Trend Micro™

INTERSCAN™ MESSAGING SECURITY

Stop inbound threats. Secure outbound data.

More than 90 percent of all email is spam. With the rise of targeted spear phishing, even your savviest employees can mistakenly click on a malicious link and expose your enterprise to cybercrime.

Trend Micro™ InterScan™ Messaging Security provides the most comprehensive protection against both traditional and targeted attacks. Using the correlated intelligence from Trend Micro™ Smart Protection Network™ and optional sandbox execution analysis, it blocks spam, phishing, and advanced persistent threats (APTs). The included hybrid SaaS deployment option combines a powerful gateway virtual appliance with a SaaS pre-filter that stops majority of threats and spam in the cloud–closer to their source. This hybrid solution delivers the best of both worlds: the privacy and control of an on-premises appliance with an in-the-cloud pre-filter for resource efficiency and proactive protection.

The Data Privacy and Encryption Module solves the toughest regulatory compliance and data protection challenges by securing outbound data. This optional module offers easy-to-use identity-based encryption and customizable data loss prevention (DLP) templates for quick deployment.

MAIL GATEWAY SECURITY

Protection Points

- Messaging gateway
- Inbound and outbound data
- Internet cloud

Threat Protection

- Targeted attacks
- Ransomware
- Compliance risks
- Data loss
- Inappropriate content
- Malicious web links
- Spear phishing
- Spam and botnets
- Spyware
- Viruses

ADVANTAGES

Protects organizations from APTs and other targeted attacks

- Minimizes targeted attacks with ScanMail™ multiple protections
- Performs execution analysis on your unique environment, and provides custom threat intelligence via Trend Micro™ Deep Discovery™ Analyzer integration (optional)
- Detects spear phishing emails with Trend Micro **Social Engineering Attack Protection**
- Includes protection for **Business Email Compromise (BEC)**, a popular new phishing technique mainly using executive spoofing
- Provides time-of-click protection against malicious URLs in email messages–rewrites and analyzes URLs at the time of click and blocks them if they are malicious

Blocks more malware, phishing, and spam with reputation technology

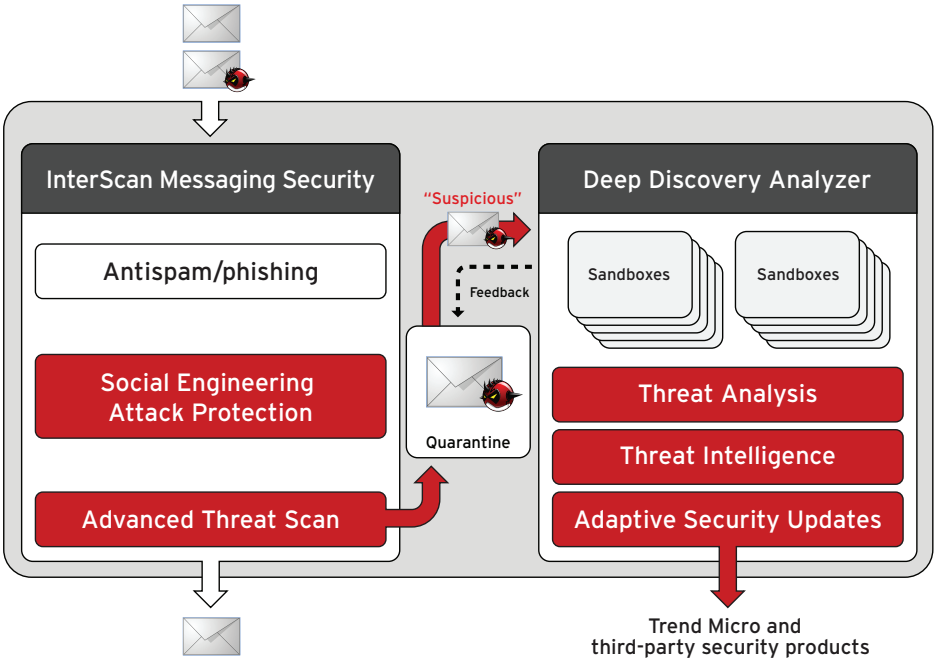
- Drops up to 85 percent of all incoming email using email sender reputation to free network resources
- Stops more spam with fewer false positives than other security solutions according to independent tests
- Tags graymail messages such as bulk marketing newsletters for optional sorting
- Checks for malicious links within the email to block phishing attacks via enhanced web reputation

Simplifies Data Protection and Encryption

- Makes securing outbound email to anyone easier through identity-based email encryption
- Eliminates pre-enrollment and certificate management of PKI encryption via dynamic key generation
- Simplifies regulatory compliance and data loss prevention with over 200 customizable DLP templates
- Reduces time management and speeds compliance audits using detailed reporting

TARGETED ATTACKS NEED A NETWORK DEFENSE

Trend Micro messaging security products provide protection against targeted attacks with enhanced web reputation, an advanced threat scan detection engine, social engineering attack protection, and a threat analysis appliance that blocks highly targeted email attacks by using sandbox execution analysis. Integration of these components provides a network defense that enables you to detect, analyze, adapt, and respond to targeted attacks.



