Trend Micro™

SCANMAIL™ SUITE FOR MICROSOFT® EXCHANGE™

Superior protection. Less administration.

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

ScanMail™ Suite for Microsoft® Exchange™ stops targeted phishing and ransomware attacks 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 as one of the simplest security solutions to setup and operate.

ADVANTAGES

Superior protection against targeted phishing and ransomware attacks

- Utilizes the most advanced detection techniques, including predictive machine learning and document exploit detection, to find unknown threats in files, macros, and scripts.
- Blocks emails with malicious URLs before delivery and re-analyzes URLs in real time when a user clicks.
- Stops multi-stage attacks which use emails sent internally from compromised accounts or devices.
- When combined with Trend Micro™ Deep Discovery™ Analyzer, suspicious files/URLs are dynamically analyzed in custom sandboxes and indicators of compromise (IOCs) are shared with Trend Micro and third-party security solutions.
- Catches business email compromise (BEC) attacks by using artificial intelligence (AI), including expert system and machine learning, to examine email header, content and authorship, and applies more stringent protection for high-profile users.
- Prevents executive spoofing scams using our unique **Writing Style DNA** technology. This protection for ScanMail checks 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.

LOWERS IT COSTS

- Streamlines email security operations with strong group management, centralized reporting, and log forwarding to security information event management (SIEM) platforms.
- Eases the cumbersome task of organization email search requests through its innovative search and destroy feature.
- Simplifies compliance and data privacy initiatives with centrally managed, template-based data loss prevention (DLP).

Software

Protection Points

- Mail server
- Internal inspection
- Inbound and outbound data

Threat and Data Protection

- Antivirus
- Ransomware
- Web threat protection
- Antispam
- Antiphishing
- Content filtering
- DLP
- Targeted attacks

KEY FEATURES

Protection from Spear Phishing and Targeted Attacks

Unlike other email security solutions, ScanMail features enhanced web reputation, document exploit detection, sandbox execution analysis, and custom threat intelligence. Together, these advanced capabilities provide comprehensive security against email threats, including spear phishing attacks associated with targeted threats.

- Detects known and unknown exploits in Adobe® PDF, Microsoft® Office®, and other document formats.
- Performs malware execution analysis, and generates custom threat intelligence and adaptive security updates with optional Deep Discovery Analyzer integration.
- Stops threats from entering your environment with immediate protection based on leading global threat intelligence.

Data Loss Prevention

Extends 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.

- Discovers and tracks sensitive data flowing through your email system and in the mail store.
- Accelerates setup and improves accuracy with 100+ compliance templates.
- Enables compliance personnel to centrally manage DLP policies and violations across other Trend Micro products from endpoint to gateway with Trend Micro™ Control Manager™.

Optimized for Exchange

ScanMail is tightly integrated with your Microsoft environment to efficiently protect email with the least overhead.

- Supports hybrid Microsoft® Office 365® and Exchange Server environments in conjunction with Trend Micro™ Cloud App Security.
- Maximizes efficiency with TrustScan to avoid duplication, multi-threaded scanning and computer processing unit (CPU) throttling.
- Integrates with Microsoft® System Center Operations Manager and Microsoft® Outlook® Junk Email Filter.
- Prevents 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.

