Trend Micro™

SCANMAIL™ SUITE FOR MICROSOFT® EXCHANGE™

Erstklassiger Schutz. Weniger Aufwand.

Über 90 % der gezielten Angriffe beginnen mit einer Spear-Phishing-E-Mail, daher ist Ihre Mailserver-Sicherheit wichtiger denn je. Leider beruhen die meisten Sicherheitslösungen für Mailserver, einschließlich der begrenzten Anzahl integrierter Schutzkomponenten in Exchange 2013, auf Pattern-Datei-Updates, die nur herkömmliche Malware erkennen. Spezieller Schutz zum Erkennen bösartiger URLs oder Exploits in Dokumenten, die häufig in komplexen, zielgerichteten Angriffen (Advanced Persistent Threats, APTs) verwendet werden, ist in der Regel nicht enthalten.

ScanMail™ Suite for Microsoft® Exchange™ stoppt selbst gezielte E-Mail-Angriffe und Spear-Phishing durch die Erkennung von Exploit-Codes in E-Mails, eine verbesserte Web-Reputation-Technologie und Sandboxing* als Teil unserer Custom Defense Strategie – ein Schutz, den andere Sicherheitslösungen nicht bieten. Zudem wehrt nur ScanMail herkömmliche Malware mit E-Mail-, File- und Web-Reputation-Technologie und korrelierten weltweiten Bedrohungsdaten aus dem cloudbasierten Sicherheitssystem des Trend Micro™ Smart Protection Network™ ab.

Dank zeitsparender Funktionen wie zentraler Verwaltung, DLP-Vorlagen und rollenbasierter Zugriffssteuerung zeichnet sich ScanMail laut Osterman Research durch den geringsten Administrationsaufwand und die niedrigsten Gesamtbetriebskosten unter den vergleichbaren Lösungen der führenden Sicherheitsanbieter aus. ScanMail bietet darüber hinaus eine hohe Leistung und native 64-Bit-Unterstützung, um höchste Durchsatzgeschwindigkeiten zu ermöglichen.

Software

Geschützte Punkte

- Mailserver
- 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 (Advanced Persistent Threats, APTs)

VORTEILE

Schützt Unternehmen vor APTs und anderen gezielten Angriffen

- Minimiert gezielte Angriffe mithilfe mehrerer Schutztechnologien
- Führt Sandbox*-Analysen für Ihre spezielle Umgebung durch und stellt individuelle Bedrohungsdaten bei Integration von Deep Discovery Advisor bereit
- Erstellt individuell angepasste Sicherheitsupdates für andere Sicherheitsschichten, um Bedrohungen zu beseitigen und weitere Angriffe von ähnlicher Malware zu verhindern

Sperrt mehr Malware, Phishing und Spam durch Technologien zur Reputationsüberprüfung

- Erkennt Malware-Anhänge und bösartige Weblinks, um den Download von Malware zu verhindern
- Nutzt als einzige Sicherheitslösung für Mailserver korrelierte E-Mail-, File- und Web-Reputation-Technologien, um mehr Messaging-Bedrohungen zu stoppen
- Stoppt laut unabhängigen Tests von Opus One mehr Spam als andere Sicherheitslösungen

