Trend Micro™ ScanMail™ Suite for Microsoft Exchange™

Superior protection. Less administration.

Most targeted attacks and ransomware incidents start with phishing emails, making email security more important than ever. Unfortunately, most mail server security solutions—including the limited set of built-in protections in the Microsoft Exchange Server—rely on older technologies. These solutions struggle to detect modern malware, malicious macros and URLs, and fileless attacks.

Trend Micro™ ScanMail™ Suite for Microsoft Exchange™ enables you to stop targeted phishing and ransomware attacks. This is achieved by using predictive machine learning, document exploit detection, and custom sandbox analysis of suspicious files and URLs—protection you can't get with other solutions.

Time-saving features like central management, search and destroy, and role-based access have earned ScanMail its reputation among the easiest security solutions to set up and operate.

Advantages

Superior protection against targeted phishing and ransomware attacks

- Gain access to the most advanced detection techniques. This includes predictive machine learning and document exploit detection to help find unknown threats in files, macros, and scripts.
- Block emails with malicious URLs before delivery. Re-analyze URLs in real-time when your users click.
- Stop multi-stage attacks which use emails sent internally from compromised accounts or devices.
- Combine with Trend Micro™ Deep Discovery™ Analyzer. Dynamically analyze suspicious files/URLs found in custom sandboxes and share indicators of compromise (IoCs) with Trend Micro and third-party security solutions.
- Catch business email compromise (BEC) attacks by using AI. Utilize expert system and machine learning to examine email header and content and authorship. Apply more stringent protection for your high-profile users.
- Prevent executive spoofing scams with our unique Trend Micro™ Writing Style DNA technology. Use this protection for ScanMail to check the writing style of an incoming English email—claimed to be from an executive—against a trained machine learning model of that executive's writing.

Lower IT costs

- Streamline email security operations with strong group management, centralized reporting, and log forwarding to security information event management (SIEM) platforms.
- Ease the cumbersome task of organization email search requests by leveraging our innovative search and destroy feature.
- Simplify compliance and data privacy initiatives with centrally managed, template-based DLP.

Software

Protection Points

- Mail server
- Internal inspection
- Inbound and outbound data

Threat and Data Protection

- Anti-malware
- Ransomware
- Web threat protection
- Anti-spam
- Anti-phishing
- Content filtering
- Data loss protection (DLP)
- Targeted attacks

Key Features

Protection from spear phishing and targeted attacks

- Unlike other email security solutions, ScanMail features enhance web reputation, document exploit detection, sandbox execution analysis, and custom threat intelligence. Together, these advanced capabilities provide you with comprehensive security against email threats. This includes spear phishing attacks associated with targeted threats.
- Detect known and unknown exploits in Adobe PDF, Microsoft 365, and other document formats.
- Perform malware execution analysis and generate custom threat intelligence and adaptive security updates with optional Deep Discovery Analyzer integration.
- Stop threats from entering your environment with immediate protection based on leading global threat intelligence.

DLP

- Extend your existing security to support compliance and prevent data loss. Integrated DLP simplifies data protection by giving you visibility and control of data in motion and at rest.
- Discover and track sensitive data flowing through your email system and in the mail store.
- Accelerate setup and improve accuracy with 100+ compliance templates.
- Enable compliance personnel to centrally manage DLP policies and violations across other Trend solutions, from endpoint to gateway, with Trend Micro™ Control Manager™.

Optimized for Exchange

- ScanMail is tightly integrated with your Microsoft environment to efficiently protect your organization's email with the least overhead.
- Gain support for hybrid Microsoft 365 and Exchange Server environments in conjunction with Trend Micro™ Cloud App Security.
- Maximize efficiency to avoid duplication, multi-threaded scanning, and CPU throttling.
- Leverage Integration with Microsoft System Center Operations Manager and Microsoft Outlook Junk Email Filter.
- Prevent unauthorized policy changes with role-based access control.

Innovative search and destroy capability

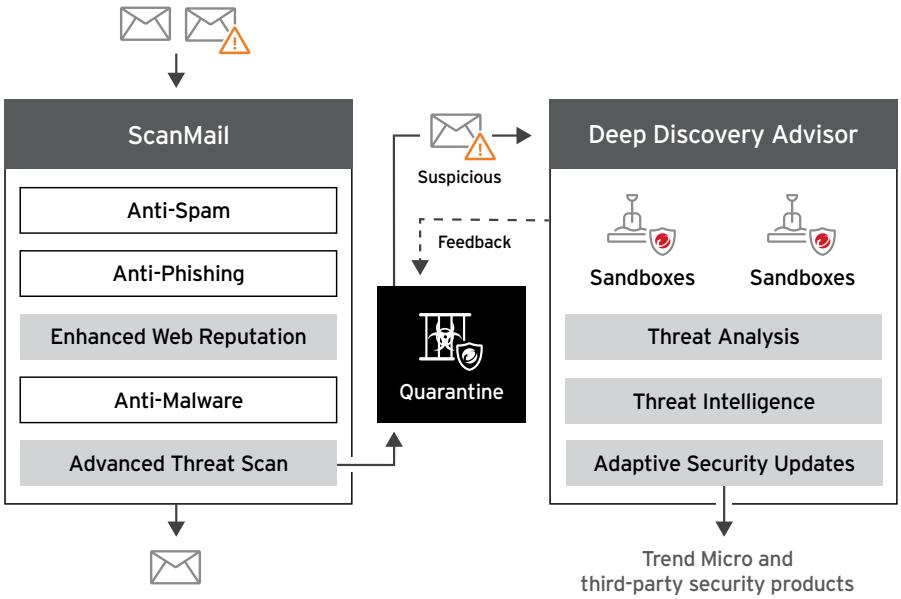
- Unlike the tools built into Exchange, ScanMail search and destroy can find emails swiftly and accurately.
- Perform targeted searches through Exchange using keywords and regular expressions.
- Empower administrators to quickly respond to urgent requests from legal, human resources, or security departments. Find, trace, and if necessary, permanently delete specific emails.

