

G CLOUD

Menlo Security

 **BARRIER**

ABOUT

At Barrier, our mission is to help our customers build cyber resilience and develop strategies to defend against cyber-attacks. We have developed a portfolio of services and solutions that suit customers small and large, in both the private and public sector. Our portfolio encompasses security consultancy, solutions from innovative vendors to mitigate attacks, through to managed services that pro-actively detect attacks and provide swift incident response measures.

We have built a practice dedicated to providing assurance that systems are resilient to attack. We provide penetration testing services to check the effectiveness of the deployed controls against real-world attacks and we can implement a vulnerability management system to maintain levels of operational resilience.

Our aim is to build trust and understanding of how our customers' organisation functions. Our work takes us across all sectors, with strong references in the Finance Sector, Legal, HMG, MOD and the Public Sector.

Established in 2006, we are a cyber security focused solutions and service provider. Our customers trust Barrier as a strategic part of their cyber security team and here's why:

- Our knowledge of the cybersecurity industry helps select the right solutions
- Our experience helps organisations build cohesive cyber resilience strategies
- Our people are empowered to work closely with our customers to forge strong partnerships
- Our services become an intrinsic part of our customer's security operations

The copyright in this work is vested in Barrier Networks Limited and the document is issued in confidence for the purpose for which it is supplied. It must not be reproduced in whole or in part or used for tendering or manufacturing purposes except under direct agreement or with the consent in writing of Barrier Networks Limited.

No information as to the contents or subject matter of this document or any part thereof arising directly or indirectly therefrom shall be given orally or in writing to any third party, being an individual firm or company, or any employee thereof without the prior consent in writing of Barrier Networks Limited.

©Barrier Networks Limited 2022
Barrier Networks Limited
272 Bath Street, Glasgow, G2 4JR
Tel: 0141 356 0101

**SECURED.
ASSURED.**

1 CONTENTS

1	Contents	3
2	Executive summary.....	4
3	Menlo pLatform architecture	4
4	Common use cases for RBI	8
5	Menlo cloud security pillars	9
5.1	Manage	10
5.2	Protect.....	13
5.3	Secure	17
6	Menlo security cloud platform bundles	21
7	Menlo security customer support	23

2 EXECUTIVE SUMMARY

The way people work and connect to the network is changing. The borders of an enterprise are fading, and employees need to be enabled with connectivity and security from all locations. Company data is more vulnerable than ever to leaks or theft as people work and communicate using an ever-increasing number of apps, devices, and platforms. Menlo Security redefines security with its Isolation Core™ architecture that overcomes the deficiencies of traditional detection-based security platforms which leave organisations open to attack.

Menlo Security was founded in 2013 to enable the world to connect, communicate and collaborate securely without compromise. Using a fundamentally different approach, Menlo Security eliminates the threat from Malware completely, fully protecting productivity with a one-of-a-kind, isolation-powered cloud security platform. It's the only solution to deliver on the promise of cloud security - by providing the most secure zero-trust approach to preventing malicious attacks and removing the guesswork from security.

Detect-and-prevent has reached its potential, and attackers have learned how to bypass it. These solutions are prone to False Negatives and Positives, they're costly to implement and come with a high operational overhead. Cyberattacks are becoming more sophisticated and increasingly targeted; detect-and-prevent cannot maintain pace and the average time to contain or remediate is still measured in a magnitude of months.

3 MENLO PLATFORM ARCHITECTURE

Superior Architecture by Design

The Menlo Security Isolation Platform (MSIP) eliminates the possibility of malware reaching user devices via compromised or malicious Websites, weaponised documents or via phishing and credential harvesting attacks. The user's entire web session (including all active content e.g., JavaScript etc.) is fully executed and contained within the Isolation Core™. Only completely safe, malware-free rendering information is delivered to the user's endpoint.

The patented Menlo Security content-rendering technology, called Adaptive Clientless Rendering™ (ACR), provides a user experience that is identical to native browsing on the desktop. ACR technology requires no endpoint software or plug-ins.

For each browsing session the following occurs:

- A new Disposable Virtual Container (DVC) is initiated
- A new browser in the DVC browses on behalf of the end user to the target website
- All content from the website is fetched & executed within the DVC
- Only 100% safe rendering instructions are sent to the user's browser
- The DVC is destroyed when the web session is complete e.g. when the tab is closed
- No information from that browsing session is stored in the MSIP Cloud

ACR leverages the fact that all modern browsers use a common framework for describing the elements on a web page (text, graphics, video, etc.). When web content executes normally in a user's browser it generates document object model (DOM) elements and an associated rendering tree that tells the browser how to create the user's display. When a web session is executed in the MSIP it also generates DOM and rendering tree information which is then optimized and delivered via the ACR protocol to the user's browser. The user's browser takes the information delivered via the protocol and generates the user's view as if the content were executing in the local browser.

ACR coupled with the Menlo Security Global Cloud's ability to automatically scale, allows customers to easily deploy RBI across unlimited numbers of users for each web request without performance degradation or user experience issues.

Other Enterprise Browsers typically require the installation of a new Chromium-based local browser to replace all other browsers. In this architecture, potentially malicious content is still downloaded and executed on the endpoint, the new local browser must be supported from an operational standpoint, it's vulnerable to all Chromium CVEs, provides savvy users with tampering options for last mile DLP and is a substantial change for end user experience.

Menlo Security is unique in the fact that we provide the only Cloud Based Enterprise Browser, which integrates seamlessly with existing local browser. This architecture is secure by design, providing true RBI rather than Process Isolation and does not suffer from any of the negative points above.

Menlo Security is deployed on Amazon Web Services (AWS) and leverages ISO27001 and SOC-2 accredited data centres globally. Details of [AWS Security Processes](#) can be found online. The Menlo Security Global Elastic Cloud was built from the ground up for unlimited elastic scalability. Menlo monitors crucial components of the architecture, automatically adding or subtracting resources as load dictates across redundant data centres. All clusters scale elastically, ensuring immediate and transparent failover between regional data centres with independent power and redundant connectivity.

Menlo Security is deployed on Amazon Web Services (AWS) and leverages ISO27001 and SOC-2 accredited data centres globally. Details of [AWS Security Processes](#) can be found online. The Menlo Security Global Elastic Cloud was built from the ground up for unlimited elastic scalability. Menlo monitors crucial components of the architecture, automatically adding or subtracting resources as load dictates across redundant data centres. All clusters scale elastically, ensuring immediate and transparent failover between regional data centres with independent power and redundant connectivity.

Operating currently in 29 geographical AWS Availability Zones, each comprised of numerous physical data centres.

