut across all ZTMM 2.0 pillars, forming the foundation for a holistic Zero Trust approach:

1. Visibility and analytics: This capability involves collecting and analyzing data from various security tools to gain insights into user activity, system behavior, and potential threats.
2. Automation and orchestration: This capability focuses on automating security processes and workflows to improve efficiency and consistency.
3. Governance: This capability involves establishing clear policies, standards, and procedures to govern security practices within the organization.

Complementary customer controls

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. Typically, this includes an in-depth approach that leverages other specialized technologies and security controls. In support of optimizing cross-cutting functions, customer should consider complementary, and often required, responsibilities supporting cross-cutting functions, including:

- Deploying a SIEM solution to collect and analyze security logs from various sources, including the Menlo Secure Enterprise Browser solution, and facilitate incident detection, investigation, and response.
- Providing ongoing security awareness and training to educate employees about cyber threats, best practices, and responsible use of applications and data.
- Establishing and implementing incident response for investigating, containing, and recovering from security incidents.
- Integration with a SOAR platform to automate broader security workflows across different security tools.
- Establishing processes for monitoring security alerts generated by the Menlo Secure Enterprise Browser solution and other security tools, investigating potential incidents, and taking appropriate action.
- Defining log retention policies for security data collected by the Menlo Secure Enterprise Browser solution and other tools to ensure compliance with regulations and facilitate incident investigations.
- Regularly conducting security assessments and audits of the overall security posture, including the Menlo Secure Enterprise Browser solution's configuration and effectiveness, to identify and address any weaknesses.

Solution support

The following provides a breakdown of how specific solution components contribute, categorized by corresponding ZTMM 2.0 function and maturity stage.

Function	Maturity Alignment	Maturity Stage	Supporting Elements
Visibility and Analytics Capability	Optimal	Agency maintains comprehensive visibility enterprise-wide via centralized dynamic monitoring and advanced analysis of logs and events.	• User access monitoring: Provides insights into user activity related to data access attempts across applications, including information about users, applications accessed, data types involved, and potential anomalies. • Threat detection and prevention: The solution's analytics can identify suspicious data access patterns or potential malware activity that could indicate security threats across applications. • Browser isolation: By isolating user sessions and data within a secure execution environment, the Menlo Secure Enterprise Browser solution allows for monitoring activity without compromising sensitive information. • The visibility gained from the Menlo Secure Enterprise Browser solution can inform security decisions and actions across various ZTMM 2.0 pillars.
Automation and Orchestration Capability	Client-driven	Client-driven	• Policy-based response actions: The Menlo Secure Enterprise Browser solution's policy engine can enable automated responses to security incidents detected during data access attempts within applications. This could include actions like quarantining suspicious files, blocking access attempts, or notifying security teams. • Potential integration with SOAR platforms can enable more complex automated workflows for handling security incidents across applications.
Governance Capability	Client-driven	Client-driven	• Client-driven

Table 6: Solution support for ZTMM 2.0 cross-cutting functions

Summary of capabilities supporting Zero Trust

Access and control

Zero Trust access and control is a foundational principle within the Menlo Secure Enterprise Browser solution, enabling organizations to adopt a proactive security posture that minimizes trust assumptions and enforces strict access controls. By integrating functionality such as CASB and FWaaS, the solution enables granular access controls and comprehensive user behavior monitoring, which helps mitigate insider threats, prevent data breaches, and ensure compliance with regulatory requirements.

Cloud Access Security Broker

CASB functionality within the solution provides visibility and control over cloud-based applications and services, enabling organizations to enforce security policies and mitigate risks associated with shadow IT and unauthorized data access. By integrating CASB capabilities, organizations can monitor user activity, detect anomalous behavior, and enforce granular access controls based on user roles, device posture, and application sensitivity.

Firewall-as-a-Service

FWaaS functionality extends traditional network security capabilities to the cloud, enabling organizations to establish secure network perimeters and enforce access policies for both on-premises and cloud-based resources. By leveraging FWaaS, organizations can define and enforce granular network security rules, restrict access to specific applications and services, and monitor network traffic for suspicious activity in real-time, ensuring robust protection against external threats and unauthorized access attempts.

