

# Trend Micro™ SCANMAIL™ SUITE for IBM® Domino™

Erstklassige Mail-Server-Sicherheit. Weniger Administrationsaufwand.

Die meisten Sicherheitslösungen für Mail-Server beruhen auf regelmäßigen Pattern-Datei-Updates über Bedrohungsdatenbanken; bösartige Links oder komplexe, zielgerichtete Angriffe (Advanced Persistent Threats, APTs) werden nicht erkannt. Diese verborgenen Bedrohungen dringen gewöhnlich über gezielte E-Mails in das Netzwerk ein. Das Messaging-Gateway und der Mail-Server sind demnach die richtigen Orte, um derartige Bedrohungen zu stoppen.

**ScanMail™ Suite for IBM® Domino™** stoppt gezielte E-Mail-Angriffe wie Spear-Phishing durch die Erkennung von Exploit-Codes in E-Mails, eine verbesserte Web-Reputation-Technologie und Sandboxing als Teil einer individuellen Abwehr gegen zielgerichtete Angriffe. ScanMail wehrt zudem herkömmliche Bedrohungen ab – mit Reputationstechnologie und korrelierten weltweiten Bedrohungsdaten aus dem cloudbasierten Sicherheitssystem des Trend Micro™ Smart Protection Network™. ScanMail, **die Nummer 1** beim Schutz vor Spam- und Phishing-Angriffen, hat seit 2011 durchweg acht Konkurrenzprodukte in vierteljährlichen Benchmark-Tests übertroffen.

ScanMail Suite wurde als native Domino-Serveranwendung entwickelt. Dabei wurde besonderer Wert auf eine hohe Leistung und einfache Verwendung gelegt. Laut Forschungsergebnissen von Analysten ermöglicht ScanMail durch zeitsparende Funktionen, wie eine zentrale Verwaltung, DLP-Vorlagen, rollenbasierte Zugriffssteuerung und Domino-Optimierungen eine Senkung der Gesamtbetriebskosten um 35 %.

## VORTEILE

### Schützt vor zielgerichteten Angriffen

- Erkennt gezielte Angriffe und komplexe Malware mit Hilfe mehrerer Schutztechnologien
- Führt Sandbox-Analysen in Ihrer spezifischen Unternehmensumgebung durch und bietet basierend auf der Integration mit Deep Discovery Advisor die Korrelation mit globalen Informationen über Bedrohungen
- Erstellt individuell angepasste Sicherheitsupdates für andere Sicherheitsschichten, um Bedrohungen zu beseitigen und weitere Angriffe von ähnlicher Malware zu verhindern

### Blockiert mehr Malware, Phishing und Spam durch Technologien zur Reputationsüberprüfung

- Stoppt Malware-Anhänge und bösartige Weblinks, um den Download von Malware zu verhindern
- Bietet als einzige Sicherheitslösung korrelierte E-Mail-, File- und Web-Reputation-Technologien, um mehr Messaging-Bedrohungen zu blockieren
- Filtert mehr Spam und übertrifft damit immer wieder andere Sicherheitslösungen in unabhängigen Tests von Opus One

### Senkt IT-Kosten, steigert die Leistung

- Vereinfacht E-Mail-Sicherheitsoperationen durch leistungsstarke Gruppenkonfiguration und -verwaltung sowie zentralisierte Protokollierung und Reporting
- Vereinfacht Initiativen zur Einhaltung von Compliance-Richtlinien und zum Datenschutz durch zentral verwalteten und vorlagenbasierten Schutz vor Datenverlust

