MENLO SECURITY

Data Sheet

Email Security

Outsmart email threats with a Zero Trust approach.

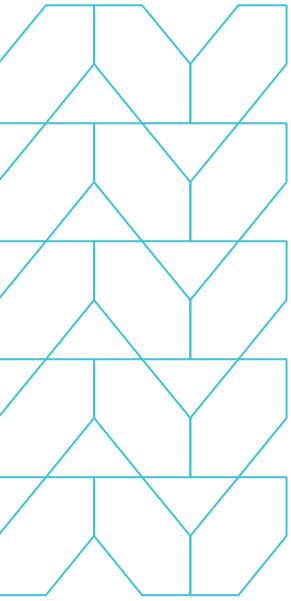
Email remains the most used business communication vehicle. Despite this—or perhaps because of this—email has become the threat vehicle of choice for cybercriminals. All it takes is a single user to click on a malicious link embedded in an email and the user's device has been breached. From there, cybercriminals can gain access to the corporate network and critical business systems, where they can do a lot of damage. Organizations already have an armory of email security solutions at their disposal—including anti-spam, anti-virus, data security, and encryption solutions. Yet, malicious email attacks such as phishing, credential theft, and weaponized documents persist and continue to be successful.

Three things to know:

Threat actors use email to deliver web links or attachments to users that, when clicked, download malicious content onto their device.

Legacy security solutions analyze web links and documents in an email to make a "good" versus "bad" determination, but the attack is typically active for only a few hours and unique to each target, limiting third-party reputational data that makes detection possible.

Menlo Email Security treats all email links and attachments as potentially risky, preventing malicious content from executing on an end user's device.



Product overview

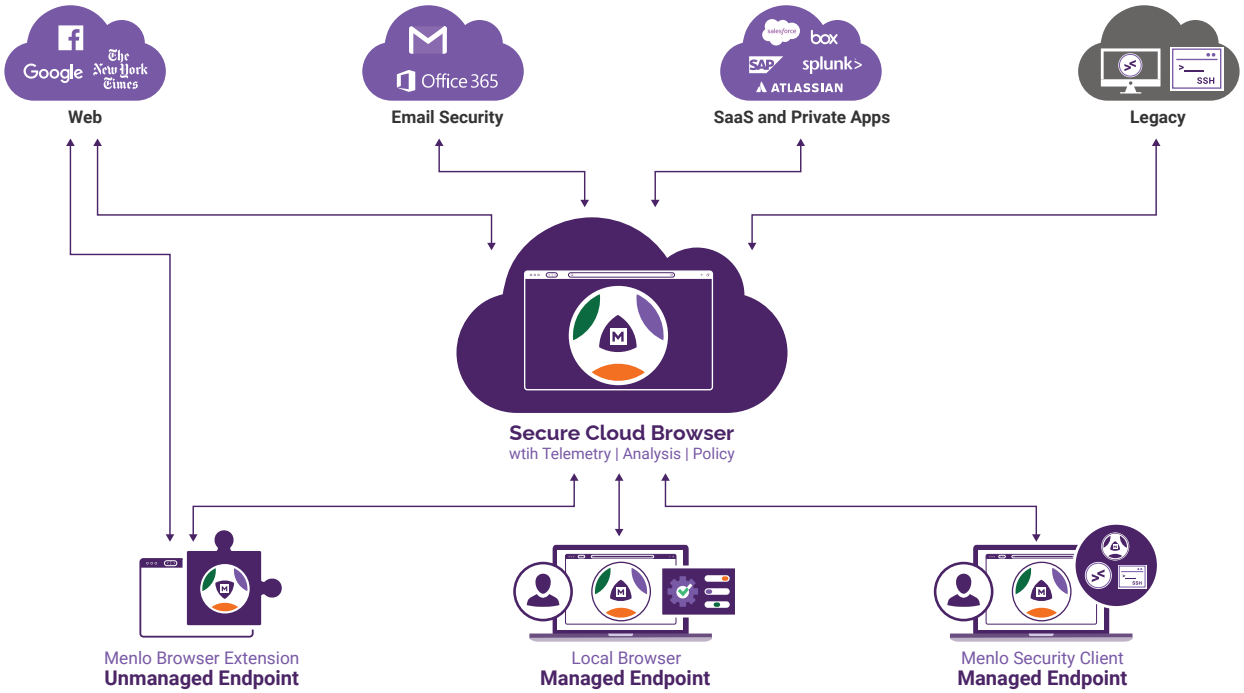
Rather than determining which links in an email are legitimate and which are not, Menlo Email Security assumes that all web content and email attachments are risky and host potentially malicious content. This Zero Trust approach eliminates the need to rely on a third-party threat intelligence feed or make an allow-or-block determination based on coarse categorization. Instead, Menlo isolates all web traffic originating from the Internet and renders high-risk or known malicious content—including email links and attachments—in read-only mode. This prevents any malicious content from ever reaching users' devices—laptop, mobile device, or desktop—where it can spread laterally across the network and do real damage.