Granular access controls

Zero Trust access and control functionality within the solution enforces granular access controls through the following mechanisms:

- Identity-based access policies: Users are authenticated based on their identity using MFA and other authentication methods, ensuring that only authorized users can access corporate resources.
- Device posture assessment: Devices accessing corporate resources undergo posture assessment to evaluate their security posture and compliance with corporate security policies. Devices that do not meet the minimum-security requirements are either denied access or granted limited access until remediation is completed.
- Contextual access policies: Access policies are enforced based on contextual attributes, such as user location, time of access, and type of device, ensuring that access privileges are dynamically adjusted based on changing risk factors and environmental conditions.
- Application sensitivity controls: Access to sensitive applications and data is restricted based on the sensitivity level of the application and the user's role within the organization. High-risk activities, such as data exfiltration and unauthorized access attempts, are detected and blocked in real-time.

User behavior monitoring

Zero Trust access and control functionality within the solution monitor user behavior through the following mechanisms:

- User activity logging: User activities, such as logins, access attempts, and data transfers, are logged and monitored in real-time, enabling organizations to detect and investigate suspicious behavior.
- Anomaly detection: Behavioral analytics and machine learning algorithms are used to identify anomalous user behavior patterns indicative of insider threats, compromised accounts, or unauthorized access attempts.
- Alerting and response: Security alerts are generated in response to detected anomalies or policy violations, triggering automated response actions such as access revocation, session termination, or user notification.
- Forensic analysis: Detailed audit logs and forensic data are collected and retained for compliance purposes, enabling organizations to reconstruct security incidents and conduct post-incident investigations.

Zero Trust access and control functionality within the solution enable organizations to enforce granular access controls and comprehensive user behavior monitoring to mitigate insider threats, prevent data breaches, and maintain regulatory compliance in a dynamic and evolving threat landscape.

Threat detection and prevention

The solution offers a unified approach to threat detection and prevention, leveraging a combination of core functions such as browser isolation, email isolation, Browser Posture Management, HEAT Shield, and threat rules to identify and mitigate threats effectively.

Browser isolation

The solution uses browser isolation as its principal threat prevention mechanism. By executing web sessions in secure, isolated environments, browser isolation prevents malicious code from reaching user devices, thereby eliminating the risk of drive-by downloads, zero-day exploits, and phishing attacks delivered through web browsers.

Email isolation

Email isolation extends the principles of browser isolation to email communications, ensuring that links and attachments in emails are processed in isolated environments to prevent malware infections, phishing attempts, and data breaches resulting from malicious email content.

Browser Posture Management

Browser Posture Management enhances security by enforcing strict browser security policies, such as disabling vulnerable plugins, blocking malicious scripts, and preventing unauthorized browser extensions. By ensuring that browsers adhere to security best practices, Browser Posture Management reduces the attack surface and mitigates the risk of browser-based threats.

HEAT Shield

HEAT Shield dynamically analyzes each browser session, examining both what the user sees and what they cannot see, applying AI / 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.

Threat rules

Threat rules enable organizations to define and enforce security policies based on threat intelligence, user behavior, and contextual attributes. By creating custom threat rules, organizations can detect and block suspicious activities, such as unauthorized access attempts, data exfiltration, and malware downloads, in real-time.

Unified defense against threats

Th The solution integrates these core functions to provide a unified defense against evolving threats:

- Prevention: By isolating web and email content, enforcing browser security policies, and analyzing web page elements for malicious indicators, the solution prevents threats from reaching user devices and networks, thereby reducing the likelihood of successful cyberattacks.
- Detection: Through continuous monitoring of user activity, analysis of web and email content, and application of threat intelligence, the solution detects suspicious behavior, anomalous activities, and known indicators of compromise, enabling organizations to identify and respond to threats in real-time.
- Response: Upon detection of a potential threat, the solution triggers automated response actions, such as blocking access to malicious websites, quarantining suspicious email attachments, and notifying security teams for further investigation and remediation. By orchestrating response actions, the solution minimizes the impact of security incidents and reduces the time to resolution.
- Adaptation: The solution continuously evolves to adapt to new and emerging threats, incorporating the latest threat intelligence, security best practices, and machine learning algorithms to enhance its detection and prevention capabilities and help ensure that organizations remain resilient and prepared to defend against cyberattacks.