- **EU:** London, Dublin, Paris, Frankfurt, Milan, Stockholm, Zurich
- **ME:** Bahrain, UAE, Tel Aviv
- **Africa:** Cape Town
- **APAC:** Singapore, Mumbai, Hong Kong, Sydney, Seoul, Jakarta, Hyderabad, Melbourne
- **Japan:** Tokyo, Osaka 1 and Osaka 2
- **Americas:** Virginia, California, Oregon, Ohio, Canada, Sao Paulo

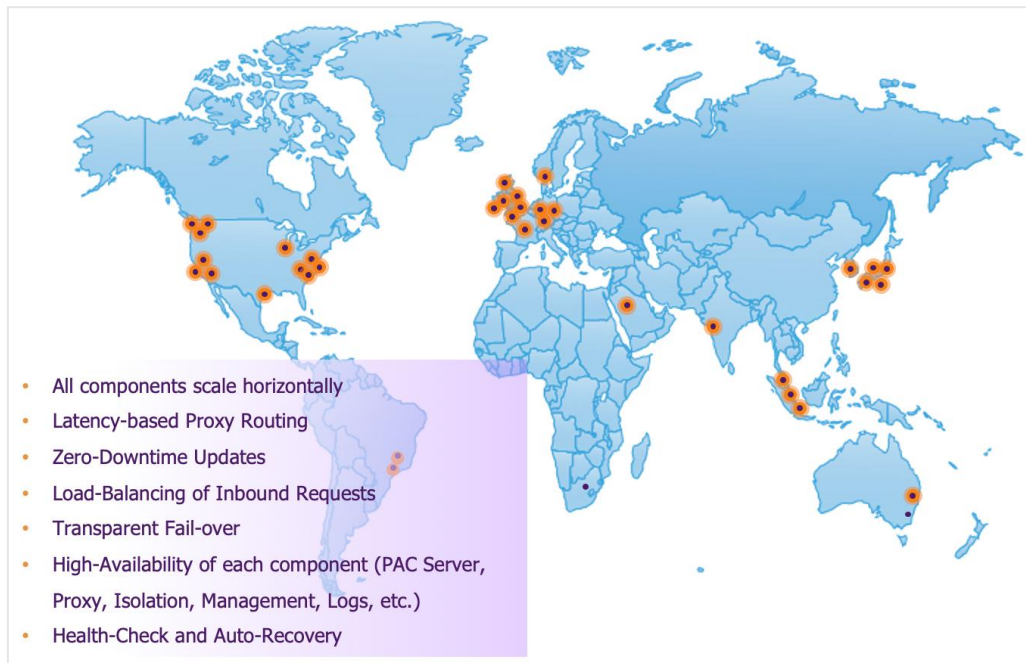


Figure 1 Menlo Security Global Elastic Cloud

High availability is achieved through complete redundancy in every region with transparent failover across multiple data centres and regions. A stateless design delivers seamless session continuity for users traveling between service regions. Geo- and latency-based routing logic ensures that users are guaranteed to always access the best region based on their location. A dynamic session management model allows new updates to be rolled out to customers without any service interruption or downtime.

Menlo takes a unique approach to Service Updates and Patch Management. We never upgrade or apply a patch to the live environment. This completely mitigates the risk of service disruption or downtime for customers.

New software versions are deployed side by side with the current running version and customers are transparently moved across in batches to the new version. For patching, each component in the Isolation Platform is an Amazon Machine Image (AMI), these are never patched. New AMIs that include the patches are deployed alongside the unpatched AMIs, at which point the unpatched AMIs are cycled out of production. All software upgrades and patching is completely transparent to all

Menlo Security Global Cloud customers. Service Availability is guaranteed by Service Level Agreement (SLA), currently 99.9%.



Demand-based Autoscale

No capacity planning required
System automatically adapts
to traffic bursts



Stateless Session Portability

Uninterrupted browsing for
roaming users

Figure 2 key differentiators for Menlo Security

Menlo Security Global Cloud provides a range of Business Benefits and Return on Investment (ROI) around cloud adoption. For instance, reducing expenditure on Physical Hardware or Appliances and not having to manage, maintain, upgrade and provision these environments locally. As well as reductions in MPLS and VPN bandwidth costs.

From a Security standpoint typical Business Benefits are listed below.

Business Benefits	Key Metrics
Reduce Web Based Malware Containment Cost	# of Web Based Malware Incidents, Cost Per Incident
Reduce Endpoint Device Reimaging Cost	# of Endpoint Device Re-imaging Events
Reduce Malware Remediation Cost	# of Endpoints Affected by Malware Attacks
Reduce Costs of Handling Endpoint Alerts	# of Alerts, Cost Per Alert
Improve Security Operations Efficiency	# of Security Operations Staff FTE

Reduce Help Desk Recategorization Cost	# of Recategorization Requests
Reduce Consulting Remediation Cost	# of Consulting Engagements
Reduce Patching Cost	# of Unscheduled Patching Events
Protect Revenue Loss Due to Infections	# of Breach Events
Mitigate Destructive Attack / Extortion Risk	# of Ransomware Breaches
Mitigate Brand / PR Damage Risk	# of Breach Events

4 COMMON USE CASES FOR RBI

Use Case	Description
Eliminate Drive-by Malware Exploits	Menlo Security Isolation Platform (MSIP) eliminates the path that drive-by malware would use to reach the user. All web requests are opened in Disposable Virtual Containers (DVC) in the Menlo Security Isolation Platform (MSIP). Only completely safe Rendering instructions and sanitized resources are transferred from the DVC to the user. No active content will ever reach the user, and as a result, there is no chance for the user to be infected. All information, and the DVC itself, is destroyed at the end of the browsing session. No data from the session is stored.
Protection against Malicious or Weaponized Documents	Menlo Security transcodes original documents from 33 different formats into a HTML5 version in real time. All text, images, formatting, and other content is extracted from the original document and built into a HTML5 version, called the SafeVersion. As such, embedded malicious code or payloads in the original documents never make it through to their target i.e., the user. The user can view, interact, or download the SafeVersion in PDF format, completely Risk free. Additionally, this includes Password Protected MS Office, Adobe PDF, and Compressed Archives.
Ensure no Active Content can reach the end user	Menlo Security Isolation creates a logical air gap between the user and the Internet. Threat Actors have no way to transmit active content to unsuspecting users. This includes all potentially active or Risky content: - JavaScript and/or Exploit Code - Images and Fonts with embedded code

	- Weaponised Documents MSIP sanitizes all resources included in the Document Object Model (DOM) that are then synchronised to the client using Menlo Security's patented Adaptive Clientless Rendering (ACR) technology. This includes Images, fonts and CSS files.
Maintain the same end user experience whilst improving Security	Menlo Security Isolation does not try to determine whether content is malicious or not, rather assuming that all content is risky and performing Isolation to remove any Risks. This zero-trust model ensures that all content is treated the same and the platform as such does not suffer from false positives nor negatives. MSIP must however be able to perform at scale without any performance degradation. Maintain the user experience and browser functions such as copy, cut, paste, print, etc. As well as supporting multiple Web Browsers as deployed by the organisation. MSIP must as close as possible provide complete security whilst being transparent to users.

