

Trend Micro™

InterScan™ Messaging Security Suite

Proaktiver Sofortschutz am Messaging-Gateway

Über 90 % aller E-Mails werden von Trend Micro Kunden als Spam gemeldet, und immer mehr Mails beinhalten Sicherheitsbedrohungen, wie z. B. bösartigen Code oder Links zu infizierten Websites. Diese Angriffe sind so konzipiert, dass selbst Ihre versiertesten Mitarbeiter nichts davon bemerken, und ohne wirksamen Schutz am Gateway ist Ihr Unternehmen der Gefahr von Infektionen, Datenverlust, Richtlinienverstößen, Rufschädigung und Geschäftseinbußen ausgesetzt.

InterScan™ Messaging Security Suite bietet den Sofortschutz, den Sie am Messaging-Gateway brauchen – mit Web Reputation und Email Reputation des Trend Micro™ Smart Protection Network™. Diese einzigartigen, webbasierten Services stoppen neue und sich ständig verändernde Bedrohungen, bevor sie ins Netzwerk eindringen. Außerdem sperrt der mehrschichtige Spam-Schutz unerwünschte Nachrichten, während der preisgekrönte Malware-Schutz die meisten komplexen Bedrohungen abwehrt. Eine weitere Komponente der Lösung sind flexible Content-Filter zur Vermeidung von Datenverlusten und Richtlinienverstößen bei gleichzeitiger Erhaltung von Ressourcen und Produktivität.

MAXIMALER SCHUTZ BEI MINIMALEM AUFWAND

Integrierte Web und Email Reputation

- Branchenneuheit: Sperrt E-Mails mit Links auf bösartige oder infizierte Websites
- Filtert E-Mails anhand der Vertrauenswürdigkeitswerte der Absender. Diese Werte werden von unserem Smart Protection Network ständig online aktualisiert.
- Stoppt neue und sich ständig verändernde Bedrohungen und Spam, bevor sie in Ihr Gateway eindringen
- Verknüpft sofort webbasierte Bedrohungsdaten aus E-Mails, Internet und Dateien miteinander, um den Schutz weiter zu verbessern

Mehrschichtiger Schutz vor Spam und Phishing

- Sperrt Spam und Phishing-Angriffe mit Links auf bösartige Websites mit Hilfe webbasierter Reputation Services
- Überprüft die IP-Adressen unbekannter Absender durch Abfrage des Smart Protection Network in Echtzeit
- Verwendet Signaturen und Heuristik, um Spam, Bots, Phishing und gezielte Angriffe abzuwehren
- Verhindert unternehmens- oder branchenspezifische Bedrohungen mit Hilfe von Content-Filter-Richtlinien

Mehrfach ausgezeichneter Schutz vor Viren und Spyware

- Bekämpft die raffinierten und komplexen Bedrohungen von heute mit branchenführendem Malware-Schutz

- Verhindert Downloads bösartiger Dateien, das Weiterleiten ausspionierter Daten an den Angreifer und das Tunneln von Malware
- Ergänzt die Reputationsfilter um eine weitere leistungsstarke Schutzschicht

Flexible Content-Filter

- Durchsucht eingehende und ausgehende E-Mails nach unangemessenen Inhalten und persönlichen Daten
- Reduziert Haftungsansprüche, erhält die Produktivität und schützt vor Datenverlusten und Richtlinienverstößen
- Ermöglicht die Anpassung von Richtlinien, Wiederherstellungsoptionen und sogar Haftungsausschlüssen
- Bietet optionale E-Mail-Verschlüsselung, damit vertrauliche E-Mails garantiert nur bei den vorgesehenen Empfängern ankommen

Geringere Gesamtkosten durch weniger Aufwand

- Vereinfacht die Verwaltung des mehrschichtigen Gateway-Schutzes, wodurch sich die Gesamtkosten deutlich verringern
- Spart Zeit und Ressourcen durch die Abwehr unerwünschter E-Mails, bevor sie in das Netzwerk gelangen
- Verringert den Verwaltungsaufwand durch die Integration in LDAP, delegierte Administration, Nachrichten-Rückverfolgung und End User Quarantine

SOFTWARE

Geschützte Punkte

- Messaging-Gateway

Bedrohungsschutz

- Komplexe Bedrohungen
- Links zu bösartigen Websites
- Viren
- Spyware
- Phishing
- Spam und Bots
- Datenverlust
- Unangemessene Inhalte
- Haftungsansprüche
- Imageschäden

ENTSCHEIDENDE VORTEILE

- Minimiert das Risiko durch proaktiven Echtzeitschutz
- Spart Ressourcen durch die Abwehr von Bedrohungen außerhalb Ihres Netzwerks
- Schützt Mitarbeiter vor bösartigen Links und Malware
- Verhindert Datenverluste und Richtlinienverstöße
- Senkt Verwaltungs- und Gesamtkosten