Data loss prevention

Last-Mile Data Protection and Secure Web Gateway play key roles in preventing data loss and maintaining ZTA objectives. When integrated, these solutions provide defense against data exfiltration threats.

Last-Mile Data Protection

Last-Mile Data Protection focuses on safeguarding data at the endpoint, ensuring that sensitive information remains secure, even as it travels outside the organization's network perimeter.

- Content inspection: Last-Mile Data Protection solutions inspect outbound network traffic, email communications, and file transfers in real-time, identifying sensitive data based on predefined policies and patterns.
- Policy enforcement: Once sensitive data is identified, Last-Mile Data Protection solutions enforce policy-based actions, such as blocking, quarantining, or encrypting data to prevent unauthorized access and exfiltration.
- User behavior monitoring: Last-Mile Data Protection solutions monitor user behavior and interactions with sensitive data, detecting anomalous activities and potential data breaches in real-time.
- Data encryption: To protect data in transit, Last-Mile Data Protection solutions encrypt sensitive information before it leaves the organization's network, ensuring confidentiality and integrity during transmission.

Secure Web Gateway

The Secure Web Gateway solution functions as the gatekeeper between internal users and the internet, monitoring and controlling web traffic to enforce security policies and protect against web-based threats. Key features of Secure Web Gateway include:

- URL filtering: Secure Web Gateway solutions filter web traffic based on URL categories, blocking access to malicious or unauthorized websites known to host malware, phishing scams, or other threats.
- Content filtering: Secure Web Gateway solutions inspect web content in real-time, scanning for malware, ransomware, and other malicious payloads embedded within web pages, downloads, or scripts.
- SSL/TLS inspection: Secure Web Gateway solutions decrypt and inspect encrypted web traffic to detect and block threats hidden within SSL/TLS-encrypted connections, ensuring comprehensive protection against advanced threats.
- DLP integration: Secure Web Gateway solutions integrate with Last-Mile Data Protection solutions to extend data protection capabilities beyond the organization's network perimeter, preventing data exfiltration through web-based channels.

Integration for comprehensive data protection

When Last-Mile Data Protection and Secure Web Gateway solutions are integrated, they provide comprehensive protection against data exfiltration threats:

- Unified policy enforcement: Integration enables unified policy enforcement across endpoints and web gateways, providing consistent protection and minimizing the risk of data leakage or unauthorized access.
- Contextual awareness: By correlating data loss events with web activity and user behavior, integrated solutions provide contextual awareness, enabling more accurate detection and prevention of data exfiltration attempts.
- Real-time response: Integrated solutions facilitate real-time response to data loss events, triggering automated actions such as blocking access to malicious websites, encrypting sensitive data, or alerting security teams for further investigation and remediation.

- Compliance assurance: By enforcing data protection policies at the endpoint- and web gateway-levels, integrated solutions help organizations maintain compliance with industry regulations and data privacy standards, reducing the risk of regulatory fines and penalties.

The integration of Last-Mile Data Protection and Secure Web Gateway solutions provides defense against data exfiltration threats by extending data protection capabilities beyond the organization's network perimeter. By enforcing unified policies, providing contextual awareness, facilitating real-time response, and ensuring compliance with regulatory requirements, these solutions can help organizations safeguard sensitive data and maintain a Zero Trust-aligned security posture.

Compliance management

The solution offers robust compliance management capabilities to assist organizations in meeting their data privacy obligations.

Data privacy regulations

Data privacy regulations, such as the GDPR, California Consumer Privacy Act (CCPA), HIPAA, and others, impose strict requirements on organizations regarding the collection, storage, processing, and transfer of personal and sensitive data. Key provisions of these regulations include:

- Data protection: Organizations must implement measures to protect personal data from unauthorized access, disclosure, alteration, or destruction, to ensure confidentiality, integrity, and availability.
- Consent management: Organizations must obtain explicit consent from individuals before collecting, processing, or sharing their personal data to provide transparency and control over data usage.
- Data breach notification: Organizations must promptly notify affected individuals and regulatory authorities in the event of a data breach, enabling timely response and mitigation efforts to minimize the impact on individuals' privacy rights.
- Privacy by design: Organizations must incorporate privacy and data protection principles into their systems, processes, and products from the outset to integrate privacy controls and safeguards into all aspects of their operations.

