Trend Micro™

INTERSCAN™ MESSAGING SECURITY

Abwehr eingehender Bedrohungen und Schutz ausgehender Daten

Über 90 % aller E-Mails sind Spam. Mit zunehmender Anzahl gezielter Spear-Phishing-Angriffe könnte selbst einer Ihrer versiertesten Mitarbeiter einmal aus Versehen auf einen bösartigen Link klicken und Ihr Unternehmen der Gefahr von Cyberkriminalität aussetzen.

Trend Micro™ InterScan™ Messaging Security bietet umfassenden Schutz vor herkömmlichen wie auch gezielten Angriffen. Mit den korrelierten Bedrohungsinformationen aus dem Trend Micro™ Smart Protection Network™ und optionalen Sandbox-Analysen sperrt die Lösung Spam, Phishing und komplexe, hartnäckige Bedrohungen (Advanced Persistent Threats, APTs). Die integrierte Option für eine hybride SaaS-Installation kombiniert eine leistungsstarke virtuelle Gateway-Appliance mit einem SaaS-Vorfilter, der den Großteil an Bedrohungen und Spam bereits in der Cloud stoppt – also sehr viel näher an ihrer Quelle. Diese hybride Lösung vereint die Vorteile beider Computing-Welten: den Datenschutz und die Kontrolle einer lokal installierten Appliance mit den Ressourceneinsparungen und dem proaktiven Schutz eines cloudbasierten Vorfilters.

Das Datenschutz- und Verschlüsselungsmodul erfüllt die strengsten Auflagen zu Regeleinhaltung und Datenschutz durch den Schutz ausgehender Daten. Dieses optionale Modul bietet benutzerfreundliche identitätsbasierte Verschlüsselung und anpassbare DLP-Vorlagen (Data Loss Prevention), um die Verteilung zu beschleunigen.

SICHERHEITSLÖSUNG FÜR MAIL-GATEWAYS

Geschützte Punkte

- Messaging-Gateway
- Ein- und ausgehende Daten
- Internetcloud

Bedrohungsschutz

- Gezielte Angriffe
- Richtlinienverstöße
- Datenverlust
- Unangemessene Inhalte
- Links zu bösartigen Websites
- Spear-Phishing
- Spam und Botnetze
- Spyware
- Viren

VORTEILE

Schützt Unternehmen vor APTs und anderen gezielten Angriffen

- Minimiert das Risiko gezielter Angriffe durch vielseitigen ScanMail-Schutz
- Führt Ausführungsanalysen in Ihrer ganz speziellen Umgebung durch und bietet individuelle Bedrohungsdaten über die Integration von Deep Discovery Advisor

Sperrt mehr Malware, Phishing und Spam durch Reputationstechnologie

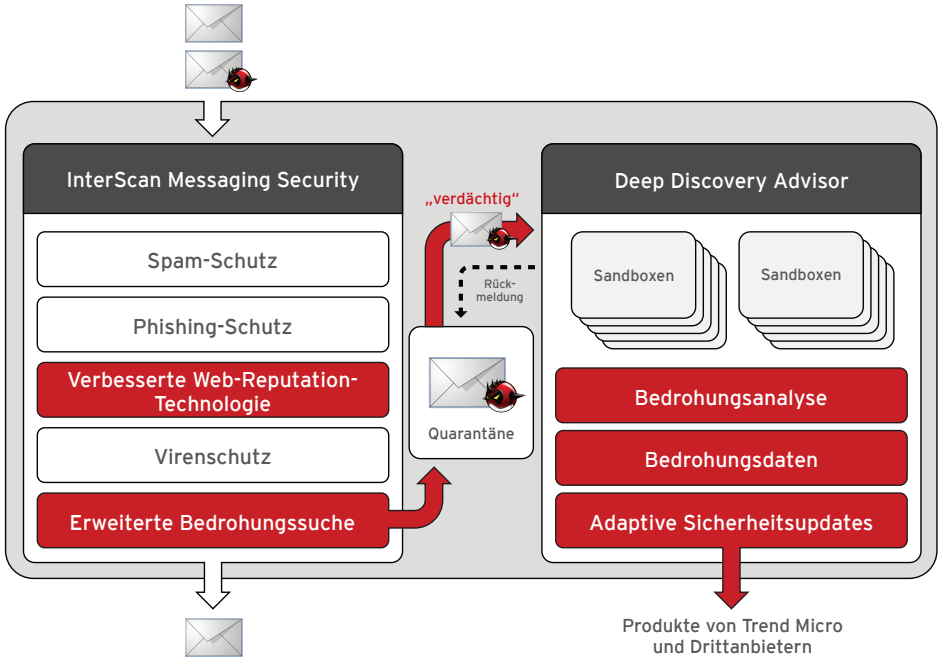
- Sondert 85 % aller eingehenden E-Mails durch Reputationsüberprüfung von Absendern aus und entlastet damit die Netzwerkressourcen
- Stoppt laut unabhängigen Tests mehr Spam mit weniger Fehlalarmen als andere Sicherheitslösungen
- Überprüft bösartige Links innerhalb der E-Mail, um Phishing-Angriffe durch verbesserte Web-Reputation-Technologie abzuwehren

