

Produktübersicht

Auf einen Blick

Symantec® Messaging Gateway (SMG) schützt Ihre E-Mail-Kommunikation vor Spam, Malware und gezielten Angriffen.

Wichtigste Vorteile

- Erweiterte Bedrohungen stoppen
- Verhinderung unerwünschter E-Mails
- Schutz sensibler Daten
- Ermöglicht einen tiefen Einblick in Messaging-Bedrohungen

Schlüsselfunktion

- Mehrschichtige Erkennungstechnologien
- Erweiterte Inhaltsfilterung
- Schutz vor Datenverlust
- Detailliertes Auditing
- Leistungsstarke Sicherheitsintegrationen

Messaging Gateway

Inbound and Outbound Messaging Security

Übersicht

Die E-Mail ist einer der wichtigsten Kommunikationskanäle für jedes Unternehmen. Sie ist auch einer der beliebtesten und am weitesten verbreiteten Vektoren für Cyber-Kriminelle, um Bedrohungen zu lancieren und zu verbreiten, einschließlich Spear-Phishing, Ransomware und Angriffe auf Unternehmens-E-Mails. Der Mensch wird oft als das schwächste Glied in jedem Sicherheitsprogramm angesehen. Ein versehentlicher Klick auf einen falschen Link oder das Versenden einer Datei mit sensiblen Daten kann katastrophale Folgen haben. Intelligente, umfassende E-Mail-Sicherheit, unabhängig davon, ob Ihr E-Mail-System vor Ort, cloudbasiert oder beides ist, beginnt damit, diese Art von Ereignissen zu verhindern. Blockieren und isolieren Sie verdächtige E-Mails, bevor sie Ihre Benutzer erreichen, und überwachen Sie ausgehende E-Mails, um sicherzustellen, dass Ihre Unternehmensdaten geschützt sind.

Symantec® Messaging Gateway (SMG) ist eine lokale E-Mail-Sicherheitslösung, die mit den folgenden Funktionen Sicherheit für ein- und ausgehende Nachrichten bietet:

- Mehrschichtige Erkennungstechnologien
- Erweiterte Inhaltsfilterung
- Schutz vor Datenverlust
- Detailliertes Auditing
- Leistungsstarke Sicherheitsintegrationen

Mit diesen Kernfunktionen schützt SMG die E-Mail-Kommunikation vor Spam, Malware und gezielten Angriffen. Es verhindert auch versehentliche oder böswillige Datenlecks. Darüber hinaus kann SMG als virtuelle oder physische Appliance implementiert werden, und Sie können die Kapazität problemlos erweitern, um den Nachrichtenfluss aufrechtzuerhalten, wenn das Spam-Aufkommen zunimmt.

Mehrschichtige Erkennungstechnologien stoppen fortgeschrittene Bedrohungen

SMG kombiniert mehrschichtige Erkennungstechnologien mit Erkenntnissen aus dem weltweit größten zivilen Threat Intelligence Network, um verdächtige E-Mails effektiv zu blockieren und unter Quarantäne zu stellen.

- **BEC-Angriffe (Business Email Compromise):** Die Lösung nutzt fortschrittliche Heuristiken, eine BEC-Betrugsanalyse-Engine, Absenderauthentifizierung und Domain-Intelligenz, um URL-Hijacking und Identitätsspoofing zu verhindern.
- **Spear-Phishing-Angriffe:** Die Lösung schützt vor böartigen Links, die in Spear-Phishing-Kampagnen verwendet werden, mit URL-Reputationsfilterung auf der Grundlage der globalen Symantec-Datenbank, die Links identifiziert, die bekannten Phishing-Angriffen ähneln.
- **Ransomware-Angriffe:** Die Lösung schützt Benutzer vor gezielten Ransomware-Angriffen, indem sie Zero-Day-Dokumentenbedrohungen aus Microsoft Office- und PDF-Anhängen entfernt. Alle potenziell böartigen aktiven Inhalte werden aus einem Anhang entfernt und ein sauberes Dokument wird rekonstruiert, wieder an die E-Mail angehängt und an den Endbenutzer gesendet.
- **Directory Harvesting-Angriffe:** Die Lösung nutzt, eine Kombination aus globalen und lokalen Symantec-Datenbanken zur Absenderreputation, Heuristiken und kundenspezifischen Spam-Regeln, die bis zu 99 Prozent der unerwünschten E-Mails zurückhalten, bevor sie Ihr Netzwerk erreichen. Darüber hinaus wird durch die Drosselung ausgehender Absender verhindert, dass ausgehende Spam-Angriffe von kompromittierten internen Benutzern ausgehen und sich negativ auf die Absenderreputation auswirken.
- **Angriffe durch Nachahmung:** Die Lösung unterstützt Absenderauthentifizierungsprotokolle wie DMARC, DKIM und SPF und schützt so alle Empfänger vor Imitationsangriffen.

