Trend Micro™

# ScanMail™ Suite for Microsoft® Exchange™

Superior protection. Less administration.

More than 90% of targeted attacks begin with a spear phishing email, which means your mail server security is more important than ever. Unfortunately, most mail server security solutions, including the limited set of built-in protections in Exchange 2013, rely on pattern file updates, which only detect traditional malware. They don't include specific protections to detect malicious URLs or document exploits commonly used in targeted attacks or advanced persistent threats (APTs).

**ScanMail™ Suite for Microsoft® Exchange™** stops highly targeted email attacks and spear phishing by using document exploit detection, enhanced web reputation, and sandboxing as part of a custom APT defense—protection you don't get with other solutions. In addition, only ScanMail blocks traditional malware with email, file, and web reputation technology and correlated global threat intelligence from Trend Micro™ Smart Protection Network™ cloud-based security.

Time-saving features like central management, template-based Data Loss Prevention (DLP), and role-based access have earned ScanMail the lowest administration overhead and TCO of the five leading security vendors, based on a comparison study by Osterman Research. ScanMail also delivers high performance with native 64-bit support—for the fastest mail throughput speeds.

**SOFTWARE**

**Protection Points**

- Mail server
- Internal inspection
- Inbound and outbound data

**Threat and Data Protection**

- Antivirus
- Web threat protection
- Antispam
- Antiphishing
- Content filtering
- Data loss prevention
- Targeted attacks, APTs

## ADVANTAGES

### Protects organizations from APTs and other targeted attacks

- Minimizes targeted attacks with multiple protection technologies
- Performs execution analysis on your unique environment and provides custom threat intelligence via Deep Discovery Advisor integration
- Issues custom security updates to other security layers to remediate and prevent further attacks from similar malware

### Blocks more malware, phishing, and spam with reputation technology

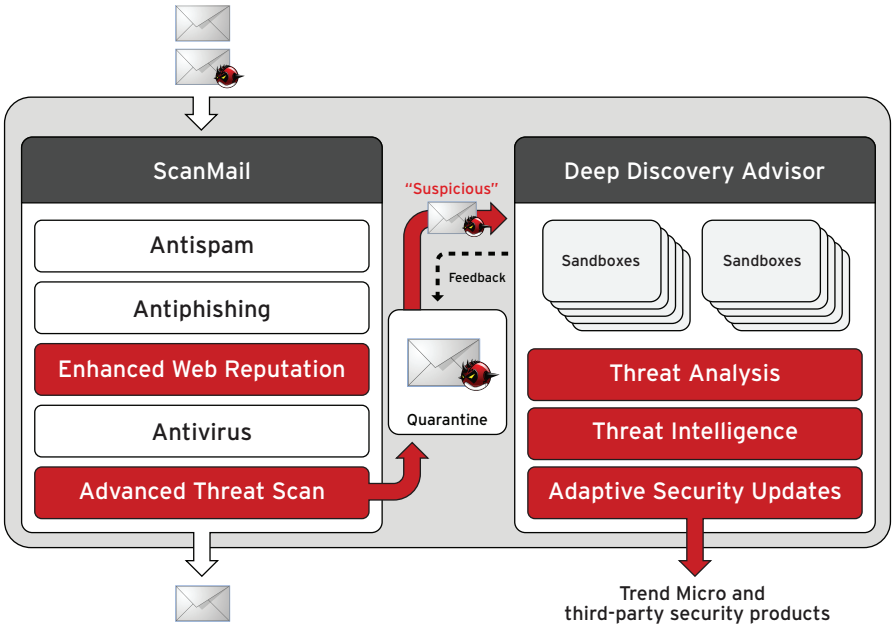
- Detects malware attachments and malicious web links to prevent malware downloads
- Utilizes correlated email, file, and web reputation to block more messaging threats—the only mail server security to do this
- Stops more spam than other security solutions based on Opus One independent tests

### Lowers IT costs, enhances performance

- Streamlines email security operations with strong group configuration and management, and centralized logging and reporting
- Simplifies compliance and data privacy initiatives with centrally managed, template-based DLP
- Lowers administration overhead and TCO, beating four other leading solutions, based on an Osterman Research study

## TARGETED ATTACKS NEED A CUSTOM DEFENSE

Trend Micro messaging security solutions provide protection against targeted attacks with enhanced web reputation, a new detection engine, and new sandbox execution for in-depth threat analysis. Integration of these components provides a custom defense that enables you to detect, analyze, adapt, and respond to targeted attacks.




### ScanMail Suite

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

**Enhanced Web Reputation** blocks emails with malicious URLs in the message body or in attachments. 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, MS Office, and other documents formats using static 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 Trend Micro™ Deep Discovery Advisor**, ScanMail quarantines suspicious attachments for automatic sandbox execution analysis which occurs in-line without impacting the delivery of majority of messages.

### Deep Discovery Advisor (additional purchase)

Deep Discovery Advisor is an appliance that provides sandboxing, network-wide log collection, and deep threat analysis in a unified intelligence platform that is the heart of Trend Micro Custom Defense.

