Menlo Security

IT'S SAFE TO CLICK

ISOLATION PLATFORM DATA SHEET

Highlights

- **100% safety via isolation** – Stops the constant "good" vs. "bad" decision loop and alleviates unknown exploits, eliminating phishing, malware, and ransomware to keep endpoints secure
- **Seamless end-user experience** – Makes it safe to click for today's digital workforce, with a native user experience
- **Cloud simplicity and proven scale** – Reduces security cost and complexity, while increasing scale by eliminating endpoint software, outdated network appliances, and web browser plug-ins

Eliminate Web and Email Threats

Today, endpoint devices and crucial, sensitive information can be attacked in any number of ways.

Virtually any website, web link, web advertisement, or link to any document can deliver malware, launching an attack on a user's endpoint device and data that quickly spreads throughout their organization, infecting any device it can. Even typically "safe," legitimate websites may be hijacked and spread malware by drive-by download or watering hole attack. Known URLs can appear to be real, but are really spoofed or use homographic attacks, leading the user to a phishing website where malware can be downloaded, user credentials stolen, or ransomware launched. Emails today can look like they are coming from a known, trusted source; instead, they're from attackers who have embedded web or document links that launch malware or steal user credentials.

Traditional legacy security solutions and conventional threat prevention products that attempt to distinguish between "good" and "bad" content, or that whitelist or blacklist websites, have failed. Malware developers have proven they can circumvent "new" technologies designed to detect their activity. New malware can determine if it has been detected or sandboxed, and delete itself before it can be captured for analysis.

A whole new approach to endpoint and user security is required, now.

Top Qualities of an Enterprise-Class Isolation Platform

A state-of-the-art, enterprise-class isolation solution:

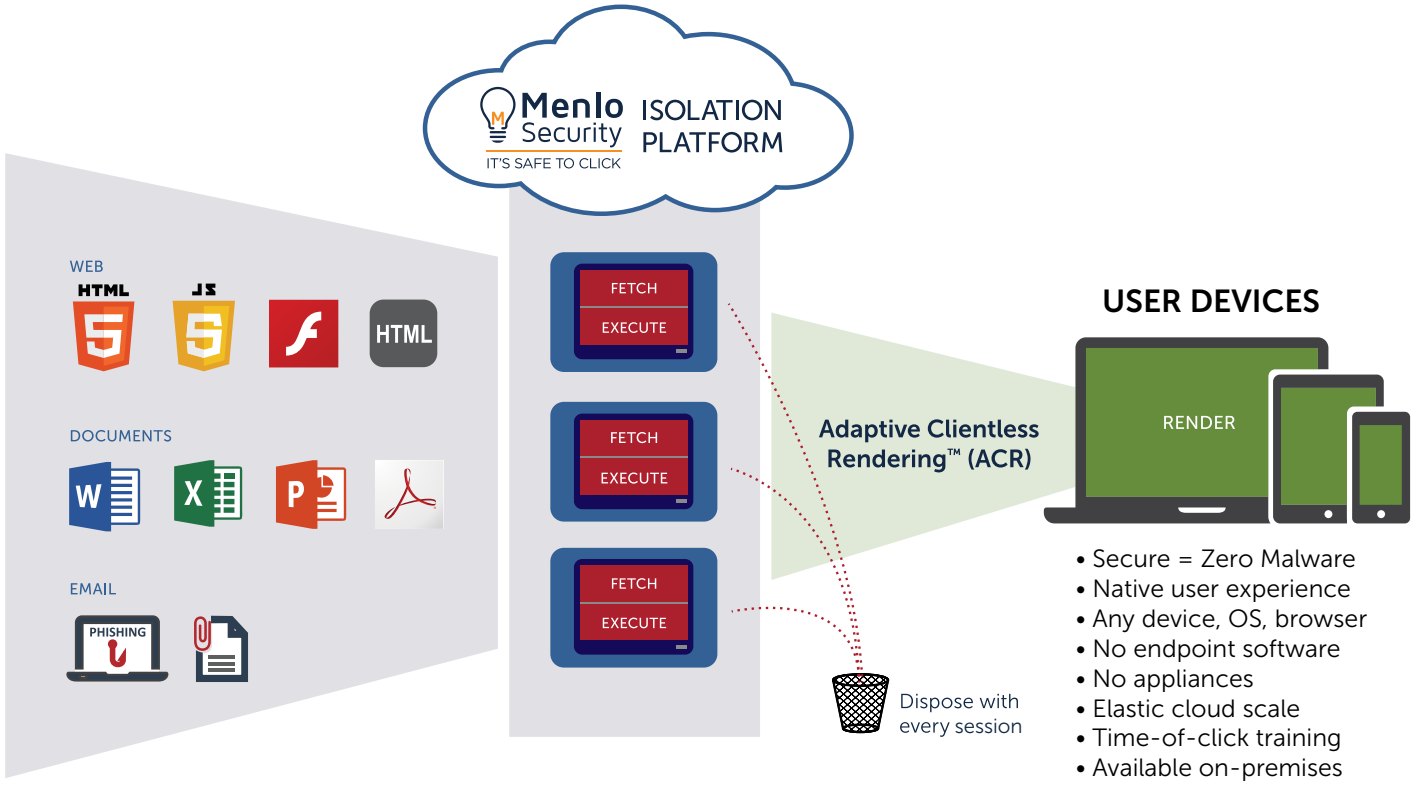
- Eliminates web-based malware (including drive-by downloads and watering hole attacks), weaponized documents, ransomware, and phishing attacks (including spear phishing and whaling attacks)
- Generates zero false positives or false negatives
- Preserves a native user experience with no noticeable latency or browser impact
- Works with any device, OS, or browser—no custom browser necessary
- Offers deployment options, including global availability as a public cloud service, as a virtual appliance, or in a private cloud
- Deploys quickly and easily, without requiring endpoint software, outdated network appliances, or web browser plug-ins
- Integrates with existing security systems (e.g., secure web gateways and next generation firewalls) and mail systems, and supports single sign-on
- Reduces the administrative burden of policy exceptions
- Provides privacy, with controls for extensive visibility and forensics

