



Menlo File Security for Email

DATA SHEET



Integrate simply and securely into existing email infrastructure

Sanitize emails and file attachments in milliseconds

Retain file fidelity and functionality - no mass flattening

Eliminate threats in complex file types, including archives

Overview

Menlo File Security uses patented Positive Selection® technology for email traffic, allowing you to communicate safely and without disrupting your workflow. Today's most sophisticated malicious email attacks are those that bypass most security barriers, leaving enterprises in their most vulnerable state: unaware and unprotected. Email is one of the most common targets for dangerous and malicious attack, exposing organizations to severe disruption. Organizations simply cannot function effectively without a seamless and instant flow of email communications.

Menlo File Security processes emails and eliminates exploit attempts before any other security system can provide protection against them. Replica EML files are constructed for a continuous, undisturbed workflow, transparent to email users.

Menlo File Security is an enterprise product, supporting hundreds of thousands of files of user traffic per day, in a scalable and highly available configuration.

KEY BENEFITS

Email is both an essential productivity tool for enterprises and a top threat vector for file-borne malware. To enable business continuity while ingesting hundreds of file types without fear of malware, security teams require a seamless, zero trust solution like Menlo File Security.

As malware becomes more sophisticated and heavily distributed due to the rise of GenAI, hidden threats are becoming harder to prevent without the help of sophisticated, AI-trained file sanitization tools. Menlo brings antivirus, sandboxing, hash check, and next-gen Content Disarm and Reconstruction under one platform to keep enterprises ahead of zero-day threats.

With Menlo File Security, threat prevention goes beyond the browser. Employees can safely access their email and download over 220+ file types without introducing file-borne malware.



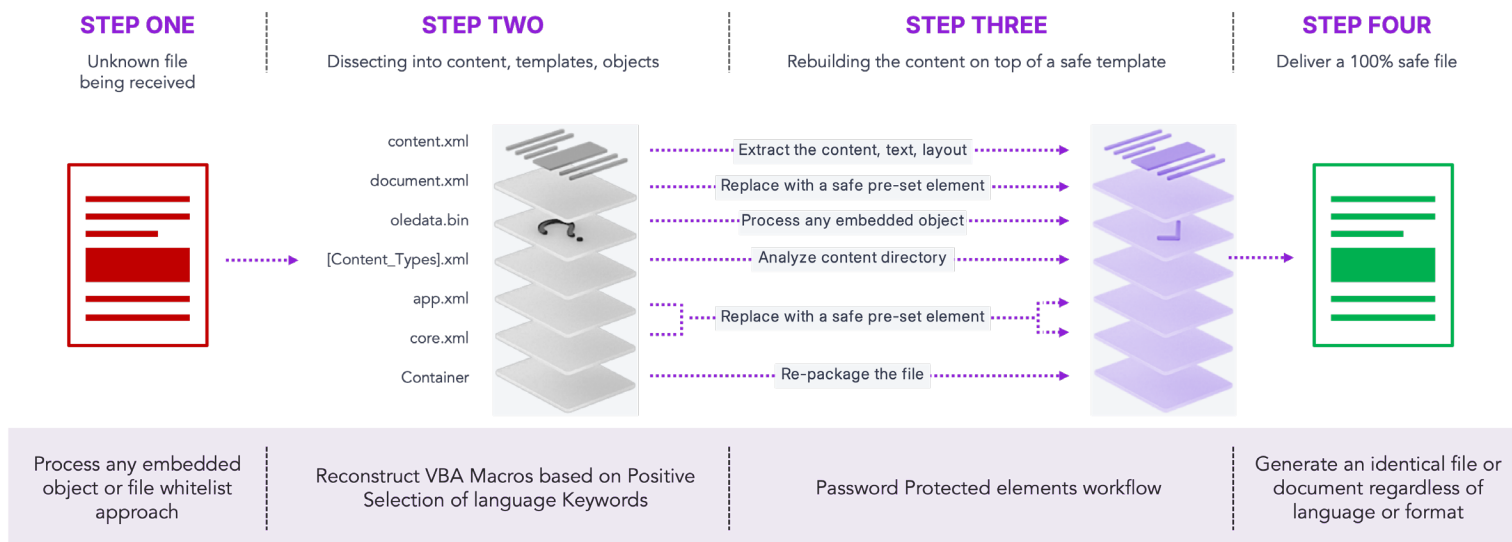
Protection Against All File Threats For Email

Rather than playing the “cat and mouse” game by searching for bad or malicious filebased content, we identify and allow only known good content to pass into your organization. This process ensures that your organization is completely free of any file-based threats.

Menlo’s Positive Selection* Technology

File based attacks are relying on exploiting the template—not the content.

Menlo has developed its own template that delivers safe files to millions of users.



