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 und 2016, auf Pattern-Datei-Updates, die nur herkömmliche Malware erkennen. Spezieller Schutz zur Erkennung 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 ermöglicht nur ScanMail die Abwehr herkömmlicher Malware durch E-Mail-, File- und Web-Reputation-Technologie in Verbindung mit korrelierten Bedrohungsdaten aus dem cloudbasierten Trend Micro™ Smart Protection Network™.

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 fünf vergleichbaren Lösungen der führenden Sicherheitsanbieter aus. ScanMail bietet darüber hinaus eine hohe Leistung und native 64-Bit-Unterstützung, um höchste Durchsatzgeschwindigkeiten zu erzielen.

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 (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

Blockiert mehr Malware, Phishing und Spam durch Technologien zur Reputationsüberprüfung

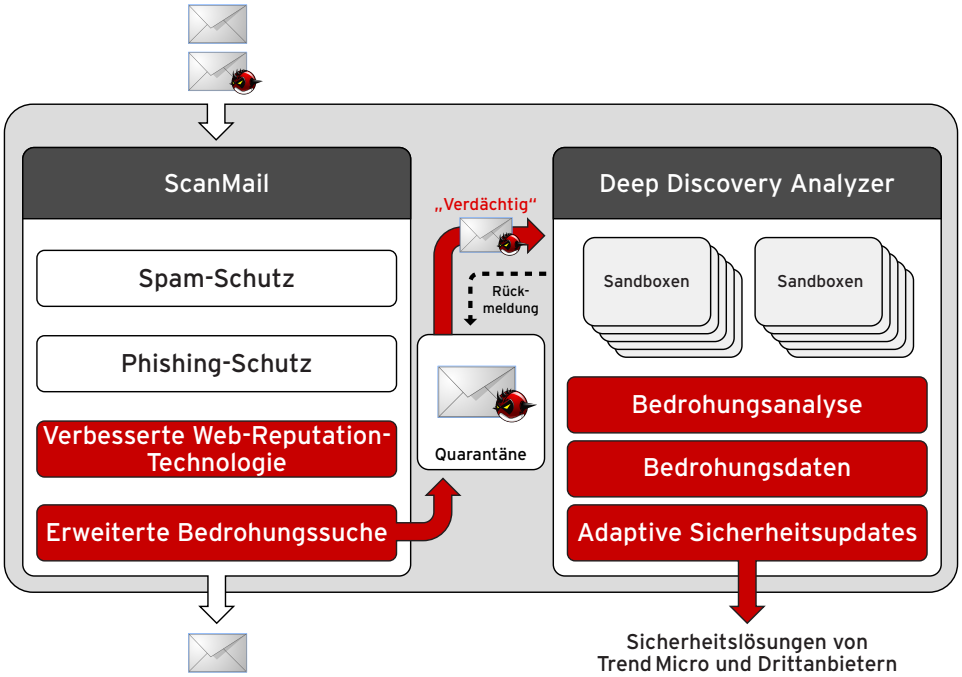
- Erkennt Malware-Anhänge und bösartige Weblinks, um den Download von Malware zu verhindern
- Nutzt als einzige Sicherheitslösung für Mailserver korrelierte E-Mail-, File- und Web-Reputation-Technologien, um mehr Messaging-Bedrohungen zu stoppen
- Stoppt laut unabhängigen Tests von Opus One mehr Spam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

Senkt IT-Kosten, steigert die Leistung

- Vereinfacht sicherheitsrelevante E-Mail-Vorgänge durch leistungsstarke Gruppenkonfiguration und -verwaltung sowie zentralisierte Protokollierung und Berichterstellung
- Vereinfacht Initiativen zur Richtlinieneinhaltung und zur Datensicherheit 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

GEZIELTE ANGRIFFE ERFORDERN EINE STRATEGIE, DIE DAS GESAMTE NETZWERK VERTEIDIGT

Trend Micro Sicherheitslösungen bieten Schutz vor gezielten Angriffen durch verbesserte Web-Reputation-Technologie, eine Erkennungs-Engine für Dokumenten-Exploits und eine Sandbox-Ausführung zur detaillierten Bedrohungsanalyse. Die Integration dieser Komponenten bietet einen Netzwerkschutz, mit dem 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 Bedrohungsdaten mit Big-Data-Analysen und Vorhersagetechnologien korreliert.

Die **optimierte Scan-Engine** erkennt komplexe Malware in Adobe PDF, MS Office und anderen Dokumentenformaten durch statisch 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 Analyzer** 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 Analyzer (zusätzlich zu erwerben)

Die Hardware-Appliance Deep Discovery Analyzer bietet Sandboxing, detaillierte Bedrohungsanalysen und lokale Sicherheitsupdates auf einer gemeinsamen Informationsplattform, dem Herzstück von Network Defense – der Trend Micro Lösung für Netzwerkschutz vor individuellen Bedrohungen.

Individuelle Bedrohungsanalysen bieten automatische und detaillierte Simulationsanalysen von potenziell bösartigen Anhängen, einschließlich ausführbarer Dateien und Office-Dokumenten in einer sicheren Sandbox-Umgebung. Anwender können mehrere vollständig benutzerdefinierte Zielimages erstellen, die genau ihren Host-Umgebungen entsprechen.

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

Adaptive Sicherheitsupdates stellen 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 Lösungen für Endpunkte und Gateways sowie Drittanbieter-Produkte.