5 MENLO CLOUD SECURITY PILLARS

Menlo Security Cloud Security Platform is made of three core pillar's providing a new paradigm in Securing the Enterprise Browser

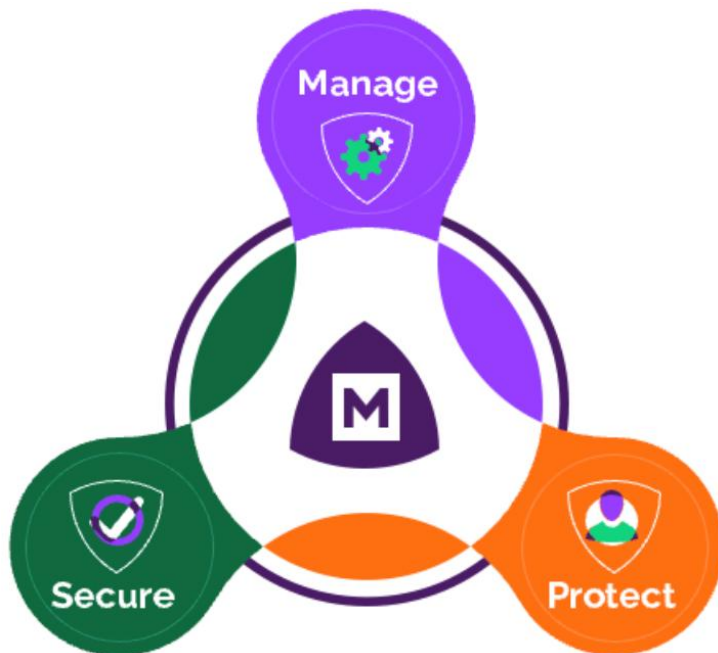
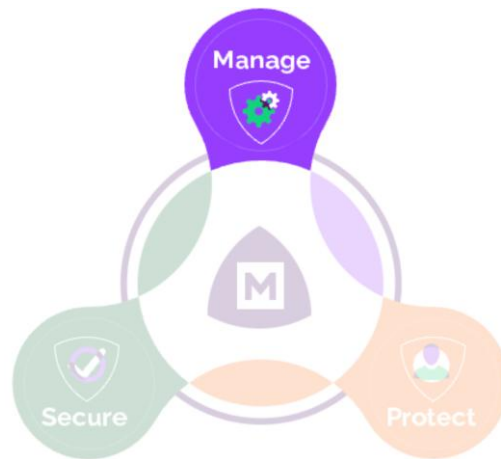


Figure 1 the Menlo Security Secure Access Service Edge (SASE) architecture built on an Isolation Core

Menlo's Secure Cloud Based Enterprise Browser platform enables organisations to use existing browser environments without fear of compromise be that from internal external threats. Menlo Security firmly believes that organisations can use their existing browsers to access both external and internal content and applications securely without compromise. Menlo security breaks these down into 3 core service pillars.

5.1 MANAGE

Eliminate the browser attack surface with simple-to-deploy security policy and end-to-end visibility.



Organisations operate with hundreds of different browser-policy options that can be hard to deploy without tools, and changes can disrupt the end user experience. **The Menlo Security Browser Posture Manager** delivers forensic visibility into the browser and deploys browser security policy automatically. Closing the browser management gap and opening up browser visibility eliminates the risk associated with the browser attack surface.

Manage Products include:

- **Browser Posture Manager**
- **Browsing Forensics**

Menlo Security Browser Posture Manager

Reduce your organization's attack surface with proven, benchmarked policies. The need to secure enterprise browsers has never been higher, as bad actors are increasingly targeting vulnerable browsers with Highly Evasive and Adaptive Threat (HEAT) attacks.

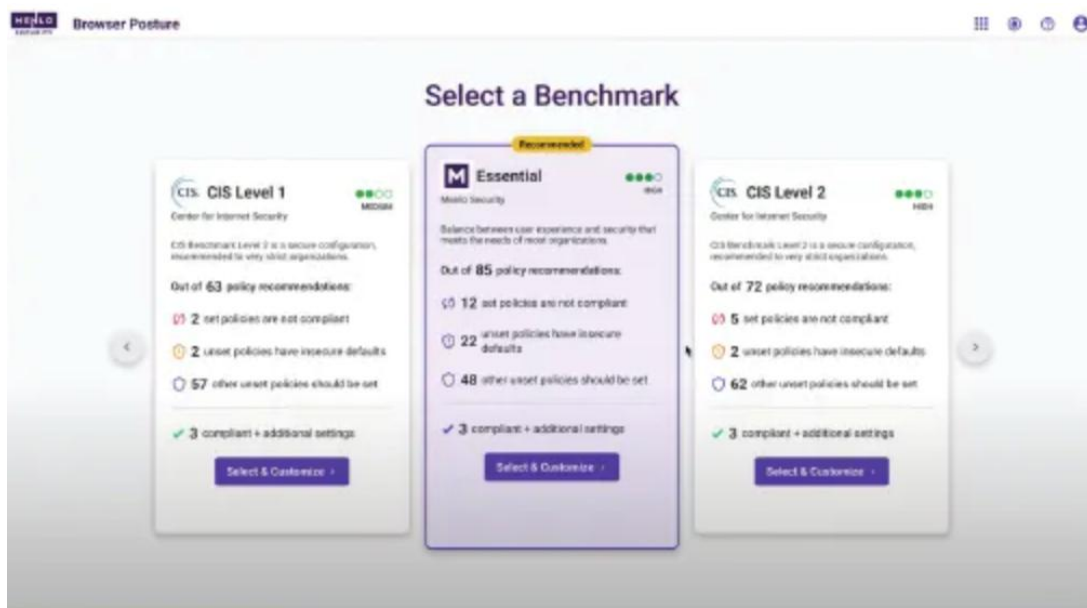
Despite the fact that the browser is understood to be the most widely used application in business, most enterprises struggle to manage it well. A big part of the problem is what "managing the browser" actually entails. Google Chrome has thousands of policies, of which a tiny fraction are typically enforced.

The stats on Microsoft Edge are similar; out of thousands of policies just a few dozen are enforced on average. With that amount of policies to consider, it is impossible for oversubscribed security teams to know exactly which are important. The result is that about 45% of browser configurations return errors, while over 60% have explicit extension policies.

Browsers provide the initial foothold for cyber adversaries. With the rising frequency and complexity of threats targeting the browser, particularly those classified as HEAT attacks, the need to secure the browser attack surface has become increasingly critical. Menlo Security Researchers observed a 206% increase in attacks classified as evasive. With so many changes continuously occurring within browsers, it is extremely difficult to keep up.

The good news is that with Menlo Browser Posture Manager, you don't have to. Menlo is constantly monitoring changes to browsers, and it enables you to compare how you stand against updated benchmarks anytime.

Menlo Security, the leader in enterprise browser security, makes the process easy and automatic with our new Browser Posture Manager. With a few clicks, you can see exactly how your browser security policies compare with a variety of policy benchmarks. Security teams only need to upload a configuration file, and Menlo Security will compare what you have in place with known best-in-class configurations.