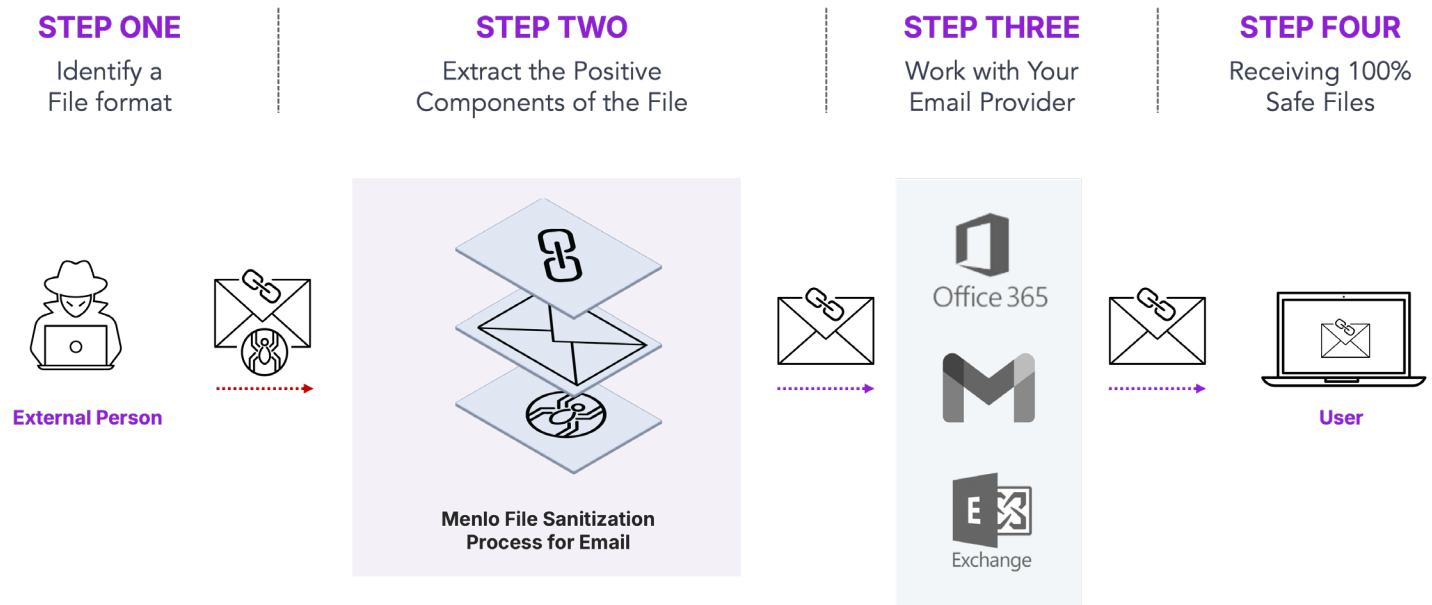
Menlo File Security singles out only the elements of files known to be fully secure, guaranteeing each and every upload is 100% safe. Now you can accept every upload without ever wondering if you are exposing your business to risk.



How It Works

Menlo File Security works with your Email Server to ensure incoming emails flow through our patented file sanitization process before passing to the user, providing protection from any email and file-based threat. We use deep expertise in the architecture of every file format to understand and protect even the most obscure file types.

First, the platform identifies the file's content type and format. It then generates a new, clean template of the file, importing the original file's content while leaving behind all exploits or malicious objects. Then, with all original content and functionality completely intact and all threats completely sanitized, the email is now safe to pass to the recipients.



Features

- Integrates simply and securely into your existing email infrastructure
- Cleans emails and their file attachments in real time, within milliseconds
- Provides the same content, while getting rid of all potential risk
- File fidelity and functionality remains intact, including embedded objects and macros
- Integrates easily into existing security infrastructure, role management systems, and SOC monitoring
- Extensively eliminates threats borne in password-protected documents and archives, encrypted attachments, and URLs