Isolate Your Way to Freedom

There is a new approach to security based on a proven, established technology: isolation. Instead of constantly distinguishing, assessing and re-assessing the moving target of "good" versus "bad" content, links, and websites, isolation inserts a secure, trusted execution environment—or isolation platform—between the user and potential sources of attack or infection. User sessions are executed away from the user's endpoint device, and what is delivered is only safe rendering information, protecting the user and their device from malware and malicious activity, eliminating phishing, web-based malware, ransomware, and credential theft.

The Menlo Security Isolation Platform (MSIP) delivers assured security without compromising the user experience or burdening your IT staff. Leveraging patented virtualization and Adaptive Clientless Rendering™ (ACR) technologies, MSIP enables enterprise-wide deployment of isolation security without the need to deploy and manage endpoint software, new browsers, or web browser plug-ins, dramatically reducing resource cost and time, and eliminating risk, while empowering your users to click on links and browse the Internet safely.

The Menlo Security Isolation Platform eliminates web- and email-based malware and credential theft, making it safe to click.



Menlo Security Isolation Platform (MSIP) Key Features & Benefits: 100% Safety via Isolation

PROTECTS USERS FROM WEB AND EMAIL THREATS

FEATURES	BENEFITS
Disposable Virtual Containers (DVC) • Web and document sessions executed away from the user's endpoint • All web and document content—including any malware—is disposed of along with the DVC at the end of every web session	• Alleviates any chance for malware to escape and infect a user's endpoint device • Eliminates false positives that block legitimate content and generate alerts, and false negatives that allow malware to reach a user's endpoint device
Read Only Mode • Safeguards against users entering critical user credentials into web forms on isolated websites	• Alleviates the threat of credential theft • Policy can be assigned by user, group, etc.
Blocks File Uploads to Isolated Websites	• Ensures no information can be uploaded from a user's endpoint device to a website in isolation
Email Link Isolation • All email links are opened in the isolation platform, away from the user's endpoint • Does not rely on error-prone threat detection • Even if a user clicks on a malicious email link, all websites are safely isolated and have input-field restrictions	• Protects against phishing attacks and ransomware • Safeguards against targeted spear-phishing attacks • Eliminates 100% of drive-by malware exploits
Credential Theft Protection • Websites opened by emailed links can be rendered in Read Only Mode	• Protects users from entering critical corporate and sensitive personal information into malicious web forms • Stops credential theft and identity theft
Protection from "Zero-Day" and Emerging Phishing Techniques • Defends against most emerging phishing methods by cyber-attackers, including attacks leveraging OAuth, data uniform resource identifier (URI), embedded PDF files, Punycode international domain name (IDN) homograph, and more	• Ensures that emerging phishing techniques are stopped before they can even start being destructive
Mail Server Integration • Integrates with existing mail server infrastructure, including Microsoft Exchange, Gmail, and Office 365 • All email links can be directed to pass through the isolation platform	• Streamlines deployment • Requires no changes to existing email platforms or user experience • Protects every users' email the instant it's deployed
Application Traffic Scanning • Scans application traffic • Defines application traffic policy controls	• Analyzes web traffic as it's retrieved to determine if it matches a major URL category • Can also determine whether the traffic looks like a threat
Neutralizes 'Command-&-Control' (C2) Communications	• Stops any malware from attempting to take control of a user's device

DISARMS WEAPONIZED DOCUMENTS

FEATURES	BENEFITS
Document Isolation • Isolates and opens documents in the isolation platform, away from a user's endpoint device	• Eliminates any user risk from weaponized documents, including documents from Adobe Acrobat, Microsoft Office (Microsoft Word, Excel and PowerPoint), Microsoft Visio, Microsoft Project, Microsoft OneNote, Ichitaro, AutoCAD, RTF, and OpenOffice
Optional 'Safe' or Original Downloads • As an option, administrators may allow users to download 'safe' PDF versions of rendered documents or allow download of original documents for designated users only	• 'Safe' downloads remove any dynamic content, such as JavaScript, within the isolation platform, ensuring safe documents in Adobe Acrobat • Original downloads may be required, and are offered as an option, on a policy controlled basis (per user, per group, per domain, per category, etc.)
Anti-virus Document Scan and Sandbox Options* • If users are permitted to download an isolated original document, Menlo Security offers cloud-based anti-virus scanning of the original document • Should the anti-virus scan not verify malware on an original document, a sandbox can further inspect the document and determine whether document is a threat • Workflow is fully customizable by administrators • Scans and inspects password protected documents contained in ZIP files	• If original documents are requested, the cloud-based anti-virus scan and sandbox ensure that only documents free of malware can be downloaded • Prevents infections by scanning documents in ZIP files, even if they are password protected

*Features are sold as separate additional licenses.

INSPECTS SSL-ENCRYPTED WEB TRAFFIC

FEATURES	BENEFITS
HTTPS Traffic Isolation/Protection • Malware increasingly uses encrypted web sessions to hide activity and bypass existing security solutions • Isolates and protects against HTTPS traffic camouflaging malware • Configure categories, or specific sources or destinations (IPs or FQDN) to be excluded from SSL inspection	• Ensures that HTTPS traffic is free of hidden malware • Allows flexibility in inspection of SSL-encrypted web traffic
HTTPS Traffic Insight • View how much HTTPS traffic is in use, where the traffic is going, and who is using it	• Provides better insight into and control of HTTPS traffic coming into your network
HTTPS Document Rendering • Render documents retrieved from sites using HTTPS	• Protects the user and their endpoint device from encrypted documents harboring malware