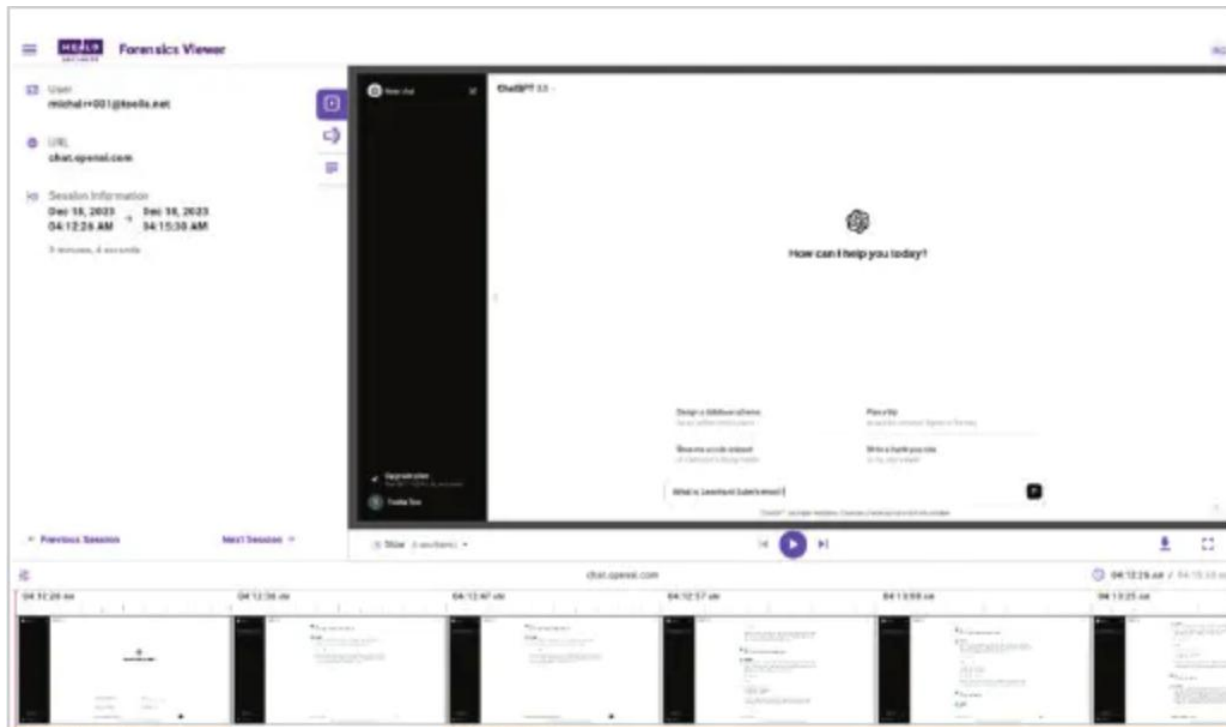
Not only will Menlo call out the disparity between your browser configuration and best practice benchmarks, but we will provide specific suggestions regarding what to change in order of possible security ramifications.

Browsing Forensics

Menlo Security Browsing Forensics records policy-defined browser sessions to support customer teams with the investigation of security, audit / compliance, HR and other necessary events. The

recordings are based on policy triggers, such as Heat Shield detections or users accessing private or sensitive applications. Each recorded session has a Menlo Forensics Log entry that includes supporting data of the event and one-click access to the recording. The Forensics log data, available in near real time, includes a link to the associated recording.

The recorded sessions are transferred to a customer's defined location for secure, access-controlled storage. Browsing Forensics supports both AWS and Azure storage options. A summary of the Browsing Forensics recording is included in logs with a link to the recording. With one click the researcher is viewing the browsing session data, significantly reducing the time required to complete an investigation.



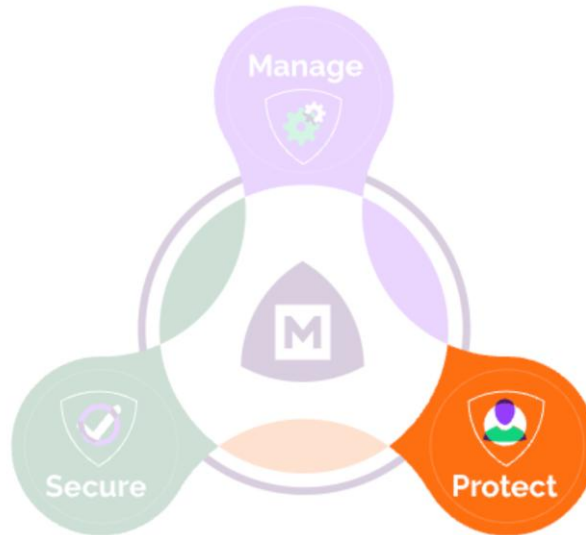
The Menlo Security Browsing Forensics Viewer presents the rich content of the recording, enabling analysts to reach substantiated conclusions quickly and easily.

Some of the use cases for Browsing Forensics include:

- Phishing Incident Response
- Data Security
- Threat Hunting
- Generative AI Visibility
- Copy & Paste Controls
- Security Research
- Insider threat
- Audit & Compliance

5.2 PROTECT

Protect the user, defend your enterprise. With Menlo Isolation Core



The Menlo Secure Cloud Browser (isolation core) and Menlo HEAT Shield stop threats cold, protecting users from browser-based threats. Menlo Security stops zero day web exploits and other evasive attacks, including the tactics that legacy security tools cannot stop. Menlo HEAT Shield shrinks the existing risk gap and brings modern protections to every single user, no matter where they work. Protect Products include:

- **Secure Cloud Browser**
- **HEAT Shield**
- **Email Security**

Secure Cloud Browser

The Menlo Security Secure Web Browser utilises Menlo's Isolation Core™ and works by simply moving the execution point of active content away from the end user's web browser to our Remote Browser in a Disposable Virtual Container (DVC) - effectively creating an "air gap" between the Internet and the end user. Only sanitized, nonexecutable content is rendered safely in users' devices, providing a completely safe yet seamless and transparent user experience. Any breaches or attacks are completely isolated away from the endpoint and user.

Delivered as a Public Cloud solution or as a Private Cloud, Menlo Security is a trusted security partner of some of the world's largest enterprises and government agencies including the US Department of Defense¹, 8 of the top 10 Global Banks and 4 of the top 5 major Credit Card companies. The Menlo Security Global Elastic Cloud isolates hundreds of million websites per day, with over 6 million users on the platform at any point in time.

¹ [*U.S. Department of Defence Leads the Industry with Cloud-Based Internet Isolation Program*](#)

Secure Cloud Browser key capabilities:

Proactive protection against zero-day browser exploits:

Rather than the user's browser accessing websites directly, each web request is sent and executed inside the Menlo Secure Cloud Browser, and only a safe, clean version is brought down to the user's browser. This closes the window of exposure from zero-day browser exploits for all browsers and endpoints ensuring that customers are fully protected before patches are even released or deployed.

Zero-touch code protection:

The Menlo Secure Cloud Browser removes any malicious, dynamic content or payloads, such as JavaScript or smuggled code, from executing locally on the endpoint, protecting against advanced malware used to evade traditional security tools.

Complete end-to-end browser visibility:

Evasive threat intelligence and actionable alerts are delivered to SOC teams for real time visibility and improved incident response. Detailed threat intelligence and browser forensics can be integrated into existing log aggregation, automation and security orchestration tools for improved optimized performance.

Inline AI-powered protection:

With Menlo, each web request is executed in the Secure Cloud Browser, enabling AI-based real-time analysis of each page, including DOM elements, logos and URL path. If a phishing or malware threat is detected, dynamic policy controls can block the site outright or render the page in read-only mode, preventing any data input.

Multi-layered content inspection:

The Menlo Secure Cloud Browser inspects password protected files, provides malware analysis for documents, and converts files into safe PDFs by applying anti-virus, file hash look up, cloud sandboxing, and file handling policies.