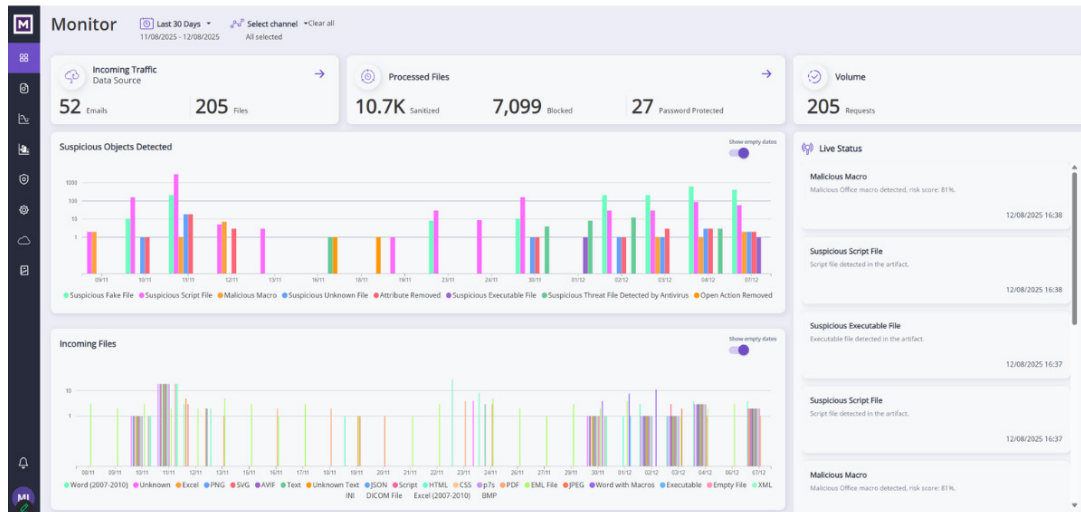
Benefits

- Eliminates users' fear of opening emails and attached files from an unknown source
- Allows security teams to focus on their work and not on noise or responding to alerts
- Maximizes productivity with zero interruption to email communication
- Enables compliance in accordance with the global financial security standards



In-Depth Threat Analytics

Beyond email threats, Menlo understands and protects all file types used in business today - from Microsoft Office and PDF to email, images and archives, so no file or document is left unsecured.



INCLUDED

OPTIONAL

Initial Deployment Support	Remote, over the phone	On site
Ongoing Software Upgrades	Remote, over the phone	On site
Swagger RESTful API	Yes	
File Type Support	<p>Microsoft Office: rtf, xlsx, doc, docx, dot, dotx, docm, dotm, xltx, xlsx, ppt, pps, pot, pptx, ppsx, potx, sldx, sldm, pptm, mpp, mpx, vss, vsdx, vsdm, xlsb, xls, xlt</p> <p>Adobe PDF: pdf, xfa</p> <p>Email: ics, dat, eml, html, msg, pst</p> <p>Images: gif, bmp, jpeg, png, tiff, wdp, jp2, emf, wmf, heic, heif, pgm, ppm, svg</p> <p>Archives: zip, 7z, cab, gz, gzip, wsp, rar, lzh, tar, msg, vmdk</p>	Custom file type support development, available on request. Currently supports over 220 standard and complex file types.
Password Protected Documents and Archives Workflow Support	Yes	

* The supported file types list evolves over time as threat landscape develops. Please ask your Menlo Security representative for the latest list.



Deployment Options

- Positive Selection® technology provided as a pre-built virtual appliance image for quick deployment
- Email solution provided for deployment on premises or on SaaS private cloud or SaaS multi-tenant premises
- User Guide and code sample for developer support

Specifications

MENLO FILE SECURITY	3 NODES CLUSTER	5 NODES CLUSTER	MENLO SAAS TIME
Performance*	35,000 files per hour per cluster	90,000 files per hour per cluster	Unlimited
High Availability	Yes	Yes	Yes
CPU Cores	8 per node	16 per node	N/A
RAM	24 GB per node	32 GB per node	N/A
Drive Capacity	500 GB per node, SSD	500 GB per node, SSDSSD	N/A
Remote Storage Support	NFS, Amazon S3, Azure disk storage, Google Storage	NFS, Amazon S3, Azure disk storage, Google Storage	EFS, Amazon S3, Azure disk storage, Google Storage
Hypervisor Support	VMWare ESXi 7	VMWare ESXi 7	N/A
Network Adapters	4 1 per node + 1 global VIP with DNS name	6 1 per node + 1 global VIP with DNS name	1 DNS name

* Performance values vary depending on the underlying hypervisor configuration and traffic profile being processed.



Technical Requirements

Hardware Requirements	CPU	Dual Core 2.7GHz or vCPU on a VM
	RAM	8 GB (minimum)
	Operating System Drive	30 GB free space (minimum)
	Network Card	Can be a vNIC on a VM
Software Requirements *	Microsoft Windows Server	2019, 2016 or 2012 R2 with latest updates
	Microsoft .NET Framework	V 4.7
	Microsoft Exchange with Edge role	2019, 2016 RTM or 2022 SP1
Network Requirements	SMTP as Mail relay	The Exchange server must be able to establish an SMTP session from an external network.
	Microsoft Exchange Edge	The Exchange connector must be able to communicate with the Positive Selection* Engine using HTTP requests and responses.

* An internet connection is required for installing and updating Microsoft components for the OS. Menlo File Security for Email solution does not require internet connectivity to run the Positive Selection® Engine.

Optional Integrations

Menlo offers optional integration with Email Servers, Web Proxies, and Web Applications. For more information and pricing please consult with your Menlo Security representative.

About Menlo Security

[Menlo Security](#) eliminates evasive threats and protects productivity with the Menlo Cloud. Menlo delivers on the promise of cloud-based security—enabling zero trust access that is simple to deploy. The Menlo Cloud 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. © 2025 Menlo Security, All Rights Reserved.



Learn more: <https://www.menlosecurity.com>
Contact us: ask@menlosecurity.com