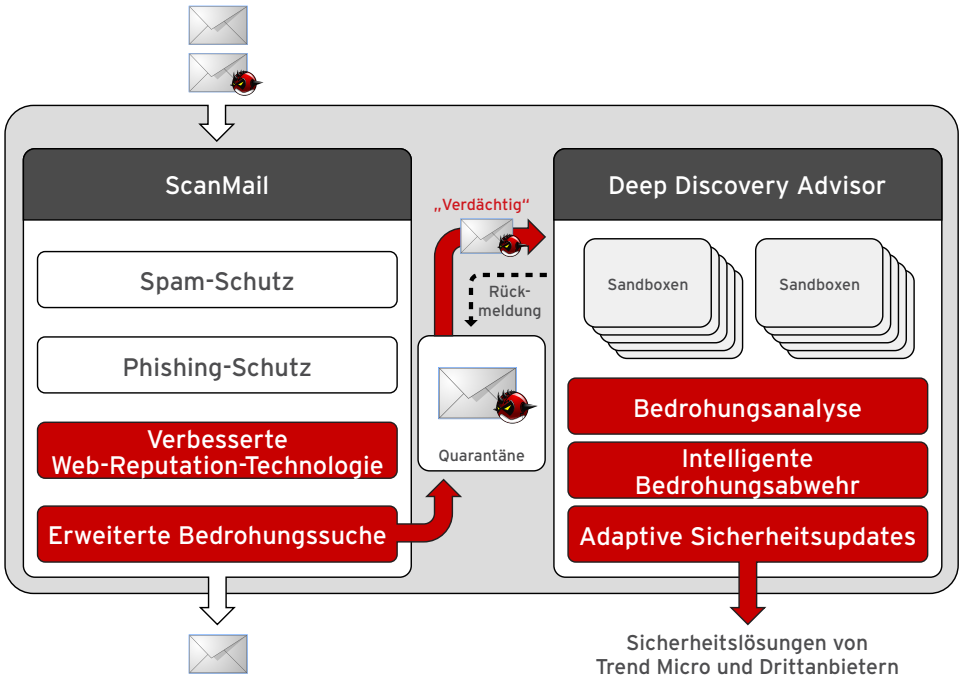
Senkt IT-Kosten, steigert die Leistung

- Vereinfacht E-Mail-Sicherheitsoperationen durch leistungsstarke Gruppenkonfiguration und -verwaltung sowie zentralisierte Protokollierung und Berichterstellung
- Vereinfacht Initiativen zur Richtlinieneinhaltung und zum Datenschutz durch zentral verwalteten, vorlagengestützten Schutz vor Datenverlust
- Reduziert den Administrationsaufwand und die Gesamtbetriebskosten erheblich und liegt damit laut Osterman Research vor vier anderen führenden Sicherheitslösungen

* Die Funktion Sandbox ist Teil der optionalen Deep Discovery Lösung.

GEZIELTE ANGRIFFE ERFORDERN EINEN FLEXIBLEN SCHUTZ VOR INDIVIDUELLEN BEDROHUNGEN

Trend Micro Messaging-Sicherheitslösungen bieten Schutz vor gezielten Angriffen mit verbesserter Web-Reputation-Technologie, einer neuen Erkennungsengine und Sandbox*-Ausführung, um eine detaillierte Bedrohungsanalyse zu ermöglichen. 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.



ScanMail Suite

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

Die **verbesserte Web-Reputation-Technologie** sperrt E-Mails mit bösartigen Links im Nachrichtentext oder in Anhängen. Unterstützt wird diese Komponente durch das Trend Micro™ Smart Protection Network™, das Bedrohungsinformationen mit Analysen von Big Data 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 Exchange nach gezielten Bedrohungen, die möglicherweise bereits in das Netzwerk eingedrungen waren, bevor der Schutz verfügbar wurde.

Bei Integration in Trend Micro™ Deep Discovery Advisor verschiebt ScanMail verdächtige Anhänge in Quarantäne, um eine automatische Sandbox-Analyse auszuführen. Die Zustellung des Großteils der Nachrichten wird durch diese Inline-Analyse nicht beeinträchtigt.

Deep Discovery Advisor (zusätzlich zu erwerben)

Die Hardware-Appliance Deep Discovery Advisor bietet Sandboxing, detaillierte Bedrohungsanalysen und lokale Sicherheitsupdates 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-Dokumente in einer sicheren Sandbox-Umgebung. Anwender können dafür mehrere vollständig benutzerdefinierte Zielimages erstellen, die genau ihren Host-Umgebungen entsprechen.

Die Komponente **Individuelle Bedrohungsinformationen** korreliert Angriffsdaten in Ihrer Umgebung mit detaillierten Bedrohungsinformationen von Trend Micro, um ausführliche Einblicke zu bieten und damit eine risikobasierte Bewertung, Eindämmung und Beseitigung von Vorfällen zu ermöglichen.

Adaptive Sicherheitsupdates stellt individuelle Sicherheitsupdates zu neuen C&C-Serverstandorten und Sites mit bösartigen Downloads bereit, die während der Sandbox-Analyse ermittelt wurden – für einen anpassbaren Schutz und eine Bedrohungsbeseitigung durch ScanMail, andere Trend Micro Produkte für Endpunkte und Gateways sowie Sicherheitsebenen Dritter.

* Die Funktion Sandbox ist Teil der optionalen Deep Discovery Lösung.

WICHTIGSTE FUNKTIONEN

Schutz vor Spear-Phishing und gezielten Angriffen

Im Vergleich zu anderen E-Mail-Sicherheitslösungen bietet ScanMail verbesserte Web-Reputation-Technologie, Erkennung von Exploits in Dokumenten, Sandbox*-Ausführungsanalysen und individuelle Bedrohungsinformationen. Zusammen schützen diese erweiterten Funktionen umfassend vor E-Mail-Bedrohungen, einschließlich Spear-Phishing-Angriffen in Verbindung mit APTs und anderen gezielten Bedrohungen.

- 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

Erweitert Ihre bestehende Sicherheit, um die Einhaltung von Richtlinien zu unterstützen und Datenverluste zu verhindern. Integrierter Schutz vor Datenverlust vereinfacht die Datensicherheit durch Transparenz und Kontrolle von Daten im Speicher und bei der Übertragung.

- Protokolliert den Missbrauch vertraulicher Daten, die durch Ihr E-Mail-System und den Mailspeicher fließen
- Beschleunigt das Einrichten und erleichtert die Umsetzung mit mehr als 100 Vorlagen für die Richtlinieneinhaltung
- Vereinfacht die Installation durch ein Add-on-Modul für sofortigen Schutz vor Datenverlust, das keine zusätzliche Hardware oder Software erfordert und eine genaue, Active Directory-basierte Richtliniendurchsetzung ermöglicht
- Ermöglicht den Verantwortlichen für Richtlinieneinhaltung 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 Microsoft® Exchange

ScanMail ist eng in Ihre Microsoft-Umgebung integriert, um Ihr E-Mail-System möglichst effizient und mit minimalem Aufwand zu schützen.