Secure cloud document & archive viewing:

Open and view any document safely in our secure document and archive viewer without the need to download files to the endpoint. This provides safe viewing of document and archive content, including nested and password protected archives without them ever touching the endpoint.

User/Group policy and authentication control:

Set and fine-tune policies and exception requests for specific users, user groups or content type (all content, risky, uncategorized). Integrates with SSO and IAM solutions with SAML support for user authentication.

Integrated browser forensics:

Incident Response teams can use the Browser Forensics tool for high-fidelity browser session recording to view a complete visual timeline of user browsing sessions including screenshots, user inputs and page resources.

HEAT Shield

Menlo Security manages browsers, protects your users, and secures access to applications and enterprise data, while providing a transparent browser security experience for any browser, across any device.

Menlo Security HEAT Shield puts AI-powered “eyes” on browser activity and dynamic web content, so users can focus on work, not threats.

By providing a complete picture into each web session and enabling dynamic policy controls, HEAT Shield eliminates the browser attack surface and brings modern protections to every single user, no matter where they work. HEAT Shield leverages AI-powered analysis and computer vision capabilities to prevent phishing attacks and provides comprehensive visibility into evasive threat signals from inside the browser, a telemetry source that is invisible to traditional network security tools.

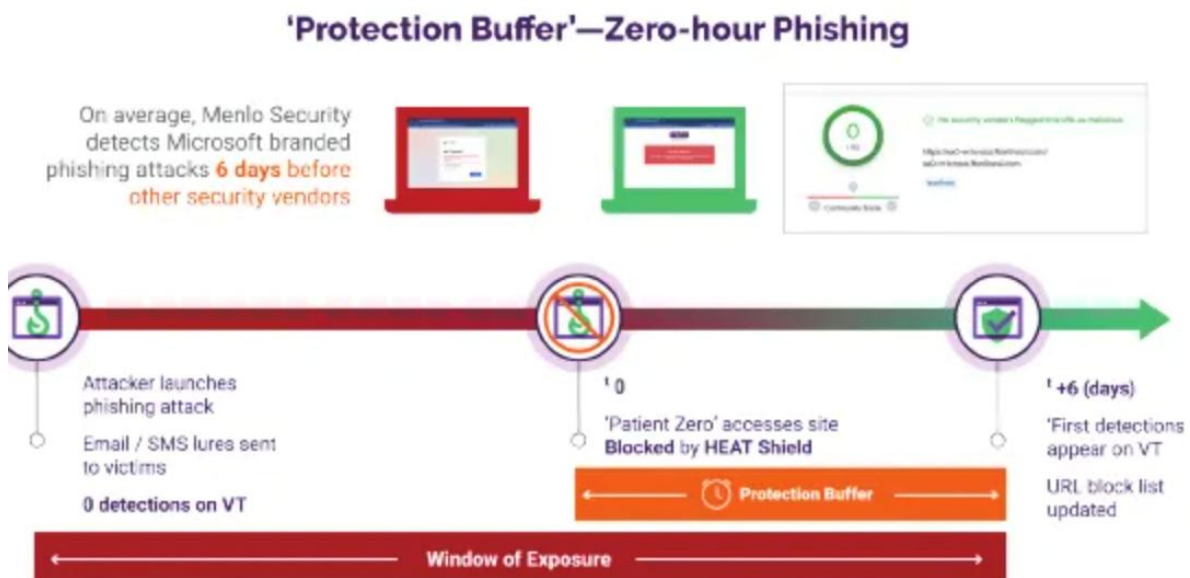
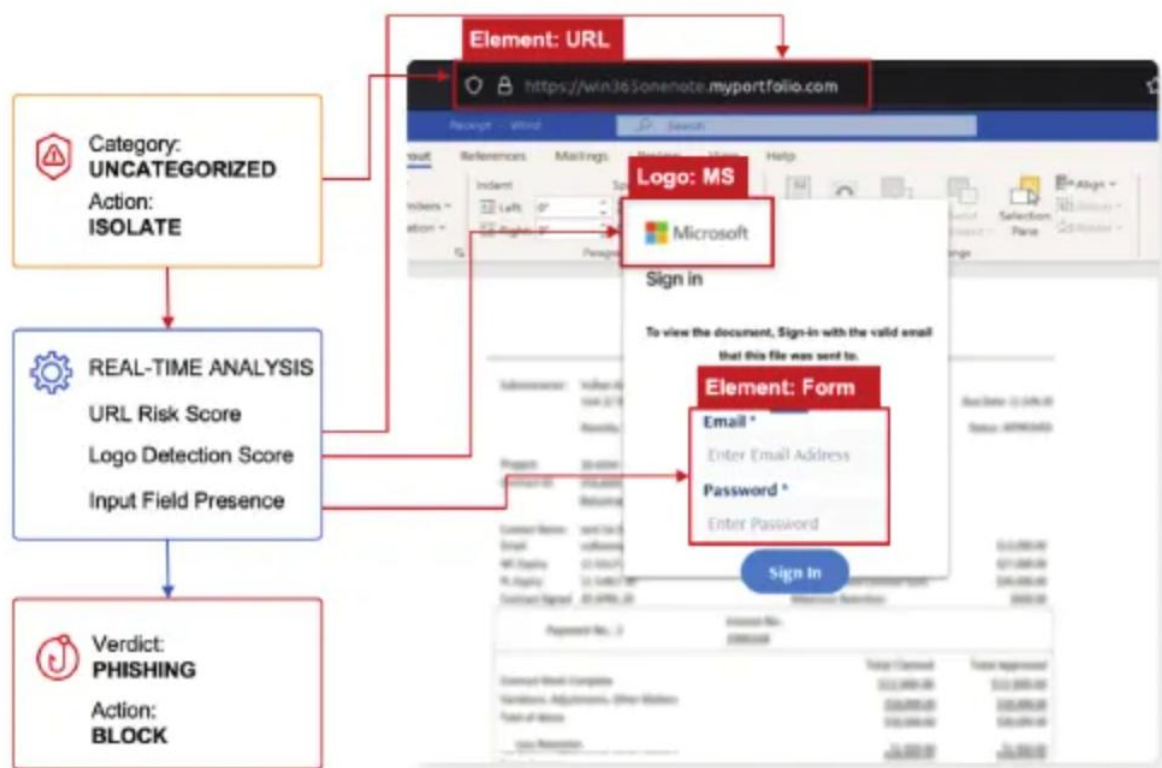


Illustration 1: The protection buffer from Menlo Security protects against zero-hour phishing attacks

Based on this telemetry, Menlo Security mitigates even the most sophisticated phishing attacks, detecting them well before traditional feeds based on indicators of compromise (IOC) and other approaches. HEAT Shield uses real-time dynamic controls to shrink the exposure window by as much as six days, providing an unmatched protection buffer. HEAT Shield intelligence is generated from analysing more than 400 billion sessions annually to enable real-time protection against browser-based threats and to improve overall security.

Enterprises can be assured that they're protected against zero-hour phishing attacks when HEAT Shield is activated. Granular access and security policies are enforced, and web sessions are monitored and protected, providing a risk-free internet experience for users. HEAT Shield supports policy compliance across all devices and locations because it leverages the Menlo Secure Cloud Browser to defend against evasive threats.