NUMMER 1 BEI DER SPAM-ABWEHR

Bei einem unabhängigen Vergleichstest von West Coast Labs war **InterScan Messaging Security** Testsieger in der Kategorie Spam-Abwehr.

 westcoast labs

Sicherheit, die passt: Wählen Sie aus verschiedenen Formfaktoren die beste Lösung für Sie

InterScan Messaging Security ist auch als virtuelle Appliance oder als gehosteter Service verfügbar. Damit verfügen Sie über zahlreiche Verteilungsoptionen.

In **InterScan™ Messaging Security Virtual Appliance** ist ein robustes Linux Betriebssystem integriert. Diese virtuelle Appliance kann entweder auf dedizierter Hardware oder auf einer VMware installiert werden. Entscheidende Vorteile:

- Datenzentrenskonsolidierung sorgt für geringere Laufkosten
- Optimierte Nutzung der vorhandenen IT-Ressourcen
- Als Einheit installiert, verwaltet, gepatcht und gewartet, um die Kosten weiter zu senken

InterScan Messaging Hosted Security erfordert keine Hardware oder Software. Das weltweite Trend Micro Experten-Team kümmert sich um alle Updates und das Anwendungstuning, damit sich Sicherheit und Leistung Ihrer Lösung stetig verbessern. Entscheidende Vorteile:

- Keine Installation oder Wartung, auch nicht bei steigendem E-Mail-Aufkommen
- Durch verwaltete Updates und Tuning können sich die Administratoren auf andere wichtige Aufgaben konzentrieren

InterScan Messaging Security Suite kann als Software auf Windows, Linux oder Solaris Betriebssystemen installiert werden. Vorteile:

- Marktführende Messaging-Sicherheit am Gateway
- Passt auch auf Ihr bevorzugtes Betriebssystem

SYSTEMVORAUSSETZUNGEN**Microsoft™ Windows™, Linux™ und Sun™ Solaris™**

- 1 GB Arbeitsspeicher
- 500 MB Festplattenspeicher für die Installation
- Zusätzlicher Festplattenspeicher zum Speichern von E-Mails und für die Datenbank
- Microsoft Internet Explorer 6 SP1 oder Firefox 1.5 (Netscape Navigator wird nicht unterstützt)
- LDAP Server Microsoft Active Directory 2000 oder 2003, IBM Lotus Domino 6.0 oder höher oder Sun One LDAP

Microsoft Windows

- Windows Server 2000 mit SP 4.0 oder höher
- Windows Server 2003 mit SP 1.0 oder höher
- Intel™ Pentium™ IV oder kompatibler 2,8 GHz-Prozessor oder höher
- 2 GB RAM
- Microsoft Desktop Engine oder Microsoft SQL Server 2000 oder höher

Linux

- Red Hat™ Enterprise Linux 3 oder 4
- SuSE™ Linux Enterprise Server 8.0 oder 9.0
- Intel Pentium IV 2,4 GHz
- 2 GB RAM
- 2 GB Auslagerungsspeicher
- PostgreSQL, Version 8.1.3
- BIND-Server 9.0 oder höher
- MTA Postfix 2.1 oder höher; Sendmail; Qmail

Sun Solaris

- Sun Solaris 8, 9 oder 10
- UltraSPARC™ II Prozessor (650 MHz)
- 2 GB RAM
- 4 GB Auslagerungsspeicher
- PostgreSQL, Version 8.1.3
- BIND-Server 9.0 oder höher
- MTA Postfix 2.1 oder höher; Sendmail; Qmail

ALTERNATIVLÖSUNGEN

- [InterScan™ Messaging Virtual Appliance](#)
- [InterScan™ Messaging Hosted Security](#)

ERWEITERN SIE IHREN SCHUTZ**Messaging-Sicherheit**

- [Email Encryption Gateway](#)

Internet-Sicherheit

- [InterScan™ Web Security Virtual Appliance](#)

Endpunktsicherheit

- [OfficeScan Client-Server Suite](#)

Zentrale Verwaltung

- [Trend Micro Control Manager](#)



©2010 Trend Micro Incorporated. Alle Rechte vorbehalten. Trend Micro, das Trend Micro T-Ball Logo, Trend Micro Control Manager, InterScan und TrendLabs sind Marken oder eingetragene Marken von Trend Micro, Incorporated. Alle anderen Firmen- oder Produktnamen sind Marken oder eingetragene Marken ihrer jeweiligen Eigentümer.
[DS05_IMSS_091202DE]
www.trendmicro.com