### Software

#### Geschützte Punkte

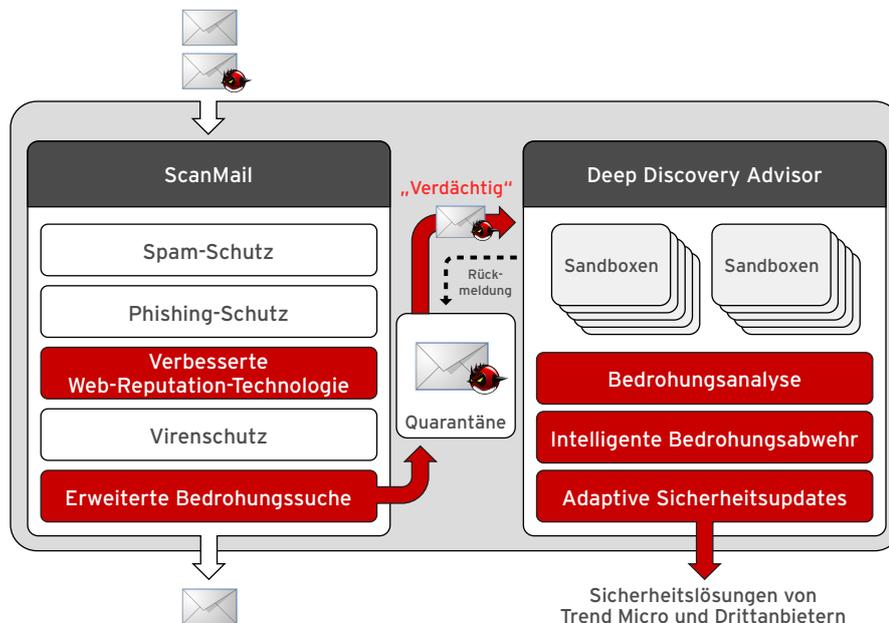
- Mail-Server
- Interne Überprüfung
- Ein- und ausgehende Daten

#### Bedrohungsschutz und Datensicherheit

- Virenschutz
- Schutz vor Internetbedrohungen
- Spam-Schutz
- Phishing-Schutz
- Content-Filter
- Schutz vor Datenverlust
- Komplexe, zielgerichtete Angriffe (APTs)

## GEZIELTE ANGRIFFE ERFORDERN EINEN FLEXIBLEN SCHUTZ VOR INDIVIDUELLEN BEDROHUNGEN

Trend Micro Messaging Security Produkte bieten Schutz vor gezielten Angriffen mit verbesserter Web-Reputation-Technologie, einer neuen Erkennungseingabe und einer neuen Appliance zur Bedrohungsanalyse, die gezielte E-Mail-Angriffe durch Sandbox-Analysen abwehrt. Die Integration dieser Komponenten bietet einen flexiblen und individuellen Schutz, damit Sie gezielte Angriffe erkennen und analysieren, Abwehrmechanismen entsprechend anpassen und so schnell und wirksam auf Angriffe reagieren können.



### KOMPONENTEN DER SCANMAIL SUITE

Die ScanMail Suite wurde durch die Integration verschiedener Komponenten zum Schutz vor gezielten Angriffen erweitert.

- Die **verbesserte Web-Reputation-Technologie** blockiert E-Mails mit bösartigen Links im Nachrichtentext oder in Anhängen. Unterstützt wird diese Komponente durch das Trend Micro™ Smart Protection Network™, das Bedrohungsinformationen mit Big-Data-Analysen und Vorhersagetechnologien korreliert.
- Die **optimierte Scan-Engine** erkennt komplexe Malware in Adobe PDF, MS Office und anderen Dokumentenformaten durch statische und heuristische Logik zur Erkennung bekannter und Zero-Day-Exploits. Die Engine durchsucht außerdem den Mailspeicher von Domino nach gezielten Bedrohungen, die möglicherweise bereits in das Netzwerk eingedrungen waren, bevor der Schutz wirksam wurde. Bei Integration in Trend Micro™ Deep Discovery Advisor werden verdächtige Anhänge in Quarantäne verschoben, um eine automatische Sandbox-Analyse auszuführen. Die Zustellung des Großteils der Nachrichten wird durch diese Inline-Analyse nicht beeinträchtigt.

### KOMPONENTEN VON DEEP DISCOVERY ADVISOR (ZUSÄTZLICH ZU ERWERBEN)

Die Appliance Deep Discovery Advisor bietet Sandboxing, netzwerkweite Erfassung von Protokolldateien und eine detaillierte Bedrohungsanalyse auf einer gemeinsamen Informationsplattform, dem Herzstück von Custom Defense - der Trend Micro Lösung für flexiblen Schutz vor individuellen Bedrohungen.