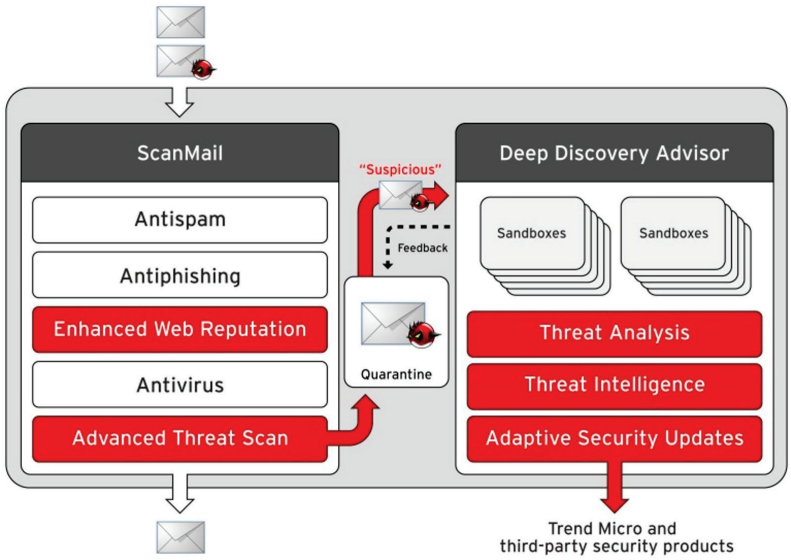
- Performs targeted searches through Exchange using keywords and regular expressions.
- Allows administrators to quickly respond to urgent requests from legal, human resources, or security departments to find, trace, and if necessary, to permanently delete specific emails.

Key Benefits

- Protects individuals from targeted attacks, like spear phishing.
- Provides leading cloud-based security to stop threats at the mail server, before they reach end users.
- Provides visibility and control of data to prevent data loss and support compliance.
- Speeds throughput with native 64-bit processing.
- Lowers administration and total cost of ownership (TCO) with central management.

CONNECTED THREAT DEFENSE

Trend Micro messaging security solutions can 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 blocks emails with malicious URLs in the message body or in attachments. URL time-of-click re-analyzes 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 detects advanced malware in Adobe PDF, Office macros, scripts, and other formats using predictive machine learning and heuristic logic to detect known and zero-day exploits. It also scans the Exchange mail store for targeted threats that may have entered before protection was available.

When Integrated with Deep Discovery Analyzer, ScanMail quarantines suspicious attachments and URLs for automatic sandbox execution analysis which occurs inline—without impacting the delivery of majority of messages.

DEEP DISCOVERY ANALYZER (ADDITIONAL PURCHASE)

Deep Discovery Analyzer is a hardware appliance that provides sandboxing, deep threat analysis, and local security updates in a unified intelligence platform that is the heart of the Trend Micro Connected Threat Defense.

Custom Threat Analysis provides automatic in-depth simulation analysis of potentially malicious attachments and URLs in a secure sandbox environment. It allows customers to create and analyze suspicious objects against multiple customized target images that precisely match their host environments. Its patented sandbox technology tested at 100 percent effective against threats and evasion in the 2017 NSS Labs Breach Detection Test.

Custom Threat Intelligence links information on attacks in your environment with extensive Trend Micro threat intelligence to provide in-depth insights for risk-based incident assessment, containment, and remediation.

Adaptive Security Updates issues security updates with custom-generated patterns of malicious files and locations of new command and control (C&C) servers malicious download sites found during sandbox analysis. This adapts and improves the protection of Trend Micro endpoint and gateway products, as well as third-party network security layers.

SYSTEM REQUIREMENTS

ScanMail Suite supports all virtual environments compatible with Exchange.

SYSTEM REQUIREMENTS FOR EXCHANGE

ScanMail with Microsoft Exchange Server 2019

RESOURCE	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	• 4GB RAM exclusively for ScanMail
Disk Space	• 5GB free disk space
Operating System	• Microsoft® Windows Server® 2019 Standard or Datacenter • Note: For ScanMail deployment on Server Core edition, Trend Micro 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

RESOURCE	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	• 1GB RAM exclusively for ScanMail (2GB RAM recommended)
Disk Space	• 5GB free disk space
Operating System	• Microsoft® Windows Server® 2016 Standard or Datacenter • Microsoft® Windows Server® 2012 R2 Standard or Datacenter • Microsoft® Windows Server® 2012 Standard or Datacenter • 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

TREND MICRO™

Securing Your Connected World

©2019 by Trend Micro Incorporated. All rights reserved. Trend Micro, and the Trend Micro t-ball logo, OfficeScan and Trend Micro Control Manager are trademarks or registered trademarks of Trend Micro Incorporated. All other company and/or product names may be trademarks or registered trademarks of their owners. Information contained in this document is subject to change without notice. [DS00_SMEX_190411US]