

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-premise 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
- 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 Deep Discovery Analyzer integration
- Detects spear phishing emails with new Trend Micro Social Engineering Attack Protection

Blocks more malware, phishing, and spam with reputation technology

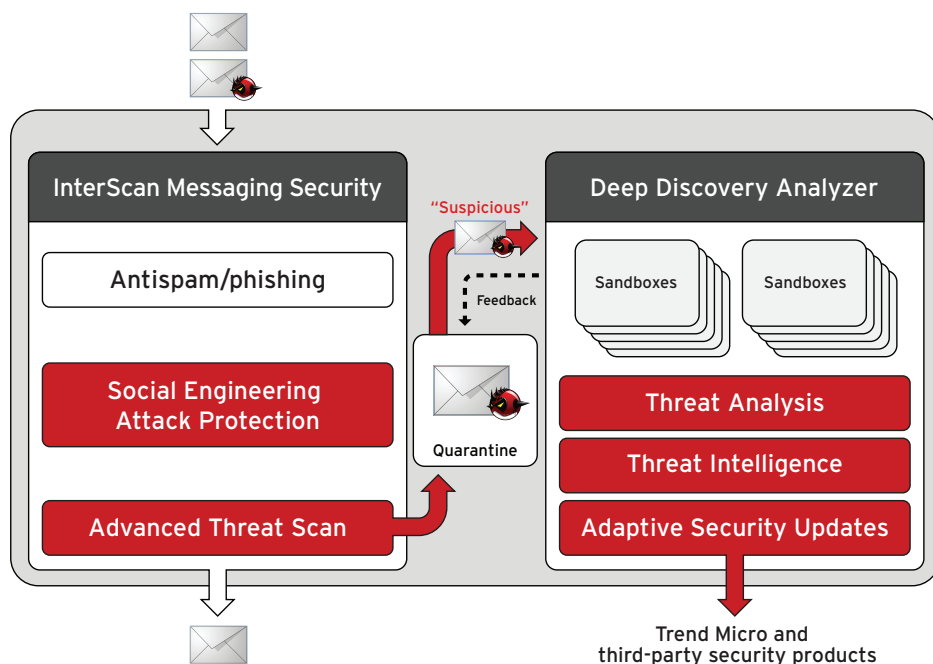
- Drops up to 85 percent of all incoming email using email sender reputation to free network resources
- Stops more spam with fewer false positives than other security solutions according to independent tests
- Tags graymail messages such as bulk marketing newsletters for optional sorting
- Checks for 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 CUSTOM DEFENSE

Trend Micro messaging security products provide protection against targeted attacks with enhanced web reputation, a new detection engine, and a new threat analysis appliance that blocks highly targeted email attacks by using sandbox execution analysis. Integration of these components provides a custom 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 for large 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 Trend Micro™ 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 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 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 datacenter 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 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
- Identifies bulk marketing messages to allow separate dispositions for these emails
- Detects and blocks botnet and targeted attack C&C communications

Single management console for customization and control

- Streamlines management of cloud pre-filter, scanning of on-premise 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

Key Benefits

- Saves resources by stopping spam in the cloud, outside your network
- Protects against malicious links and in spear phishing attacks
- Blocks targeted malware with sandbox analysis
- Minimizes risk with real-time, predictive protection
- Encrypts sensitive outbound email
- Prevents data loss and compliance risks
- Reduces management and overall costs
- Furthers datacenter consolidation initiatives

VIRTUAL AND SOFTWARE APPLIANCES

Server Platform Compatibility

- Virtual Appliances:
 - VMware ESX v4.0, 4.1 or ESXi 4.0, 4.1, 5.0, 5.5
 - Microsoft Windows Server with Hyper-V 2008 R2 SP1, 2012, 2012 R2 or Microsoft Windows Hyper-V Server 2008 R2 SP1, 2012 R2
- Software Appliances: for the latest Certified by Trend Micro platforms, please go to www.trendmicro.com/go/certified

Minimum Hardware Requirements

- Dual-core Intel™ Xeon processor or equivalent
- 4GB RAM
- 120GB of disk space

Recommended Hardware Requirements

- 8-core Intel™ Xeon processor or equivalent
- 8GB RAM
- 250GB of disk space

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
- 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
- PostgreSQL version 8.1.3 or above
- Intel Dual Pentium IV 3 GHz
- MTA Postfix 2.1 or above; Sendmail; Qmail
- 2GB swap space

Flexible Deployment

Virtual Appliance: virtualized deployments via Hypervisor technologies. Includes hybrid SaaS pre-filter and option to purchase Data Privacy and Encryption module.

- Microsoft® Hyper-V™ Virtual Appliance
- VMware Ready Virtual Appliance: Rigorously tested and validated by VMware, achieving VMware Ready validation. Supports VMware ESX or ESXi



Software Appliance: bare metal installation with tuned, security-hardened OS. Includes hybrid SaaS Pre-filter and option to purchase Data Privacy and Encryption module.

- Certified by Trend Micro: Through extensive testing and validation, Trend Micro certifies platforms for compatibility with Trend Micro software appliance solutions. See Certified server platforms

Software Solution: installs easily on standard hardware running Microsoft Windows or Linux OS.

- InterScan Messaging Security Suite: Includes the same world-class antispam, anti-malware, and content filtering in a standard software solution. SaaS pre-filter and Data Privacy and Encryption module are not available in this implementation.



Securing Your Journey to the Cloud

©2014 by Trend Micro Incorporated. All rights reserved. Trend Micro, the Trend Micro t-ball logo, InterScan, and Smart Protection Network 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. [DS03_IMS_Datasheet_141112US]