- Die Komponente **Individuelle Bedrohungsanalysen** bietet automatische und detaillierte Simulationsanalysen von potenziell bösartigen Anhängen, einschließlich ausführbarer Dateien und Office-Dokumenten in einer sicheren Sandbox-Umgebung. Anwender können dafür mehrere vollständig benutzerdefinierte Zielimages erstellen, die genau ihren Host-Umgebungen entsprechen.
- Die Komponente **Individuelle Bedrohungsanalysen** analysiert Protokolldateien von Trend Micro Produkten und Drittanbieterlösungen, um in Korrelation mit Bedrohungsanalysen von Trend Micro ausführliche Einblicke zu bieten und damit eine risikobasierte Bewertung, Eindämmung und Beseitigung von Vorfällen zu ermöglichen.
- Die Komponente **Adaptive Sicherheitsupdates** stellt individuelle Sicherheitsupdates bereit, um einen anpassbaren Schutz und eine wirksame Bedrohungsabwehr durch ScanMail sowie weitere Trend Micro Produkte und Sicherheitslösungen von Drittanbietern auf verschiedenen Ebenen zu ermöglichen.

## DIE WICHTIGSTEN FUNKTIONEN

### Schutz vor Spear-Phishing und gezielten Angriffen

Verbesserte Web Reputation, Erkennung von Exploits in Dokumenten, Ausführung von Sandbox-Analysen und individuelle Bedrohungsdaten bieten umfassende Sicherheit vor E-Mail-Bedrohungen, einschließlich Spear-Phishing-Angriffen verbunden mit komplexen, zielgerichteten Angriffen.

- Erkennt bekannte und unbekannte Exploits in Adobe PDF, MS Office und anderen Dokumentenformaten
- Führt Malware-Ausführungsanalysen durch und erstellt individuelle Bedrohungsdaten sowie adaptive Sicherheitsupdates (bei optionaler Integration von Deep Discovery Advisor)
- Verhindert das Eindringen von Bedrohungen in Ihre Umgebung durch sofortigen Schutz basierend auf führenden weltweiten Bedrohungsdaten

### Data Loss Prevention Add-on-Modul

Erweitern Sie Ihre bestehende Sicherheit, um Compliance-Richtlinien einzuhalten und Datenverluste zu verhindern. Integrierter Schutz vor Datenverlust vereinfacht die Datensicherheit durch Transparenz und Kontrolle von Daten im Speicher und bei der Übertragung.

- Protokolliert vertrauliche Daten, die durch Ihr E-Mail-System und den Mailspeicher fließen
- Beschleunigt die Installation und verbessert die Präzision mit mehr als 100 Vorlagen zur Einhaltung von Compliance-Richtlinien
- Vereinfacht die Installation durch ein Add-on-Modul für sofortigen Schutz vor Datenverlust, das keine zusätzliche Hardware oder Software erfordert und eine strenge, LDAP-basierte Richtlinien-durchsetzung ermöglicht
- Ermöglicht Compliance-Verantwortlichen DLP-Richtlinien und -Verstöße für dieses und andere Trend Micro Produkte über den Control Manager™ zentral und durchgängig zu verwalten - vom Endpunkt bis zum Gateway

### Optimiert für Domino

ScanMail ist eine native 64-Bit-Anwendung, die eng in Ihre Domino-Umgebung integriert ist, um Ihr E-Mail-System möglichst effizient und mit minimalem Aufwand zu schützen.

- Umfasst vollständige Cluster-Unterstützung
- Verwaltet Bedrohungen plattformübergreifend mit einem einzigen Update-Server
- Unterstützt Remoteverwaltung

### Leistungsstarke Konfiguration und Verwaltung

- Ermöglicht die Automatisierung von Aufgaben und Skriptinstallation
- Senkt IT-Kosten durch eine einfache Verwaltung

### Einzige Reputationstechnologie zur Abwehr von Spam, Phishing und Malware

Verwendet Big-Data-Analysen und Vorhersagetechnologien, um File-, Web- und E-Mail-Reputation-Daten in der Cloud zu korrelieren und damit sofortigen Schutz zu bieten.