PROTECTS ENDPOINTS FROM DYNAMIC CONTENT

FEATURES	BENEFITS
Dynamic Content Protection • Dynamic content, such as JavaScript, may be leveraged to deliver malware to infect a user's endpoint device and ultimately your entire network • Potentially harmful dynamic content is executed within the isolation platform, with only safe rendering information sent to the user's endpoint device	• Produces a safe, secure user experience without delivering potentially dangerous dynamic content to the user's endpoint device
Protection from Adobe Flash • Adobe Flash is potentially dangerous because it can mask malicious background operations that infect a user's endpoint device • Flash content is transferred into the isolation platform, active content is removed, and the video is encoded into a new, clean HTML5 video (H.264) and pushed to the user's web browser for viewing	• Enables the removal of Flash from a user's endpoint device and browsers, while allowing users access to Flash-produced content, without risk of infection
Native Internet Content and Resources Isolation • No native content or resources are passed to the user's endpoint device • All native Internet content and resources are loaded only within the isolation platform	• Protects the user's endpoint device from potentially dangerous native Internet content and resources • Ensures only safe rendering information is sent to the user's endpoint device

A Seamless User Experience

SECURES A NATIVE USER EXPERIENCE

FEATURES	BENEFITS
Adaptive Clientless Rendering™ (ACR) • Patented technology uses an optimal encoding mechanism for each content type and delivers it securely to the user's endpoint device via industry-standard rendering elements compatible with any device, browser, or OS	• Enables a consistent, known user experience nearly indistinguishable from direct web browsing • Allows for continued use of standard web browsers • No noticeable latency or impact to browser functionality, including cut-and-paste or printing functions • No pixelation, choppy scrolling or other visual artifacts common with 'screen-scraping' technologies such as virtual desktop interface (VDI)

SUPPORTS MOST POPULAR DOCUMENT TYPES AND WEB BROWSERS

FEATURES	BENEFITS
Popular Document Type Support • Supports the most popular document types users rely on to be productive	• Includes support for: – Adobe Acrobat (.pdf) – Microsoft Word (.doc, .docm, .docx) – Microsoft Excel (.xls, .xlsx, .xlsm) – Microsoft PowerPoint (.ppt, .pptm, .pptx) – Microsoft OneNote (.one) – Rich Text Format (.rtf) – Ichitaro (.jtd) – Many other document types
Popular Web Browser Support • Supports most popular and deployed web browsers • Does not require any special or custom browser	• Supports standard, user accepted and operated web browsers, including: – Google Chrome – Microsoft Edge – Microsoft Internet Explorer – Mozilla Firefox – Apple Safari – Other standard web browsers • Ensures a familiar, uninterrupted web user experience

REDUCES WEB CLASSIFICATION AND RECLASSIFICATION REQUESTS

FEATURES	BENEFITS
Reduces Classification/Reclassification Requests • No need to limit user access to websites or web apps to eliminate malware, phishing, or other cyberattack • Users may access any web app or content they need to be productive	• Eliminates costly help desk requests for website/content reclassification • Alleviates user productivity impediments

Cloud Simplicity with Proven Scale

DEPLOYS QUICKLY AND EASILY

FEATURES	BENEFITS
24x7 Global, Elastic Cloud-based Service • Scales quickly and effortlessly to meet the demands of small to global enterprises **On-premises Open Virtual Appliance (OVA)** • Allows for an on-premises solution for organizations requiring an in-house solution	• No endpoint software to deploy and manage • No outdated network appliances to install and maintain • No browser plug-ins to load and administer • Deployable and scalable in minutes • Simplifies operations • Cuts operating costs • Eliminates alert fatigue with zero false positives or negatives