Example how HEAT Shield works against an uncategorized website

HEAT Shield key capabilities:

Zero-day exploit protection:

Rather than a local browser accessing websites directly, each web request from the user executes inside the Menlo Secure Cloud Browser. Only safe, clean content is delivered to the user's local browser. This approach prevents any malicious activity from ever reaching the endpoint.

AI-powered On-click inspection:

Each web request is executed in the Secure Cloud Browser, enabling AI-based runtime analysis of each page, including JavaScript, DOM elements, logos, input fields, and URL paths. If a phishing or malware threat is detected, dynamic policy controls can block the site outright or render the page in read-only mode, preventing any data input.

Real-time logo detection:

HEAT Shield uses computer vision to identify websites impersonating known brands and services. Computer vision-based classification provides fast and accurate protection at scale against dynamic attacks that trick users with images. Custom logos are supported to protect users against attacks targeting your organization.

Zero-hour phishing protection buffer:

Menlo Security mitigates the threat of zero-hour phishing attacks by detecting such attacks before other security vendors and threat-intel feeds, in some cases up to six days, using real-time dynamic policy controls.

End-to-end browser visibility:

Provides evasive threat intelligence and alerting for real-time visibility and improved incident response. Detailed threat intelligence and alerts can be viewed via a dedicated dashboard inside the Menlo Security admin portal, as well as consumed via API directly by your SIEM/SOC tools for improved performance.

Effortless deployment, ease of management:

Menlo HEAT Shield is simple to deploy and manage, supporting any browser on any device and allowing users to continue working with their browser of choice. There's no new endpoint software for IT to manage. After activation, enforcement actions can be easily defined and monitored inside the admin portal.

Globally available:

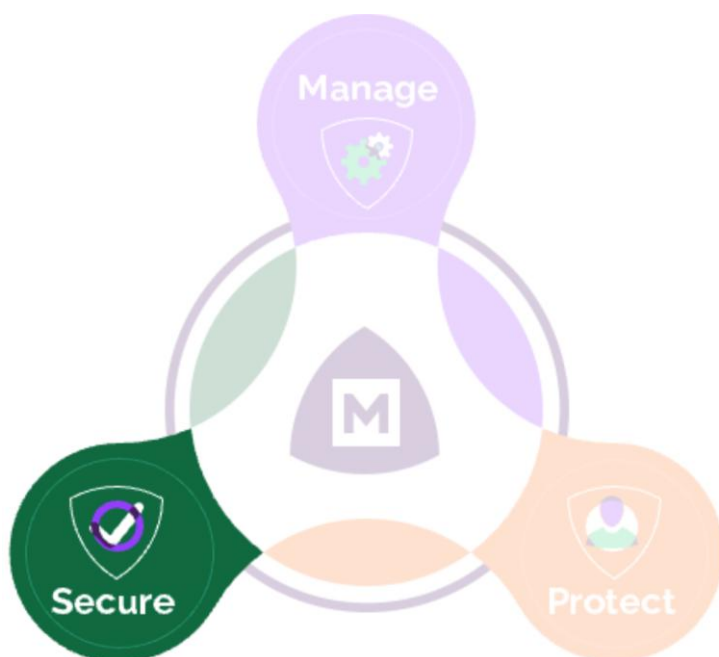
HEAT Shield scales seamlessly across >50 global points of presence (PoPs), providing security coverage throughout 145 countries and territories.

Menlo Email Isolation

Menlo Security Email Isolation preserves the native user experience by integrating easily with existing mail server infrastructures such as Exchange, Office 365, Gmail, and most other webmail offerings. It does this without disrupting existing workflows and while giving users a consistent email experience that's no different than before. In addition, users can click or open anything without having to worry about accidentally downloading malware, because they know that malicious content has no avenue to reach their device.

5.3 SECURE

Secure access to applications and protect data to the last mile.



Securing access to applications and data has proven more difficult as threat actors escalate their tactics. Enterprises need a zero-trust solution that works everywhere, for managed and unmanaged devices.

The **Menlo Secure Cloud Browser** and **Menlo Secure Application Access** enables secure access and application protection for both private web applications and SaaS applications while simultaneously protecting the associated intellectual property and application data.

Secure Products include:

- Secure Application Access
- Cloud Security Services
- Last Mile Data Protection
- Secure Web Gateway
- FWaaS

Enable seamless access to enterprise applications for employees and partners without compromising security. Menlo Secure Application Access enables least-privileged access on a resource-by-resource basis, supporting access and application protection for both private and SaaS applications.

Menlo Secure Application Access

Menlo Secure Application Access enables least-privileged access on a resource-by-resource basis. It supports access and application protection for both private and SaaS applications. Data security and information leakage protection works hand-in-hand with easy-to-manage access control. Menlo Secure Application Access ensures secure application access while simultaneously protecting the associated intellectual property and application data when you provide secure intranet access to contractors or provide access from a native RDP or SSH client.

When you deploy Menlo Secure Application Access, you also protect your data and protect your application from infected endpoints.

Continuously enforce policy and safeguard applications, users and data In addition to hiding applications from the Internet, Secure Application Access protects against the threat of an infected endpoint or an insider seeking to elevate privileges. Secure Application Access safeguards applications from evasive threats by using the Menlo Secure Cloud Browser to communicate between the local browser and application.

Secure Application Access protects against attacks that employ:

- **HTTP header manipulation**
- **HTTP request smuggling**
- **Server-side request forgery**
- **And other protocol or payload manipulations**

Rather than access the original application, the Menlo Secure Cloud Browser creates a rendered representation of the application on the endpoint device directly in the user's browser. The content rendering provides access, while shielding the user from content-based attacks and shielding the application from malicious requests that might involve parameter tampering, web scraping, API abuse,

and a host of other problems. Even if the endpoint somehow gets compromised, the threat actor cannot get direct access to issue requests to the server.

Additionally, Menlo Secure Application Access provides Sandboxing for all the content that is shared between the user and the application. If a user uploads an infected file, Menlo Secure Application Access stops the file from infecting the application and other potential malicious activity.

To provide further protection for the valuable data these applications hold, Menlo Secure Application Access has additional layers of granular security controls. These controls, which can be used to help with compliance, data leakage prevention, and more, include:

- **Download/upload**
- **Read-only/read-write**
- **Watermarking**
- **Data redaction**
- **Copy/paste**

Cloud Security Services

- **Last-Mile Data Protection** Stop deliberate or accidental leakage of critical business information. Menlo Last-Mile Data Protection identifies and prevents sensitive data from leaving your company. It provides 100 percent reliable inspection of all file uploads and user input for both isolated and non-isolated browsing sessions by creating an air gap between the user and the Internet through which all traffic flows. This isolation technology-powered approach controls the channel between the user and the isolated browser, enabling the system to inspect everything.

Menlo Last-Mile Data Protection helps organizations monitor every device in their ecosystem with completely reliable data inspection.

Generative AI usage

Menlo Last-Mile DLP functionality provides security teams with the ability to control data input into Generative AI platforms and safeguard sensitive content from being uploaded. This gives security organizations peace of mind knowing that any potential risk of data leakage is mitigated within an isolated layer as we begin to see organizations adopt AI tools over time, controls include.

