Trend Micro™

SCANMAIL™ SUITE FOR MICROSOFT® EXCHANGE™

Erstklassiger Schutz. Weniger Aufwand.

Die meisten gezielten Angriffe und Ransomware-Vorfälle beginnen mit Phishing-E-Mails, daher ist Ihre E-Mail-Sicherheit wichtiger denn je. Leider beruhen die meisten Sicherheitslösungen für Mailserver, einschließlich der begrenzten Anzahl integrierter Schutzkomponenten in Microsoft Exchange Server, auf älteren Technologien. Diese sind mit der Erkennung moderner Malware, bösartiger Makros und dateiloser Angriffe häufig überfordert.

ScanMail™ Suite for Microsoft® Exchange™ stoppt selbst gezielte Phishing- und Ransomware-Angriffe durch Predictive Machine Learning die Erkennung von Exploit-Codes in E-Mails und kundenspezifische Sandbox-Analysen verdächtiger Dateien und URLs – ein Schutz, den andere Sicherheitslösungen nicht bieten.

Dank zeitsparender Funktionen wie zentraler Verwaltung, Search & Destroy und rollenbasierter Zugriffssteuerung gilt ScanMail mittlerweile als eine der am einfachsten einzurichtenden und zu bedienenden Sicherheitslösungen.

Software

Geschützte Angriffspunkte

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

Bedrohungsschutz und Datensicherheit

- Virenschutz
- Ransomware-Schutz
- Schutz vor Internetbedrohungen
- Spam-Schutz
- Phishing-Schutz
- Content-Filter
- Schutz vor Datenverlust
- Schutz vor gezielten Angriffen

VORTEILE

Überlegener Schutz vor gezielten Phishing- und Ransomware-Angriffen

- Nutzt modernste Erkennungstechniken, einschließlich Predictive Machine Learning und Erkennung von Exploit-Codes in E-Mails, um unbekannte Bedrohungen in Dateien, Makros und Skripts aufzuspüren
- Sperrt E-Mails mit bösartigen URLs vor der Auslieferung und analysiert URLs erneut in Echtzeit, wenn diese vom Benutzer angeklickt werden
- Stoppt mehrstufige Angriffe, die sich auf E-Mails stützen, welche intern von infizierten Konten oder Geräten aus gesendet wurden
- In Kombination mit Trend Micro™ Deep Discovery™ Analyzer werden verdächtige Dateien/URLs in kundenspezifischen Sandboxes dynamisch analysiert und Kompromittierungsindikatoren (IoCs) an Trend Micro und Sicherheitslösungen von Drittanbietern weitergeleitet

Senkt IT-Kosten

- Vereinfacht sicherheitsrelevante E-Mail-Vorgänge durch leistungsstarke Gruppenkonfiguration und -verwaltung sowie zentralisierte Protokollierung und Berichterstellung
- Eine innovative Search & Destroy-Funktion vereinfacht die mühsame Suche nach Unternehmens-E-Mails
- Vereinfacht Initiativen zur Richtlinieneinhaltung und zur Datensicherheit durch zentral verwalteten, vorlagengestützten Schutz vor Datenverlust

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 kundenspezifische 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 kundenspezifische Bedrohungsdaten sowie adaptive Sicherheitsupdates (bei optionaler Integration von Deep Discovery Analyzer)
- Verhindert das Eindringen von Bedrohungen in Ihre Umgebung durch sofortigen Schutz basierend auf weltweit führenden 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 gespeicherten Daten sowie von Daten während der Übertragung.

- Protokolliert den Fluss vertraulicher Daten durch Ihr E-Mail-System und den Mail-Speicher.
- Beschleunigt die Installation und verbessert die Präzision mit mehr als 100 Vorlagen zur Einhaltung von Compliance-Richtlinien
- 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 Hybrid-Umgebungen mit Office 365 und Exchange Server in Verbindung mit Trend Micro™ Cloud App Security
- Maximiert mit TrustScan die Effizienz durch Multi-Thread-Suchen sowie automatische Anpassung der CPU-Last und vermeidet doppelte Scans
- Integriert sich in den 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 mit Search & Destroy gesuchte E-Mails schnell und präzise.