Vereinfacht Datenschutz und Verschlüsselung

- Erleichtert den Schutz ausgehender E-Mails für alle Beteiligten durch identitätsbasierte E-Mail-Verschlüsselung
- Eliminiert Voranmeldung und Zertifikatsverwaltung bei der PKI-Verschlüsselung durch einen dynamischen Schlüsselgenerator
- Vereinfacht das Erfüllen von Auflagen zur Richtlinieneinhaltung und den Schutz vor Datenverlust durch anpassbare DLP-Vorlagen
- Reduziert Verwaltungsaufwand und beschleunigt Überprüfungen der Richtlinieneinhaltung durch Erstellung ausführlicher Berichte

GEZIELTE ANGRIFFE ERFORDERN EINE INDIVIDUELLE ABWEHR

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



Komponenten von InterScan Messaging Security

InterScan Messaging Security wurde durch die Integration verschiedener Arten von 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 großer Datenmengen und Vorhersagetechnologien korreliert.

Die **optimierte Scan-Engine** erkennt komplexe Malware in Adobe PDF, MS Office und anderen Dokumentformaten durch statische und heuristische Logik zur Erkennung bekannter und Zero-Day-Exploits. 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.

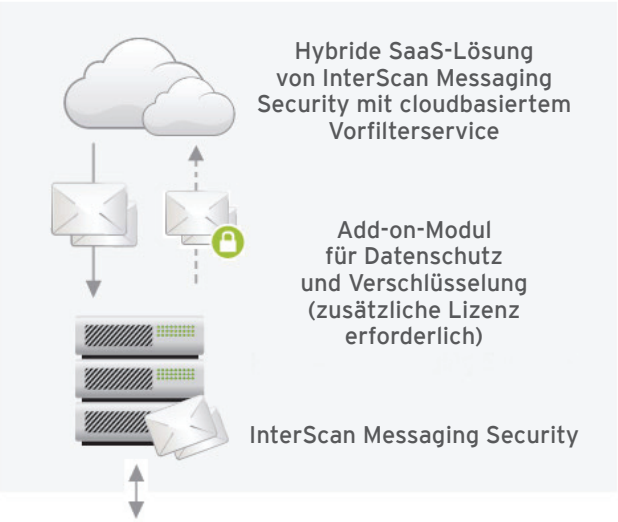
Komponenten von Deep Discovery Advisor (zusätzlich zu erwerben)

Die Appliance Deep Discovery Advisor bietet Sandboxing, netzwerkweite Protokollerfassung und eine detaillierte Bedrohungsanalyse auf einer gemeinsamen Informationsplattform, dem Herzstück der individuellen Bedrohungsabwehr von Trend Micro.

Individuelle Bedrohungsanalysen bieten automatische und detaillierte Simulationsanalysen von potenziell bösartigen Anhängen, einschließlich ausführbaren und gemeinsamen Office-Dokumenten in einer sicheren Sandbox-Umgebung. Der Anwender kann damit mehrere vollständig benutzerdefinierte Zielimages erstellen und analysieren, die genau ihren Host-Umgebungen entsprechen.