- **Download/upload**
- **300+ Granular configurable Data Loss Prevention Policies**
- **Read-only/read-write**
- **Watermarking**
- **Data redaction and Browser forensics**
- **Copy/paste**

FWaaS Protection

Menlo Security's Firewall as a Service (FWaaS) enables fast and secure Internet for organizations, and because it's 100% in the cloud, there's no traditional hardware to buy, deploy, or manage. FWaaS takes a software-based approach to delivering security services to distributed and mobile users throughout the cloud—eliminating the need to backhaul cloud app and SaaS traffic to a central data

center. This allows organizations to provide secure local internet breakouts to remote users at cloud scale.

FWaaS along with the Menlo Security Client gives security teams visibility into traffic and the ability to apply the appropriate security controls to all traffic regardless of physical location or the underlying connection. And we do this without relying on vulnerable VPN services or physical security appliances that impact performance and add IT overhead. Remote users have the same application experience they expected from the office.

Cloud-based simplicity and scale

Delivering firewall controls and unmatched security to all employees and roaming users no matter their location, and all ports and protocols.

No physical appliance in sight

Traditional physical firewall appliances aren't suited for the modern workplace. We were born in the cloud and built to secure it.

Accelerating productivity

Traditional firewalls result in increased latency and network bottlenecks. We've erased those issues, focusing on preserving the employee experience, making security invisible to the end user.

6 MENLO SECURITY CLOUD PLATFORM BUNDLES

To best fit Customer requirements the annual subscription packages available to customers are laid out in the following product modules:

INDIVIDUAL

Browser-Manage-1-YR

Browser Assessment and Posture Management, Industry Benchmark Comparisons, Integration with Intune, and Browser Configuration Tracker

Browser-Protect-1-YR

Browser Zero-Day Protection, HEAT Visibility, Enterprise Extension, Cloud Browser, Cloud Document and Archive Viewer, File Upload/Download Controls, Copy & Paste, Read-Only Policy, DLP, Last-mile DLP - Watermarking and Data Redaction, File Hashcheck, Antivirus, and Cloud Sandbox

Browser Secure-1-YR

Secure Application Access, Enterprise Extension, Menlo Security Client, File Upload/Download Controls, Copy & Paste, Read-Only, DLP, Last mile DLP - Watermarking and Data Redaction, SaaS Tenant Restrictions, SaaS Application Control, Shadow IT Discovery, File Hashcheck, Antivirus, and Cloud Sandbox

PACKAGE

Browser-Security-Enterprise-1YR

BROWSER-MANAGE-1-YR, BROWSER-PROTECT-1-YR,
and BROWSER-SECURE-1-YR

ADD-ONS

Add-Browser-Forensics-1-YR to BROWSER-PROTECT, BROWSER-SECURE, or BROWSER-SECURITY-ENTERPRISE

Add-HEAT Shield-1-YR to BROWSER-PROTECT or BROWSER-SECURITY-ENTERPRISE bundle.

HSM-Customer Cert-1-YR Cloud HSM for customers to bring their own certificate that will be used for SSL Inspection

Recast-Route-All-1-YR

Add-FWaaS-Menlo-Client-1-YR

FWaaS and Steering Client can be added to CLOUD-PROXY, BROWSER-PROTECT, and BROWSER-SECURITY-ENTERPRISE

Cloud-Proxy-1-YR

URL-Filtering, SSL Inspection, File Hashcheck, Antivirus, Cloud Sandbox, and Microsoft Defender for Cloud Apps Integration

v2024.0305	USER BANDS 0 - 1000 INCLUDES			US AND EMEA			MENLO SECURITY CONFIDENTIAL				
	0-99	100-500	500-1000	1001-2500	2501-5000	5001-7500	7501-10,000	10,001-25,000	25,001-50,000	50,000-100,000	100,000+
BROWSER-MANAGE-1-YR	POA	POA	POA	POA	POA	POA	POA	POA	POA	POA	POA
Browser Assessment and Posture Management, Industry Benchmark Comparisons, Integration with Intune, and Browser Configuration Tracker											
BROWSER-PROTECT-1-YR	POA	POA	POA	POA	POA	POA	POA	POA	POA	POA	POA
Browser Zero-Day Protection, HEAT Visibility, Enterprise Extension, Cloud Browser, Cloud Document and Archive Viewer, File Upload/Download Controls, Copy & Paste, Read-Only Policy, DLP, Last-mile DLP - Watermarking and Data Redaction, File Hashcheck, Antivirus, and Cloud Sandbox											
BROWSER-SECURE-1-YR	POA	POA	POA	POA	POA	POA	POA	POA	POA	POA	POA
Secure Application Access, Enterprise Extension, Menlo Security Client, File Upload/Download Controls, Copy & Paste, Read-Only, DLP, Last mile DLP - Watermarking and Data Redaction, SaaS Tenant Restrictions, SaaS Application Control, Shadow IT Discovery, File Hashcheck, Antivirus, and Cloud Sandbox											
BROWSER SECURITY PACKAGE											
BROWSER-SECURITY-ENTERPRISE-1-YR	POA	POA	POA	POA	POA	POA	POA	POA	POA	POA	POA
BROWSER-MANAGE-1-YR, BROWSER-PROTECT-1-YR, and BROWSER-SECURE-1-YR											
ADD-CDN											
CLOUD-PROXY-1-YR	POA	POA	POA	POA	POA	POA	POA	POA	POA	POA	POA
URL-Filtering, SSL Inspection, File Hashcheck, Antivirus, Cloud Sandbox, and Microsoft Defender for Cloud Apps Integration											
ADD-BROWSER-FORENSICS-1-YR	POA	POA	POA	POA	POA	POA	POA	POA	POA	POA	POA
Add to BROWSER-PROTECT, BROWSER-SECURE, or BROWSER-SECURITY-ENTERPRISE											
ADD-HEAT-SHIELD-1-YR	POA	POA	POA	POA	POA	POA	POA	POA	POA	POA	POA
Add to BROWSER-PROTECT or BROWSER-SECURITY-ENTERPRISE											
HSM-CUSTOMER-CERT-1-YR	POA	POA	POA	POA	POA	POA	POA	POA	POA	POA	POA
Cloud HSM for customers to bring their own certificate that will be used for SSL Inspection											
ADD-FWAAS-MENLO-SECURITY-CLIENT-1	POA	POA	POA	POA	POA	POA	POA	POA	POA	POA	POA
FWaaS and Steering Client can be added to CLOUD-PROXY, BROWSER-PROTECT, and BROWSER-SECURITY-ENTERPRISE											
ADD-REDGE-FIXED-EGRESS-1-YR	POA	POA	POA	POA	POA	POA	POA	POA	POA	POA	POA
The customer gets 1 dedicated IP address in one region with ingress from all Menlo regions.											
ADD-REDGE-FIXED-EGRESS-EXTRA-IP-1	POA										
This can only be added to ADD-REDGE-FIXED-EGRESS. The customer gets an additional IP address in any of the Menlo REDGE regions.											
ADD-1HR-TAB-DETACH-1YR	POA										
User's browser tab will continue to be connected to an isolated browser for one hour even if there is no user activity. Streaming media, webpages with user input will not detach from the isolated browser as per the default behavior.											
ADD-2HR-TAB-DETACH-1YR	POA										
User's browser tab will continue to be connected to an isolated browser for two hours even if there is no user activity. Streaming media, webpages with user input will not detach from the isolated browser as per the default behavior.											