INTEGRATES WITH EXISTING ANTI-VIRUS, SECURITY, MAIL, AND ACCESS SYSTEMS

FEATURES	BENEFITS
Flexible Web Traffic Proxy • User web traffic can be directed through the isolation platform by configuring user browsers with proxy auto-configuration (PAC), automatically provisioned via Microsoft Active Directory (AD) or other device management systems • User web traffic may also be routed to an integrated, existing web proxy system	• Eases configuration and integration with the isolation platform, as well as existing legacy proxy systems or services
Simplified Deployment with Existing Legacy Security Solutions • Certified and deployed with firewalls, web proxy systems, and threat detection offerings from leading vendors worldwide	• Eases deployment with existing, legacy security solutions • Enables a layered defense-in-depth strategy to address phishing, malware, and other cyber threats
Integration with Existing Anti-virus (AV) • Enables anti-virus scans of downloaded documents and files • Hash of downloaded documents or files checked against over 50 AV engines • Alerts generated for scan of any downloaded document or file if an 'infected' status is determined	• Streamlines integration with deployed AV solutions • Ensures and maintains document and file integrity and security
Integration with Deployed Single Sign-on (SSO) and Identity & Access Management (IAM) Solutions • Supports SSO to Microsoft Office and Office 365 • Supports SAML integration with most popular cloud-based IAM solutions	• Simplifies login, and identity and access control • Integrates with: – Microsoft Active Directory Federation Service (ADFS) – Centrify – Okta – OneLogin – Ping Identity

ENABLES ROBUST FORENSICS AND REPORTING

FEATURES	BENEFITS
MSIP Administrative Portal • Views log data and reports directly in the administrative portal • Exports log data to SIEM or operational management systems	• Enables extensive information collection and analysis for attacks stopped • Certified and deployed with leading vendor SIEM solutions
Rich, Valuable Reports • Suitable for forensics and analysis	• Available reports include: – Activity by user and web category – Browsing activity to sites with known vulnerabilities – Threats averted – More reports available

About Menlo Security

Menlo Security makes it safe to click via isolation, protecting organizations from cyber attack by eliminating the threat of malware and phishing attack from web and email. The Menlo Security Isolation Platform (MSIP) isolates all active content in the cloud, enabling users to safely interact with websites, links, and documents online without compromising security. Menlo Security is trusted by some of the world's largest enterprises, including Fortune 500 companies and financial services institutions.

The company was founded by security industry experts, in collaboration with acclaimed researchers from the University of California, Berkeley, and backed by General Catalyst, Sutter Hill Ventures and Osage University Partners.

For more information,
visit menlosecurity.com.

Menlo Security
IT'S SAFE TO CLICK

2300 Geng Rd, Ste. 200
Palo Alto, CA 94303
Tel: 650 614 1795
info@menlosecurity.com

Menlo Security Isolation Platform Deployment Options

Global, 24x7 Cloud Service

The Menlo Security Isolation Platform (MSIP) is a global, 24x7 cloud service, with worldwide accessibility. Multi-tenant capable, with worldwide tenant awareness, the MSIP supports hundreds of thousands of users, with automatic scaling to handle surges in cloud traffic. It routes access via any of its worldwide nodes based on location to alleviate any possible latency and to deliver the best user experience possible. With the cloud-based MSIP, there is no need to increase network bandwidth requirements. And reliability is paramount, which is why MSIP enjoys a 99.95% cloud uptime.

Open Virtual Appliance (OVA)

The Menlo Security Isolation Platform is also available as a virtual appliance that may be deployed on-premises for organizations that require or demand local network access, or have security requirements that a third-party hosting model cannot meet. MSIP may also be deployed in a private cloud. Available as a pre-configured virtual machine image, ready to run on a hypervisor, MSIP's OVA deployment option is intended to eliminate the installation, configuration, and maintenance costs associated with running complex stacks of software. Its underlying virtualization technology also allows for the rapid movement of virtual appliance instances between physical execution environments.

OVA System Requirements:

Hypervisor Environment

- VMware vCenter Server 5.1 or newer version(s)
- VMware ESXi 5.1 or newer version(s)
- Oracle VM Manager version 3.4 or newer version(s)

Virtual Appliance Resources

- 6 GB RAM (default); 32 GB RAM is recommended
- 8 vCPUs
- 270 GB of Virtual Disk space (one 200 GB drive and one 70 GB drive on the virtual machine)
- One virtualized network interface card (VNIC)