- Überprüft bösartige Links in E-Mail-Texten und -Anhängen, um Phishing-Angriffe durch verbesserte Web-Reputation-Technologie abzuwehren
- Sondert bis zu 85 % aller eingehenden E-Mails durch Reputationsüberprüfung von Absendern aus und entlastet damit die Netzwerkreisourcen
- Stoppt laut unabhängigen Tests mehr Spam als andere Sicherheitslösungen

### Entscheidende Vorteile

- Schützt den Einzelnen vor gezielten Bedrohungen wie Spear-Phishing-Angriffen
- Bietet führende, cloudbasierte Sicherheit, um Bedrohungen am Mail-Server zu stoppen, noch bevor sie den Endanwender erreichen
- Bietet Transparenz und Kontrolle von Daten, um Datenverlust zu verhindern und die Einhaltung von Compliance-Richtlinien zu unterstützen
- Senkt Verwaltungsaufwand und Gesamtbetriebskosten durch eine zentrale Verwaltung

„Wir waren so beeindruckt von der einfachen Installation und Verteilung von Trend Micro ScanMail for IBM Domino, dass wir gleich im Anschluss daran begannen, Gespräche mit Trend Micro über Endpunktsicherheitslösungen zu führen.“

**Paul Key**

IT Security Manager  
Wincanton

## MINDESTSYSTEMVORAUSSETZUNGEN

Trend Micro ScanMail Suite for IBM Domino wird direkt auf dem Domino-Server ausgeführt, um Benutzer, Systeme und Daten zu schützen. Daher unterstützt diese native Domino-Anwendung auch weiterhin die branchenweit größte Bandbreite an Domino-Betriebsumgebungen: Windows, Linux (auf x86-Hardware und IBM System z), AIX, i5/OS, z/OS und Solaris.

32-Bit-Versionen von Domino werden noch mit reduziertem Funktionsumfang von ScanMail v3 unterstützt.

Aktuelle und detaillierte Systemvoraussetzungen finden Sie im Trend Micro Download Center oder in der Knowledge Base für ScanMail Suite for IBM Domino.

### SYSTEMVORAUSSETZUNGEN FÜR DIE 64-BIT-VERSION VON DOMINO™: R9.0.4, R8.0.1, R8.0.2, R8.5.0, R8.5.1, R8.5.2 UND R8.5.3

#### LINUX X86

- Novell SUSE Linux Enterprise Server (SLES) 10
- Novell SUSE Linux Enterprise Server (SLES) 11
- Red Hat Enterprise Linux (RHEL) 5
- Red Hat Enterprise Linux (RHEL) 6

#### LINUX FOR SYSTEM Z

- Novell SUSE Linux Enterprise Server (SLES) 10
- Novell SUSE Linux Enterprise Server (SLES) 11
- Red Hat Enterprise Linux (RHEL) 5
- Red Hat Enterprise Linux (RHEL) 6

#### AIX

- AIX 5.2, 5.3, 6.1, 7.1

#### MICROSOFT WINDOWS

- Microsoft Windows 2012 Server
- Microsoft Windows 2008 R2 Server
- Microsoft Windows 2008 Server x64 Edition
- Microsoft Windows 2008 Server
- Microsoft Windows 2003 R2 Server x64 Edition
- Microsoft Windows 2003 Server x64 Edition
- Microsoft Windows 2003 Server Enterprise Edition, Service Pack 2
- Microsoft Windows 2003 Server Standard Edition

### SYSTEMVORAUSSETZUNGEN FÜR DIE 32-BIT-VERSION VON DOMINO: R8, R8.0.1, R8.0.2, R8.5.1, R8.5.3

#### OS-Plattform

- RHEL 5, 6
- RHEL 5, 6 x64
- SuSE 10, 11
- SuSE 10 x64, 11 x64
- Solaris 10
- AIX 5.2, 5.3, 6.1, 7.1
- i5/OS V5R4, V6R1, V7R1



Securing Your Journey to the Cloud

• ©2013 Trend Micro Incorporated. Alle Rechte vorbehalten. Trend Micro,  
• das Trend Micro T-Ball-Logo, Smart Protection Network™ und SafeSync™  
• sind Marken oder eingetragene Marken von Trend Micro Incorporated. Alle  
• anderen Firmen- bzw. Produktnamen sind Unternehmenskennzeichen  
• oder eingetragene Marken ihrer jeweiligen Eigentümer. Die in diesem  
• Dokument enthaltenen Informationen können sich ohne vorherige  
• Ankündigung ändern. [DS04\_SMID\_131015DE]