		MENLO ENTERPRISE			
		MANAGE	PROTECT	SECURE	Add
Capability					
Browser Assessment		✓			
Posture Management		✓			
Industry Benchmark Comparisons		✓			
Integration with Intune		✓			
Browser Configuration Tracker		✓			
Browser Zero-Day Protection			✓		
HEAT Visibility			✓		
Add HEAT Shield (Protect, Enterprise)					+
Add Security Client (Protect)					+
Secure Cloud Browser			✓	✓	
Cloud Document and Archive Viewer			✓	✓	
File Upload/Download Control			✓	✓	
Copy & Paste Control			✓	✓	
Read-Only Policy			✓	✓	
Last-mile DLP - Watermarking and Data Redaction			✓	✓	
File Hashcheck			✓	✓	
Antivirus			✓	✓	
Cloud Sandbox			✓	✓	
Secure Application Access				✓	
Enterprise Extension			✓	✓	
SaaS Tenant Restrictions				✓	
SaaS Application Control				✓	
Shadow IT Discovery				✓	
Menlo Security Client and FWaaS (Secure)					+
Browsing Forensics (Protect, Secure, Enterprise)					+

7 MENLO SECURITY CUSTOMER SUPPORT

Menlo Security Support services are designed to offer fast response times as well as ensure that customers have direct and immediate access to senior Support Engineers for any support issues.

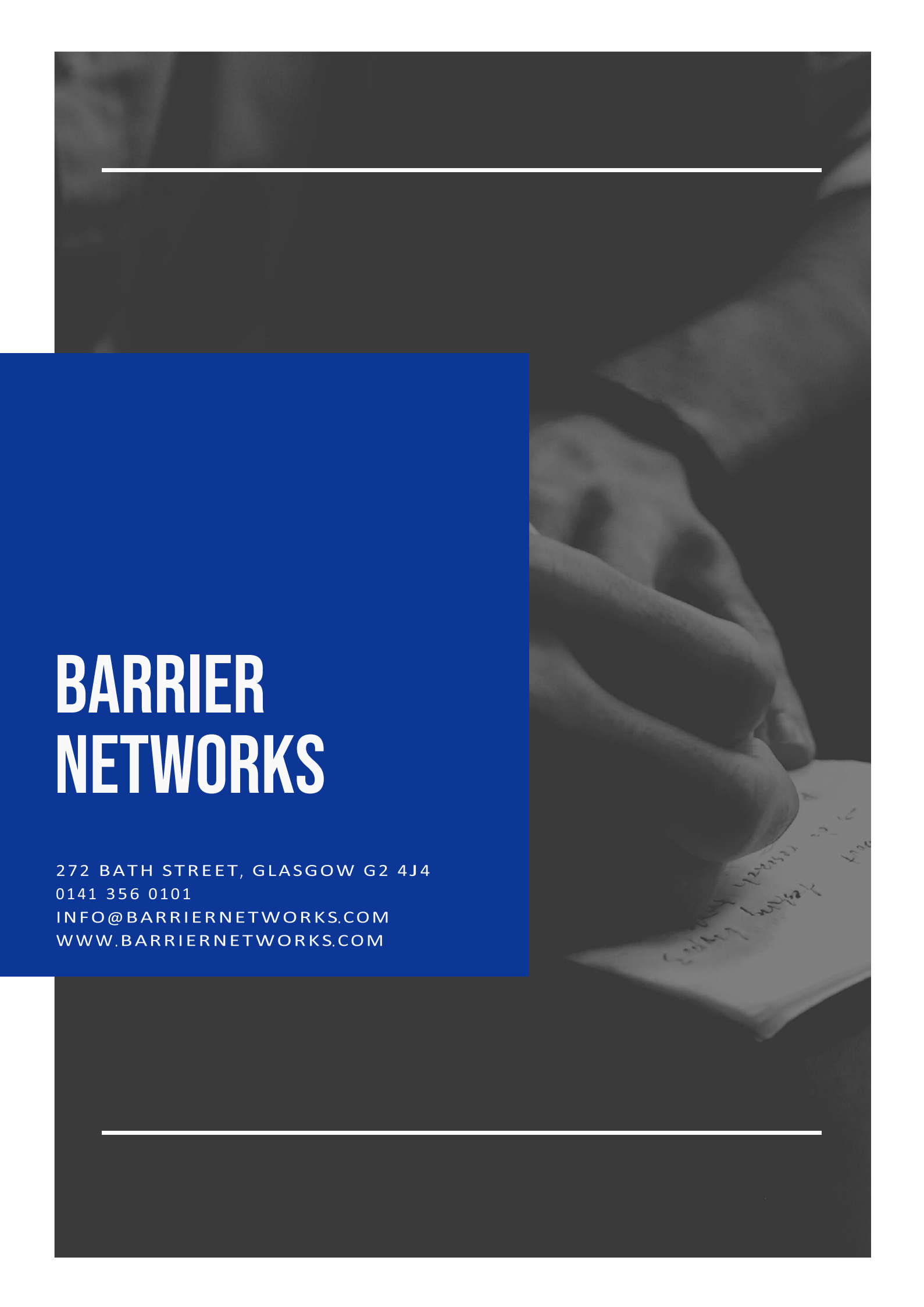
Starting on day one of your Menlo Security deployment with Premium Support, experienced support experts are available to ensure product and policy configuration related issues are resolved quickly. This will reduce the risk of exposure to malware, phishing attacks, and other threat actors on the Internet.

Optionally, our Platinum offering provides access to a Technical Account Manager (TAM) drawn from Menlo Security senior support staff for additional support continuity. The Technical Account Manager functions as an extension of your IT security team, developing in-depth knowledge of your IT environment and providing services ranging from issue troubleshooting to business and services reporting, and encompassing regular updates in weekly operational status calls and quarterly business reviews. One key differentiator with Menlo Security's TAM is their ability to provide insight into the threats discovered via our Isolation Core™. This additional data is an invaluable resource for your Security Operations Centre (SOC) team.

Menlo Security—Support Overview	Basic	Premium	Platinum
Technical support access	12x5	24x7	24x7
Support case analytics	Yes	Yes	Yes
Online learning and training	Yes	Yes	Yes
Technical onboarding, including configuration guidance	Yes	Yes	Yes
Designated Technical Account Engagement			Yes

SLA Goals	Basic	Premium	Platinum
P1 (Urgent)	1 hr	30 min	15 min
P2 (High)	4 hr	1 hr	30 min
P3 (Normal)	4 hr	3 hr	2 hr
P4 (Low)	4 hr	4 hr	4 hr

Customers are provided access to the Menlo Security Customer success portable, from here they're able to log and manage any support cases and access the Technical Knowledge Base and Information portals. Support Tickets can be raised via directly via Email, Telephone, or the Customer Success Portal.



BARRIER NETWORKS

272 BATH STREET, GLASGOW G2 4J4

0141 356 0101

INFO@BARRIERNETWORKS.COM

WWW.BARRIERNETWORKS.COM