DIE WICHTIGSTEN 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 Bedrohungsdaten. 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 Analyzer)
- 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 genaue, Active Directory-basierte Richtliniendurchsetzung 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 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 2016, 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 Suchläufe 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 Big-Data-Analysen 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 der Absender 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 die Einhaltung von Compliance-Richtlinien zu unterstützen
- Beschleunigt den Durchsatz durch native 64-Bit-Verarbeitung
- 57 % schneller als MS Forefront
- Senkt Verwaltungsaufwand und Gesamtbetriebskosten durch zentrale Verwaltung

SYSTEMVORAUSSETZUNGEN

ScanMail Suite unterstützt alle virtuellen Umgebungen, die mit Microsoft Exchange kompatibel sind.

SYSTEMVORAUSSETZUNGEN FÜR MICROSOFT EXCHANGE

ScanMail mit Microsoft Exchange Server 2016

Ressource	Anforderungen
Prozessor	Prozessor mit x64-Architektur, der die Intel™ 64-Architektur unterstützt (offizielle Bezeichnung: Intel EM64T) Computer mit x64-Architektur und 64-Bit-Prozessor von AMD™, der die AMD64-Plattform unterstützt
Arbeitsspeicher	1 GB Arbeitsspeicher nur für ScanMail (2 GB Arbeitsspeicher empfohlen)
Festplattenspeicher	5 GB freier Festplattenspeicher
Betriebssystem	Microsoft™ Windows Server™ 2012 R2 Standard oder Datacenter (64 Bit) Microsoft™ Windows Server™ 2012 Standard oder Datacenter (64 Bit)
Mail-Server	Microsoft Exchange Server 2016
Webserver	Microsoft Internet Information Services (IIS) 8.5 Microsoft Internet Information Services (IIS) 8.0 Microsoft Internet Information Services (IIS) 7.5
Browser	Microsoft™ Internet Explorer™ 6.0 oder höher Mozilla Firefox™ 3.0 oder höher
MSXML	4.0 Service Pack 2 oder höher
.NET Framework	4.0 oder 4.5

ScanMail mit Microsoft Exchange Server 2013

Ressource	Anforderungen
Prozessor	Prozessor mit x64-Architektur, der die Intel™ 64-Architektur unterstützt (offizielle Bezeichnung: Intel EM64T) Computer mit x64-Architektur mit AMD™ (64 Bit)
Arbeitsspeicher	1 GB Arbeitsspeicher nur für ScanMail (2 GB Arbeitsspeicher empfohlen)
Festplattenspeicher	5 GB freier Festplattenspeicher
Betriebssystem	Microsoft™ Windows Server™ 2012 R2 Standard oder Datacenter (64 Bit) Microsoft™ Windows Server™ 2012 Standard oder Datacenter (64 Bit) Microsoft™ Windows Server™ 2008 R2 Standard mit Service Pack 1 oder höher (64 Bit) Microsoft™ Windows Server™ 2008 R2 Enterprise mit Service Pack 1 oder höher (64 Bit) Microsoft™ Windows Server™ 2008 R2 Datacenter RTM oder höher (64 Bit)
Mail-Server	Microsoft Exchange Server 2013 SP1 oder höher
Webserver	Microsoft Internet Information Services (IIS) 8.5 Microsoft Internet Information Services (IIS) 8.0 Microsoft Internet Information Services (IIS) 7.5
Browser	Microsoft™ Internet Explorer™ 6.0 oder höher Mozilla Firefox™ 3.0 oder höher
MSXML	4.0 Service Pack 2 oder höher
.NET Framework	4.0 oder 4.5

ScanMail mit Microsoft Exchange Server 2010

Ressource	Anforderungen
Prozessor	Prozessor mit x64-Architektur, der die Intel™ 64-Architektur unterstützt (offizielle Bezeichnung: Intel EM64T) Computer mit x64-Architektur mit AMD™ (64 Bit)
Arbeitsspeicher	1 GB Arbeitsspeicher nur für ScanMail (2 GB Arbeitsspeicher empfohlen)
Festplattenspeicher	5 GB freier Festplattenspeicher
Betriebssystem	Microsoft™ Windows Server™ 2012 R2 Standard oder Datacenter (64 Bit) Microsoft Windows Server 2012 Standard oder Datacenter (64 Bit) Microsoft Windows Server 2008 R2 oder höher (64 Bit) Microsoft Windows Server 2008 mit Service Pack 2 oder höher (64 Bit) Microsoft Small Business Server (SBS) 2011* * Microsoft Small Business Server (SBS) 2011 wurde nur eingeschränkt hinsichtlich der Kompatibilität mit ScanMail Version 12 getestet. Es wird empfohlen, Microsoft ForeFront vor der Installation von ScanMail unter Microsoft Small Business Server (SBS) 2011 zu deinstallieren.
Mail-Server	Microsoft Exchange Server 2010 SP3 oder höher
Webserver	Microsoft Internet Information Services (IIS) 8.0 Microsoft Internet Information Services (IIS) 7.5 Microsoft Internet Information Services (IIS) 7.0
Browser	Microsoft™ Internet Explorer™ 6.0 oder höher Mozilla Firefox™ 3.0 oder höher
MSXML	4.0 Service Pack 2 oder höher
.NET Framework	3.5 Service Pack 1

TREND MICRO™

Securing Your Journey to the Cloud