> "Hybrid protection offered by the InterScan Messaging Security Virtual Appliance represents a very cost-effective and forward-looking solution forlarge organizations like ours."
>
> **Steven Jones**
> Senior Systems Administrator
> Dane County, Wisconsin

INTERSCAN MESSAGING SECURITY COMPONENTS

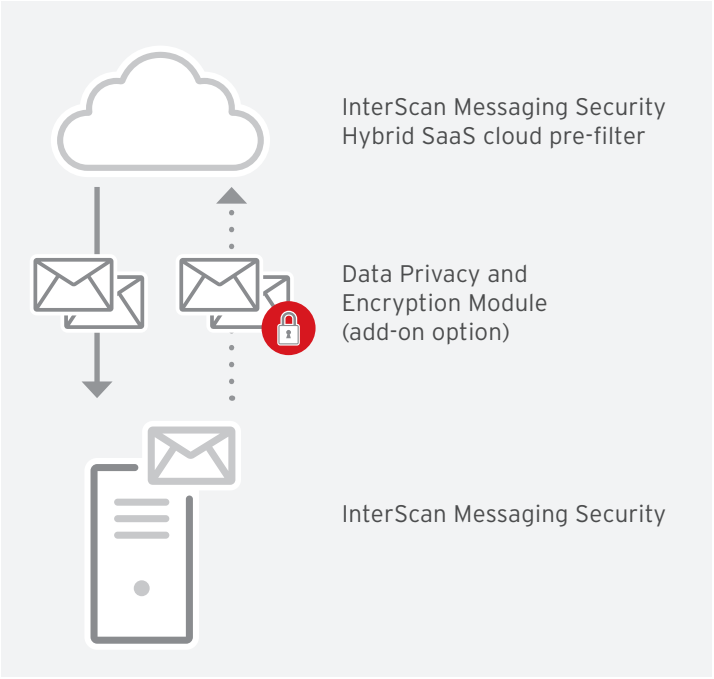
InterScan Messaging Security has been enriched with built-in protections against targeted attacks.

- **Enhanced Web Reputation** blocks emails with malicious URLs in the message body or in attachments. Its 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. When integrated with Deep Discovery Analyzer, it quarantines suspicious attachments for automatic sandbox execution analysis which occurs in-line without impacting the delivery of majority of messages
- **Social Engineering Attack Protection** identifies targeted attack emails by correlating email components such as the header, body, and network routing

DEEP DISCOVERY ANALYZER COMPONENTS (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 Trend Micro Network 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 on new malicious download sites and targeted attack command and control (C&C) locations found during sandbox analysis. Custom updates enable adaptive protection and remediation by Trend Micro endpoint, data center, and web security products, and third-party security layers



VIRTUAL APPLIANCE HYBRID SAAS DEPLOYMENT

Virtual appliance + cloud security: Trend Micro integrated hybrid SaaS gives you one unified console to manage everything—the cloud pre-filter service, virtual appliance content security, and the add-on Data Protection and Encryption Module.

KEY FEATURES

Inbound in-the-cloud email filtering

- Lowers impact at the email gateway by filtering email in the cloud
- Reduces data center footprint and lowers IT staff time
- Allows you to deploy new capacity quickly where needed
- Includes Service Level Agreement that ensures email traffic uptime

Add-on Data Privacy and Encryption Module

(additional license required; available for virtual appliance or software appliance deployments)

- Triggers automatic encryption, quarantine, or notification-based filtering policies
- Speeds set up of DLP content filtering rules with customizable compliance templates
- Reduces your reliance on user-driven encryption with an automated policy-driven gateway solution
- Eliminates the complexity of key management with identity-based encryption
- Enables compliance personnel to centrally manage DLP policies, and violations across other Trend Micro products from endpoint to gateway with Trend Micro Control Manager™