**Custom Threat Analysis** provides automatic in-depth simulation analysis of potentially malicious attachments, including executables and common office documents in a secure sandbox environment. It allows customers to create and analyze multiple customized target images that precisely match their host environments.

**Custom Threat Intelligence** analyzes logs of Trend Micro products and third-party solutions combined with Trend Micro threat intelligence to provide in-depth insights for risk-based incident assessment, containment and remediation.

**Adaptive Security Updates** issues custom security updates for adaptive protection and remediation by ScanMail, other Trend Micro products, and third-party security at various layers.

## 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 APTs and other targeted threats.

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

### Data Loss Prevention Add-on Module

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.

- Tracks sensitive data flowing through your email system and in the mail store
- Accelerates setup and improves accuracy with 100+ compliance templates
- Simplifies deployment with an add-on for immediate data loss prevention, requiring no additional hardware or software, enabling granular Active Directory-based policy enforcement
- Enables compliance personnel to centrally manage DLP policies and violations across other Trend Micro products from endpoint to gateway with Control Manager™

### Optimized for Microsoft® Exchange

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

- Accelerates throughput—up to 57 percent faster than other solutions
- Avoids duplicate inspection with AV stamp multi-threaded scanning and CPU throttling
- Scans efficiently with native 64-bit support
- Integrates with Microsoft® System Center Operations Manager and Outlook® Junk E-mail 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 permanently delete specific emails if necessary

## 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 through-put with native 64-bit processing
- Accelerates throughput, performing 57% faster than MS Forefront
- Lowers administration and TCO with central management

### Unique Reputation Technology for Blocking Spam, Phishing, and Malware

Uses big data analytics and predictive technology to correlate file, web, and email reputation data in the cloud for immediate protection from emerging threats—before they can reach end users who may be accessing email on laptops or mobile devices.

- Checks for malicious links within both the email body and attachments to block phishing attacks via enhanced web reputation
- Drops up to 85 percent of all incoming email using email sender reputation to free network resources
- Stops more spam than other security solutions according to independent tests

## SYSTEM REQUIREMENTS

**ScanMail Suite supports all virtual environments compatible with Microsoft Exchange.**

| MINIMUM SYSTEM REQUIREMENTS | | | |
|---|---|---|---|
| Memory | Disk Space | Browser | Web Server |
| 1GB RAM, 2GB RAM recommended (Exclusively for ScanMail) | 2GB free disk space | • Microsoft Internet Explorer 6.0, 7.0, 8.0, and 9.0 (Compatibility view is suggested)<br>• Mozilla Firefox 3.0 or later<br>• MSXML<br>• MSXML 4.0 SP2 or above | Microsoft Internet Information Services (IIS) 6.0 or 7.0 |

| SYSTEM REQUIREMENTS FOR MICROSOFT EXCHANGE | | | | |
|---|---|---|---|---|
| | Processor | Operating System | Mail Server | Web Browser |
| Microsoft Exchange 2010 | • x64 architecture-based processor that supports Intel Extended Memory 64 Technology (Intel EM64T)<br>• x64 architecture-based computer with AMD 64-bit processor that supports AMD64 platform | • Microsoft Windows Server 2008 with Service Pack 2 (64-bit)<br>• Microsoft Windows Server 2008 R2 with Service Pack 1 (64-bit)<br>• Microsoft Windows Server 2008 R2 (64-bit)<br>• Microsoft Small Business Server (SBS) 2011 | • Microsoft Exchange Server 2010 with Service Pack 1 or 2<br>• Microsoft Exchange Server 2010 | • Microsoft Internet Information Services (IIS) 7.5<br>• Microsoft Internet Information Services (IIS) 7.0 |
| Microsoft Exchange 2007 | • x64 architecture-based processor that supports Intel Extended Memory 64 Technology (Intel EM64T)<br>• x64 architecture-based computer with AMD 64-bit processor that supports AMD64 platform | • Microsoft Windows Server 2008 with Service Pack 2 (64-bit)<br>• Microsoft Windows Server 2008 R2 with Service Pack 1 (64 bit)<br>• Microsoft Windows Server 2008 R2 (64 bit)<br>• Microsoft Windows Small Business Server 2008 (64 bit)<br>• Microsoft Windows Server 2003 R2 with Service Pack 2 (64-bit)<br>• Microsoft Windows Server 2003 with Service Pack 2 (64-bit) | Microsoft Exchange Server 2007 with Service Pack 1, 2 or 3 | • Microsoft Internet Information Services (IIS) 7.5<br>• Microsoft Internet Information Services (IIS) 7.0 |
| Microsoft Exchange 2003 | Intel(TM) Pentium II 266 MHz or higher processor (Intel Pentium or compatible 733MHz processor recommended) | • Microsoft Windows Server 2003 with Service Pack 2 (32-bit)<br>• Microsoft Windows Server 2003 R2 with Service Pack 2 (32-bit) | Microsoft Exchange Server 2003 with Service Pack 2 | • Microsoft Internet Information Services (IIS) 7.5<br>• Microsoft Internet Information Services (IIS) 7.0 |