Solution capabilities for compliance management:

The solution offers a range of capabilities to assist organizations in achieving compliance with data privacy regulations:

- Data encryption: The solution provides robust encryption capabilities to protect sensitive data in transit, supporting compliance with encryption requirements mandated by data privacy regulations.
- Data loss prevention: Integrated DLP features enable organizations to identify, monitor, and protect sensitive data across endpoints, networks, and cloud applications, preventing unauthorized access, sharing, or exfiltration of sensitive information.
- Policy-based controls: The solution allows organizations to define and enforce granular security policies based on regulatory requirements, ensuring consistent application of access controls, data protection measures, and threat prevention mechanisms.
- Audit and reporting: Comprehensive audit logs and reporting functionality provide visibility into security events, user activities, and policy enforcement actions, facilitating compliance monitoring, audit trails, and regulatory reporting requirements.

- User awareness and training: The solution includes features for user awareness and training, such as security awareness modules, simulated phishing exercises, and compliance training courses, allowing organizations to educate employees about data privacy best practices and regulatory requirements.
- Regulatory mapping: The solution offers regulatory mapping capabilities, allowing organizations to align their security controls, policies, and procedures with specific data privacy regulations to help ensure adherence to regulatory requirements and industry standards.

Benefits of compliance management with the Menlo Secure Enterprise Browser solution

Use of the solution can offer a range of compliance management benefits for organizations:

- Reduced compliance risk: By leveraging the solution's comprehensive compliance management capabilities, organizations can reduce compliance risk, mitigate potential regulatory violations, and avoid costly fines, penalties, and the reputational damage associated with non-compliance.
- Streamlined compliance processes: The solution streamlines compliance processes through automated policy enforcement, centralized management, and audit-ready reporting functionality, enabling organizations to achieve and maintain compliance.
- Enhanced data protection: By implementing robust security controls, encryption mechanisms, and DLP measures, organizations can enhance data protection and safeguard sensitive information against unauthorized access, disclosure, or misuse, ensuring compliance with data privacy regulations.
- Improved security posture: Compliance management efforts contribute to an organization's overall security posture by promoting best practices, risk awareness, and continuous improvement in security policies, procedures, and technologies, helping to mitigate cyber threats and protect against data breaches.

By leveraging these capabilities, organizations can reduce compliance risk, streamline compliance processes, enhance data protection, and improve Zero Trust-aligned security posture.

Conclusion

Coalfire has determined that the Menlo Security Secure Enterprise Browser solution aligns with core Zero Trust principles, with its strengths lying with access control, user behavior monitoring, and application security. The solution's unified approach (including CASB, DLP, and FWaaS functionality) demonstrates a broader reach towards data protection and network segmentation.

Achieving optimal Zero Trust posture 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 aligns with the ZTMM 2.0 framework and highlighted the customer responsibilities that are crucial for successful implementation.

By understanding these alignments and responsibilities, organizations can leverage the Menlo Secure Enterprise Browser solution strengths while implementing additional security controls and processes to achieve a holistic ZTA. This layered approach, combining solution capabilities with customer commitment to best practices, can empower organizations to minimize trust assumptions, enforce granular access controls, and continuously improve their security posture.

Legal disclaimer

Additional information, resources, and references

Zero Trust resources

- The CISA Zero Trust Maturity Model provides the official ZTMM 2.0 framework and guidance from CISA:
  - https://www.cisa.gov/zero-trust-maturity-model
- NIST Special Publication 800-160 Rev. 2 Zero Trust Architecture offers a technical definition and considerations for implementing Zero Trust:
  - https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-207.pdf
- NIST Cybersecurity Framework provides a broader framework for managing cybersecurity risk, which can be aligned with Zero Trust principles:
  - https://www.nist.gov/cyberframework

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 Zero Trust:
  - 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_ZTMM_2024