Individuelle Bedrohungsinformationen analysieren Protokolle von Trend Micro Produkten und Drittanbieterlösungen, um in Kombination mit Trend Micro Bedrohungsinformationen ausführliche Einblicke zu bieten und damit eine risikobasierte Bewertung, Eindämmung und Beseitigung von Vorfällen zu ermöglichen.

Adaptive Sicherheitsupdates stellen individuelle Sicherheitsupdates bereit, um einen anpassbaren Schutz und eine wirksame Bedrohungsbeseitigung durch InterScan Messaging Security sowie weitere Trend Micro Produkte und Sicherheitslösungen von Drittanbietern auf verschiedenen Ebenen zu ermöglichen.



Virtuelle Appliance mit hybrider SaaS-Installation

Virtuelle Appliance und Cloud-Sicherheit Die integrierte hybride SaaS-Lösung von Trend Micro bietet eine einheitliche Management-Konsole zur umfassenden Verwaltung aller Komponenten – des cloudbasierten Vorfilterservices, der virtuellen Content Security-Appliance und des zusätzlichen Moduls für Datenschutz und Verschlüsselung.

DIE WICHTIGSTEN FUNKTIONEN

Cloudbasierter Filter eingehender E-Mails

- Reduziert den Aufwand am E-Mail-Gateway, indem E-Mails bereits in der Cloud gefiltert werden
- Senkt Rechenzentrumskosten und IT-Personalaufwand
- Ermöglicht die schnelle und bedarfsgerechte Bereitstellung neuer Kapazitäten
- Beinhaltet ein Service Level Agreement mit garantierter E-Mail-Verfügbarkeit

Add-on-Modul für Datenschutz und Verschlüsselung (zusätzliche Lizenz erforderlich; verfügbar für Installationen als virtuelle Appliance oder Software-Appliance)

- Löst automatische Verschlüsselung, Quarantäne oder benachrichtigungsbasierte Filterrichtlinien aus
- Beschleunigt die Konfiguration von DLP-Content-Filterregeln durch anpassbare Vorlagen für die Richtlinieneinhaltung
- Reduziert die Abhängigkeit von anwendergesteuerter Verschlüsselung durch eine automatische richtliniengesteuerte Gateway-Lösung
- Behebt den bisherigen Aufwand für die Schlüsselverwaltung durch identitätsbasierte Verschlüsselung
- Ermöglicht es dem Personal, das für die Richtlinieneinhaltung verantwortlich ist, DLP-Richtlinien und -Verstöße für dieses und andere Trend Micro Produkte über den Control Manager™ zentral und durchgängig zu verwalten

Echtzeitschutz vor sich ständig entwickelnden Bedrohungen

- Führt Web-Reputation-Datenbankabfragen in Echtzeit aus, um E-Mails mit bösartigen Links zu sperren
- Überprüft die Reputation von E-Mails, um Nachrichten aus Spam-Quellen und betrügerischen „Fast Flux"-Service-Netzwerken zu sperren
- Verbessert Präzision und Reaktionsgeschwindigkeit durch cloudbasierten Abgleich von Bedrohungen
- Erkennt Marketing-Massenmails, um eine separate Verfügung für diese E-Mails zu ermöglichen
- Integriert ausgezeichneten mehrschichtigen Spam-Schutz, leistungsstarke Reputationsfilter und Virenschutz

Anpassung und Kontrolle über eine einzige Management-Konsole

- Vereinfacht die Verwaltung des cloudbasierten Vorfilters, die Überprüfung von lokal gespeicherten Inhalten sowie DLP und Verschlüsselung
- Unterstützt konfigurierbare Richtlinien und gezielte regelbasierte Filter
- Identifiziert Massenmails, damit Kunden diese durch separate Richtlinien bewältigen können
- Integriert Quarantäne, Protokolle und Berichte, um die Verwaltung, Nachrichtenprotokollierung und Transparenz zu optimieren

ENTSCHEIDENDE VORTEILE

- Spart Ressourcen ein, da Spam im Internet – außerhalb des Netzwerks – gestoppt wird
- Schützt vor bösartigen Links und Spear-Phishing-Angriffen
- Sperrt gezielte Malware mithilfe von Sandbox-Analysen
- Minimiert Risiken dank prädiktivem Echtzeitschutz
- Verschlüsselt vertrauliche, ausgehende E-Mails
- Verhindert Datenverlust und Richtlinienverstöße
- Senkt Verwaltungs- und Gesamtbetriebskosten
- Fördert Initiativen zur Konsolidierung von Rechenzentren

> „Die hybride Sicherheitslösung InterScan Messaging Security Virtual Appliance stellt eine äußerst kosteneffiziente und zukunftsorientierte Lösung für Großunternehmen wie uns dar."