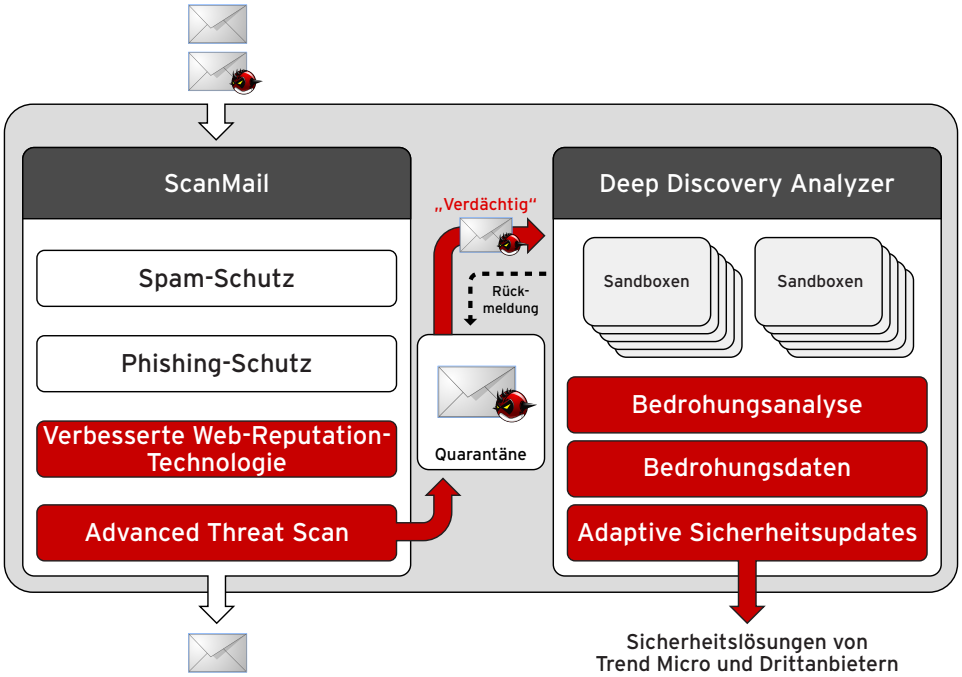
- Führt gezielte Suchläufe über Exchange mithilfe von Schlüsselwörtern und regulären Ausdrücken durch
- Ermöglicht Administratoren, schnell auf dringende Anfragen von z. B. Rechts-, Personal- und Sicherheitsabteilungen zu reagieren, um bestimmte E-Mails bei Bedarf zu suchen, nachzuverfolgen oder auch dauerhaft zu löschen.

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

CONNECTED THREAT DEFENCE

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 **Advanced Threat Scan Engine** (ATSE) erkennt komplexe Malware in Adobe PDF, MS Office und anderen Dokumentenformaten durch heuristische Logik zur Erkennung bekannter und Zero-Day-Exploits. Die Engine durchsucht außerdem den Mail-Speicher von Exchange nach gezielten Bedrohungen, die möglicherweise bereits in das Netzwerk eingedrungen waren, bevor der Schutz verfügbar wurde.

Bei **Integration in Deep Discovery Analyzer** verschiebt ScanMail verdächtige Anhänge und URLs 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 und URLs in einer sicheren Sandbox-Umgebung. Anwender können mehrere vollständig kundenspezifische Ziel-Images erstellen, die genau ihren Host-Umgebungen entsprechen, und damit verdächtige Objekte analysieren.

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 anpassbaren Schutz und Bedrohungsbeseitigung durch ScanMail, andere Trend Micro Lösungen für Endpunkte und Gateways sowie Drittanbieter-Produkte.

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™ 2016 Standard oder Datacenter (64 Bit) 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) 10.0 Microsoft Internet Information Services (IIS) 8.5 Microsoft Internet Information Services (IIS) 8.0
Browser	Microsoft™ Internet Explorer™ 7.0 oder höher Mozilla Firefox™ 3.0 oder höher
MSXML	4.0 Service Pack 2 oder höher
.NET Framework	4.5 oder 4.6

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™ 7.0 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
Browser	Microsoft™ Internet Explorer™ 7.0 oder höher Mozilla Firefox™ 3.0 oder höher
MSXML	4.0 Service Pack 2 oder höher
.NET Framework	3.5 Service Pack 1