Real-time protection from evolving threats

- Queries web reputation database in real time to block emails containing malicious links
- Checks email reputation to block mail from spam sources and rogue "fast flux" service networks
- Improves accuracy and responsiveness with in-the-cloud threat correlation
- Detects spear phishing emails with Trend Micro **Social Engineering Attack Protection**
- Includes protection for **Business Email Compromise (BEC)**, a popular new phishing technique mainly using executive spoofing
- Identifies bulk marketing messages to allow separate dispositions for these emails
- Detects and blocks botnet and targeted attack C&C communications
- Provides time-of-click protection against malicious URLs in email messages—rewrites and analyzes URLs at the time of click and blocks them if they are malicious

Single management console for customization and control

- Streamlines management of cloud pre-filter, scanning of on-premises content, and DLP and encryption
- Supports customizable policies and granular, rule-based filtering
- Identifies bulk marketing messages to allow customers to manage with separate policies
- Integrates quarantines, logs, and reports for easy management, message tracking and visibility

Blocks ransomware before it ever gets to your users

- Detects and blocks ransomware with malware scanning, anti-spam, and file (including executables and macro) scanning
- Gives you advanced threat protection with sandbox malware analysis (optional), social engineering protection, and zero-day and document exploit detection
- Uses web reputation to protect against web links in emails that are malicious

Connected Threat Defense

Using the Control Manager™ console, you can specify customized actions for malicious objects detected by other Trend Micro endpoints, gateways, and network breach detection technology. This allows you to provide a custom defense against targeted threats specific to your environment.

Virtual Appliance

Operating System

A standard CentOS™ Linux™ operating system is contained within InterScan Messaging Security Virtual Appliance (IMSVA)

Hardware Requirements for Bare Metal Server

Recommended System Requirements

- 8-core Intel™ Xeon™ processor or equivalent
- 8 GB RAM
- 250 GB hard disk space or more. IMSVA automatically partitions the detected disk space based on recommended Linux practices
- Monitor that supports 800 x 600 resolution with 256 colors or higher

Minimum System Requirements

- Dual-core Intel Xeon processor or equivalent
- 4 GB RAM
- At least 120 GB hard disk space. IMSVA automatically partitions the detected disk space based on recommended Linux practices
- Monitor that supports 800 x 600 resolution with 256 colors or higher

To obtain a list of Trend Micro certified servers that are guaranteed to be compatible with IMSVA, access the following URL:
http://www.trendmicro.com/go/certified

To obtain a list of available platforms that should operate with IMSVA, access the following URL:
http://wiki.centos.org/HardwareList

System Requirements for Virtual Machines

Recommended Virtual Machine Requirements and System Settings

- 8-core Intel Xeon processor or equivalent
- 8 GB RAM
- 250 GB of disk space or more. IMSVA automatically partitions the detected disk space based on recommended Linux practices

Minimum Virtual Machine Requirements and System Settings

- Dual-core Intel Xeon processor or equivalent
- 4 GB RAM
- 120 GB disk space. IMSVA automatically partitions the detected disk space based on recommended Linux practices

Platform support

- VMware ESXi 5.0 Update 3
- VMware ESXi 5.5 Update 2
- VMware ESXi 6.0
- Microsoft™ Windows™ Server 2008 R2 Service Pack 1 with Hyper-V™
- Windows Sever 2012 with Hyper-V
- Windows Sever 2012 R2 with Hyper-V
- Microsoft Hyper-V Server 2008 R2 Service Pack 1
- Microsoft Hyper-V Server 2012 R2

Software Deployment

Microsoft™ Windows™, Linux™

- 2G RAM of memory
- 80 GB hard disk space - 500MB of disk space for installation and additional disk space needed for mail storage and database
- Microsoft Internet Explorer 6 SP1, 7, 8 or Firefox 3 or above
- LDAP Server Microsoft Active Directory 2000 or 2003, IBM Lotus Domino 6.0 or above, or Sun One LDAP

Microsoft® Windows™

- Windows Server 2012, 2012 R2
- Windows Server 2008 SP2, 2008 R2 SP1
- Windows Server 2003 SP2, 2003 R2 SP2
- Intel Dual Pentium 3GHz or higher
- Microsoft SQL Server 2008 or above, SQL Express 2008 or above

Linux

- Red Hat™ Enterprise Linux 3, 4, 5 or 6
- Intel Dual Pentium IV 3 GHz
- 2GB swap space
- PostgreSQL version 8.1.3 or above
- MTA Postfix 2.1 or above; Sendmail; Qmail

TREND MICRO™

Securing Your Journey to the Cloud