- Unterstützt Exchange 2013, 2010 und 2007 Server, einschließlich gemischter Umgebungen während Migrationsphasen
- Beschleunigt den Durchsatz und ist bis zu 57 Prozent schneller als andere Lösungen
- Vermeidet redundante Überprüfungen durch Multi-Thread-Suche mit AV-Stempel; weitere Leistungsoptimierung durch CPU-Drosselung
- Durchsucht effizient mit nativer 64-Bit-Unterstützung
- Bietet Integration in Microsoft® System Center Operations Manager und Outlook® Junk-E-Mail-Filter
- Verhindert unautorisierte Richtlinienänderungen durch rollenbasierte Zugriffssteuerung

Innovative Search & Destroy-Funktionen

Im Gegensatz zu den in Exchange integrierten Tools findet ScanMail Search & Destroy E-Mails schnell und präzise.

- Führt gezielte Suchen über Exchange mithilfe von Schlüsselwörtern und regulären Ausdrücken durch
- Ermöglicht Administratoren, schnell auf dringende Anfragen von rechtmäßigen Quellen oder Sicherheitsabteilungen zu reagieren, um bestimmte E-Mails bei Bedarf zu suchen, nachzuverfolgen und dauerhaft zu löschen

Einzigartige Reputationstechnologie zur Abwehr von Spam, Phishing und Malware

Verwendet Analysen von Big Data und Vorhersagetechnologien, um File-, Web- und E-Mail-Reputationsdaten in der Cloud zu korrelieren und damit sofortigen Schutz vor neuen Bedrohungen zu bieten – noch bevor diese die Anwender erreichen, die möglicherweise über Laptops oder mobile Geräte auf E-Mails zugreifen.

- 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 Netzwerkressourcen
- 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 Anwender erreichen
- Bietet Transparenz und Kontrolle von Daten, um Datenverlust zu verhindern und Richtlinieneinhaltung zu unterstützen
- Beschleunigt den Durchsatz durch native 64-Bit-Verarbeitung
- 57 % schneller als MS Forefront
- Senkt Verwaltungsaufwand und Gesamtbetriebskosten durch eine zentrale Verwaltung

* Die Funktion Sandbox ist Teil der optionalen Deep Discovery Lösung.

MINDESTSYSTEMVORAUSSETZUNGEN

Arbeitsspeicher	Festplattenspeicher	Browser	Webserver
• 1 GB Arbeitsspeicher • 2 GB Arbeitsspeicher empfohlen (ausschließlich für ScanMail)	• 2 GB freier Festplattenspeicher	• Microsoft Internet Explorer 6.0, 7.0, 8.0 und 9.0 (Kompatibilitätsansicht wird empfohlen) • Mozilla Firefox 3.0 oder höher • MSXML • MSXML 4.0 SP2 oder höher	• Microsoft Internet Information Services (IIS) 7.5 oder 7.0

SYSTEMVORAUSSETZUNGEN FÜR MICROSOFT EXCHANGE

	Prozessor	Betriebssystem	Mail-Server
Microsoft Exchange 2013	• Computer mit x64-Architektur mit Intel-Prozessor, der die Intel 64-Architektur unterstützt (ehemals Intel EM64T) • AMD-Prozessor, der die AMD64-Plattform unterstützt	• Windows Server 2012 Standard oder Datacenter • Windows Server 2008 R2 Standard mit SP1 • Windows Server 2008 R2 Enterprise mit SP1 • Windows Server 2008 R2 Datacenter RTM oder höher	• Microsoft Exchange Server 2013
Microsoft Exchange 2010	• Computer mit x64-Architektur mit Intel-Prozessor, der die Intel 64-Architektur unterstützt (ehemals Intel EM64T) • AMD-Prozessor, der die AMD64-Plattform unterstützt	• Windows Server 2012 Standard oder Datacenter • Microsoft Windows Server 2008 mit Service Pack 2 (64 Bit) • Microsoft Windows Server 2008 R2 mit Service Pack 1 (64 Bit) • Microsoft Windows Server 2008 R2 (64 Bit) • Microsoft Small Business Server (SBS) 2011	• Microsoft Exchange Server 2010 mit Service Pack 1, 2 oder 3 • Microsoft Exchange Server 2010
Microsoft Exchange 2007	• Computer mit x64-Architektur mit Intel-Prozessor, der die Intel 64-Architektur unterstützt (ehemals Intel EM64T) • AMD-Prozessor, der die AMD64-Plattform unterstützt	• Microsoft Windows Server 2008 mit Service Pack 2 (64 Bit) • Microsoft Windows Server 2008 R2 mit Service Pack 1 (64 Bit) • Microsoft Windows Server 2008 R2 (64 Bit) • Microsoft Windows Small Business Server 2008 (64 Bit) • Microsoft Windows Server 2003 R2 mit Service Pack 2 (64 Bit) • Microsoft Windows Server 2003 mit Service Pack 2 (64 Bit)	• Microsoft Exchange Server 2007 mit Service Pack 1, 2 oder 3

TREND MICRO™

Securing Your Journey to the Cloud