Key Benefits

- Protect your employees from targeted attacks, like spear phishing
- Leverage leading cloud-based security to stop threats at the mail server, before they reach your end users
- Gain visibility and control of data to prevent data loss and support compliance
- Accelerate throughput with native 64-bit processing
- Lower administration and total cost of ownership (TCO) with central management

Connected Threat Defense

Trend messaging security solutions integrate with Deep Discovery Analyzer for sandbox execution and sharing of IoCs. This connects your email, endpoint, and network defenses—enabling you to detect, analyze, adapt, and respond to targeted attacks.



ScanMail Suite

The ScanMail Suite has been enriched with built-in protections against targeted attacks.

- **Enhanced URL protection** allows you to block emails with malicious URLs in the message body or in attachments. URL time-of-click helps you re-analyze websites upon user access. It's powered by the Trend Micro™ Smart Protection Network™, which correlates threat information with big data analytics and predictive technology.
- **Advanced Threat Scan Engine** enables you to detect advanced malware in Adobe PDF, Microsoft 365 macros, scripts, and other formats. Predictive machine learning and heuristic logic lets you detect known and zero-day exploits. Scan the Exchange mail store for targeted threats that may have entered before protection was available.
- **When Integrated with Deep Discovery Analyzer**, ScanMail allows you to quarantine suspicious attachments and URLs for automatic sandbox execution analysis. This occurs inline—without impacting the delivery of the vast majority of your users' messages.

Deep Discovery Analyzer (Additional Purchase)

This hardware appliance that provides sandboxing, deep threat analysis, and local security updates in a unified intelligence platform is the heart of our unified platform.

- **Custom threat analysis** provides you with automatic in-depth simulation analysis of potentially malicious attachments and URLs in a secure sandbox environment. Create and analyze suspicious objects against multiple customized target images that precisely match their host environments. Its patented sandbox technology is certified by ICSA Labs.
- **Custom threat intelligence** links information on attacks in your environment with extensive Trend threat intelligence. This provides in-depth insights for risk-based incident assessment, containment, and remediation.
- **Adaptive security updates**, with custom-generated patterns of malicious files, help you locate new command and control (C&C) servers and malicious download sites found during sandbox analysis. This adapts and improves the protection of Trend endpoint and gateway products, as well as third-party network security layers.

System Requirements

ScanMail Suite supports all virtual environments compatible with Exchange.

ScanMail with Microsoft Exchange Server 2019

	REQUIREMENTS
Processor	• x64 architecture-based processor that supports Intel 64 architecture (formally known as Intel EM64T) • x64 architecture-based computer with AMD 64-bit processor that supports AMD64 platform
Memory	• 4 GB RAM exclusively for ScanMail
Disk Space	• 5 GB free disk space
Operating System	• Microsoft Windows Server 2019 Standard or Data Center **Note:** For ScanMail deployment on Server Core edition, Trend recommends running the installation package on Windows Server with the Desktop Experience feature and deploy ScanMail remotely
Mail Server	• Microsoft Exchange Server 2019
Web Server	• Microsoft Internet Information Services (IIS) 10.0
Browser	• Microsoft Internet Explorer 7.0 or later • Mozilla Firefox 3.0 or later
MSXML	• 4.0 SP2 or later
.NET Framework	• 4.7.2

ScanMail with Microsoft Exchange Server 2016 or Exchange Server 2013

	REQUIREMENTS
Processor	• x64 architecture-based processor that supports Intel 64 architecture (formally known as Intel EM64T) • x64 architecture-based computer with AMD 64-bit processor that supports AMD64 platform
Memory	• 1 GB RAM exclusively for ScanMail (2 GB RAM recommended)
Disk Space	• 5 GB free disk space
Operating System	• Microsoft Windows Server 2016 Standard or Data Center • Microsoft Windows Server 2012 R2 Standard or Data Center • Microsoft Windows Server 2012 Standard or Data Center • Microsoft Windows Server 2008 R2 Standard or Enterprise with SP1
Mail Server	• Microsoft Exchange Server 2016 • Microsoft Exchange Server 2013 SP1 or later
Web Server	• Microsoft Internet Information Services (IIS) 10.0 • Microsoft Internet information Services (IIS) 8.5 • Microsoft Internet information Services (IIS) 8.0 • Microsoft Internet information Services (IIS) 7.5
Browser	• Internet Explorer 7.0 or later • Mozilla Firefox™ 3.0 or later
MSXML	• 4.0 SP2 or above
.NET Framework	• 4.5 or later