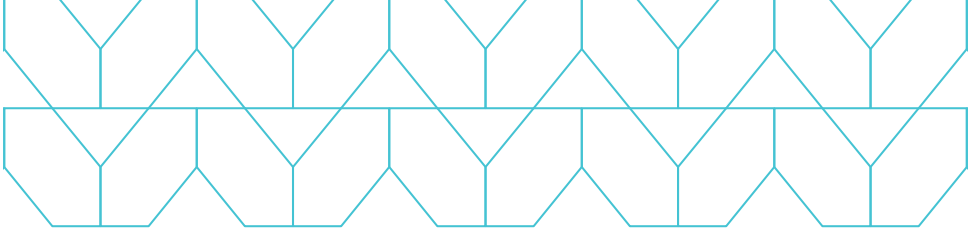
With Menlo, web content is accessed in the secure cloud browser, and only safe and authorized content is delivered to end-user browsers. There are no new email systems or browsers to learn or software to install.

Menlo Email Security 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.

With users safely isolated, administrators can monitor behavior statistics and provide customizable time-of-click messages that provide real-time teachable moments. These messages help reinforce anti-phishing awareness training based on live threats rather than simulated campaigns. Administrators can also define workflow policies for groups or individuals that determine if or when web input field restrictions can be relaxed. In addition, they can provide users with an option to download an active content–free, safe PDF version of an attached document. In the event an administrator chooses to allow certain users to download original document attachments, a cloud-based anti-virus scan and sandbox can be added to check the file's reputation and ensure that only original documents that are free of malware may be downloaded. Menlo integrates with Content Disarm and Reconstruction (CDR) to sanitize the files at the time of click, even if they are password protected.

With zero dependence on error-prone threat detection methods such as data analytics, Menlo Email Security is the only email security solution that protects every email user the instant it's deployed.





Menlo Email Security: Key features and benefits

Feature	Benefits
Email Link Isolation	Protects against targeted spearphishing and drive-by exploits without relying on error-prone threat detection.
	All native web content originating from an email is discarded in disposable containers using stateless web sessions.
Optional Read-Only Access to Websites	Protects users from credential phishing sites delivered via links in an email.
Anti-Phishing Awareness Training	Provides visibility into user behavior, helping administrators determine which users are clicking on potentially risky links.
	Even if users do click on malicious links, all sites are safely isolated and have input-field restrictions.
	Creates teachable moments with configurable, real-time warning messages.
Attachment Isolation	Eliminates any risk to the user and their device from weaponized email attachments, including documents from Adobe Acrobat, Microsoft Office (Microsoft Word, Excel, and PowerPoint), Microsoft Visio, Microsoft Project, Microsoft OneNote, Ichitaro, AutoCAD, RTF, and OpenOffice.
	Offers full visibility into password-protected files.
	Provides users with safe PDF version of original attachments for offline viewing.
Optional Safe or Original Attachment Download	Removes all dynamic content from documents, creating safe document attachments in PDF format.
	When downloading of original attachments is required, this option is offered on a policy-controlled basis (per user, per group, per domain, per category, etc.).
	Only files that have gone through reputation check, AV, sandbox, and any other third-party integration can be downloaded directly to the endpoint.

Feature	Benefits
Anti-Virus Document Scan and Sandbox Options	Should the anti-virus scan not verify malware on an original attachment, a CDR solution, sandbox, or other third-party integration can further inspect the document and determine whether the document is a threat.
	Workflow is fully customizable by administrators.
	Scans and inspects password-protected documents contained in ZIP files.
	If original attachments are requested, the cloud-based anti-virus scan and sandbox ensure that only documents free of malware may be downloaded.
Integrates with Existing Email Infrastructure—Including Native Integration with Microsoft 365 and Google Workspace	Significantly reduces deployment and installation time.
	Decreases management overhead time and expense.
	Maintains existing user experience and does not interrupt existing user email workflows.
	Preserves user experience and productivity.

Tricking a user into clicking on a malicious link or attachment in a carefully crafted spear-phishing email is one of the easiest and most effective methods that cyberattackers use to infiltrate business systems. Despite an armory of email security solutions at their disposal—including anti-spam, anti-virus, data security, and encryption solutions—organizations continue to struggle to contain malicious email attacks. Menlo Security Email Isolation takes a Zero Trust approach to email security by treating all email links and attachments as risky. This prevents malicious content from executing on an end user's device, giving users the confidence to click with impunity because they know their emails are safe.

To learn more about securing the ways people work, visit menlosecurity.com or email us at ask@menlosecurity.com.

MENLO SECURITY

To find out more, contact us:

menlosecurity.com

(650) 695-0695

ask@menlosecurity.com

About Menlo Security

Menlo Security eliminates evasive threats and protects productivity with the Menlo Secure Cloud Browser. Menlo delivers on the promise of cloud-based security—enabling Zero Trust access that is simple to deploy. The Menlo Secure Cloud Browser prevents attacks and makes cyber defenses invisible to end users while they work online, reducing the operational burden on security teams.

Menlo protects your users and secures access to applications, providing a complete enterprise browser solution. With Menlo, you can deploy browser security policies in a single click, secure SaaS and private application access, and protect enterprise data down to the last mile. Secure your digital transformation with trusted and proven cyber defenses, on any browser.

Work without worry and move business forward with Menlo Security.