Steven Jones
Leitender Systemadministrator
Der Bezirk Dane in Wisconsin

INTERSCAN MESSAGING SECURITY

MINDESTSYSTEMVORAUSSETZUNGEN

VIRTUELLE APPLIANCE UND SOFTWARE-APPLIANCE

Server-Plattform-Kompatibilität

- Virtuelle Appliances: VMware ESX/ESXi v3.5 und höher; Microsoft Hyper-V Windows 2008 SP1 oder Windows 2008 R2
- Software Appliances: Die neuesten, von Trend Micro zertifizierten Plattformen finden Sie unter www.trendmicro.com/go/certified

Hardwarevoraussetzungen

- Zwei Intel™ Xeon Prozessoren
- 4 GB Arbeitsspeicher
- 120 GB Festplattenspeicher

Empfohlene Hardwarevoraussetzungen

- Vier Intel™ Xeon Prozessoren
- 8 GB Arbeitsspeicher
- 250 GB Festplattenspeicher

SOFTWAREVERTEILUNG

Microsoft™ Windows™, Linux™

- 2 GB Arbeitsspeicher
- 80 GB Festplattenspeicher: 500 MB Festplattenspeicher für die Installation, zusätzlicher Festplattenspeicher für E-Mail-Speicher und Datenbank erforderlich
- Microsoft Internet Explorer 6 SP1, 7, 8 oder Firefox 3
- LDAP Server Microsoft Active Directory 2000 oder 2003, IBM Lotus Domino 6.0 oder höher oder Sun One LDAP

Microsoft Windows:

- Windows Server 2008 mit SP 2.0 oder höher
- Windows Server 2003 mit SP 2.0 oder höher
- Windows Server 2003 R2 mit SP 2.0 oder höher
- Zwei Intel Xeon Prozessoren, 3 GHz oder höher
- Microsoft Desktop Engine oder Microsoft SQL Server 2000 oder höher, SQL Express 2005 oder höher

Linux

- Red Hat™ Enterprise Linux 3, 4 oder 5
- Intel Dual Pentium IV 3 GHz
- 2 GB Auslagerungsspeicher
- PostgreSQL Version 8.1.3 oder höher
- MTA Postfix 2.1 oder höher; Sendmail; Qmail

FLEXIBLE VERTEILUNG

Virtuelle Appliance: virtualisierte Verteilung über Hypervisor-Technologien. Enthält hybriden SaaS-Vorfilter und die Option zum Kauf eines zusätzlichen Datenschutz- und Verschlüsselungsmoduls.

- Microsoft® Hyper-V™ Virtual Appliance
- VMware Ready-zertifizierte virtuelle Appliance: streng getestet und geprüft von VMware; ausgezeichnet durch VMware Ready-Zertifizierung. Unterstützung von VMware ESX oder ESXi v3.5 und vSphere.

Software Appliance: „Bare-Metal"-Installation mit optimiertem, robustem Betriebssystem. Enthält hybriden SaaS-Vorfilter und die Option zum Kauf eines zusätzlichen Datenschutz- und Verschlüsselungsmoduls.

- Von Trend Micro zertifiziert: In ausführlichen Tests und Prüfungen zertifiziert Trend Micro Hardwareplattformen hinsichtlich der Kompatibilität mit Trend Micro Software-Appliances. Zertifizierte Server-Plattformen anzeigen

Softwarelösung: einfache Installation auf Standardhardware unter Microsoft Windows oder Linux OS.

- Die InterScan Messaging Security Suite bietet denselben erstklassigen Spam- und Malware-Schutz sowie ausgezeichnete Content-Filter in einer standardmäßigen Softwarelösung. Der SaaS-Vorfilter sowie das Datenschutz- und Verschlüsselungsmodul sind in dieser Implementierung nicht verfügbar. Die Integration in Deep Discovery Advisor ist für 2013 geplant.