Inhaltsfilterung verhindert unerwünschte E-Mails

Die fortschrittliche Inhaltsfilterung von SMG verhindert, dass unerwünschte E-Mails wie Newsletter und andere Marketing-Inhalte die Benutzer erreichen. Die Lösung nutzt außerdem eine Kombination aus globalen und lokalen Symantec-Datenbanken zur Absenderreputation, Heuristiken und kundenspezifischen Spam-Regeln, die bis zu 99 % des Spams abfangen, bevor er Ihr Netzwerk erreicht.

Data Loss Prevention schützt sensible Daten

SMG bietet integrierte Richtlinien zum Schutz vor Datenverlust, die den Schutz von Unternehmensdaten in Nachrichten oder Anhängen erleichtern. Administratoren können mithilfe von 100 vorgefertigten Wörterbüchern, Mustern und Richtlinienvorlagen wirksame und flexible Richtlinien erstellen, die Sie bei der Implementierung automatisierter Datenschutz- und Durchsetzungsrichtlinien unterstützen. Darüber hinaus bietet die Lösung eine automatische SMTP-over-TLS-Verschlüsselung, die gewährleistet, dass die gesamte E-Mail-Kommunikation während der Übertragung sicher ist.

Detailliertes Auditing ermöglicht Messaging Sicherheitsmanagement mit tiefer Transparenz

Detailliertes Auditing ermöglicht Messaging Sicherheitsmanagement mit tiefem Einblick. SMG umfasst eine einzige webbasierte Konsole, die eine granulare Richtlinienkonfiguration und -kontrolle, detaillierte Berichte und eine konsolidierte Ansicht von Bedrohungstrends, Angriffsstatistiken und Vorfällen, die gegen die Vorschriften verstoßen, bietet.

- **Überwachungswerkzeuge:** Dashboard-, Übersichts- und Detailberichte, einschließlich 50 voreingestellter Berichte, die nach Inhalt und Zeitplan anpassbar sind, zeigen Bedrohungstrends und potenzielle Compliance-Probleme auf.
- **SIEM-Integration:** Erstellte Syslog-Daten können zur weiteren Korrelationsanalyse in Sicherheits- und Informationstools (SIEM) von Drittanbietern exportiert werden.
- **Benutzerfreundlich:** Die einfache Nachverfolgung von Nachrichten über eine grafische Schnittstelle zur Nachrichtenprüfung ermöglicht eine schnelle Bestimmung der Nachrichtenverwendung und des Zustellungsstatus.

Darüber hinaus gewährleistet die Lösungsarchitektur, dass mehrere SMG-Appliances in einer gemischten IPv4- und IPv6-Umgebung verwaltet werden können.

Leistungsstarke Sicherheitsintegrationen

Für zusätzlichen erweiterten Schutz vor Bedrohungen kann SMG dateibasierte Nachrichteninhalte zur weiteren Prüfung an Symantec Content Analysis weiterleiten. Diese Prüfung umfasst verwertbare Informationen, die statische Analyse, maschinelles Lernen und Verhaltensanalyseverfahren kombinieren. Eine adaptive und anpassbare Sandbox bietet eine umfassende Malware-Detonation, um verdächtige Dateien schnell zu analysieren, mit laufender Malware zu interagieren, um deren vollständiges Verhalten aufzudecken und Zero-Day-Bedrohungen und unbekannte Malware zu entlarven. SMG lässt sich eng mit Symantec DLP integrieren, um die Durchsetzung von Richtlinien auf den E-Mail-Kanal auszuweiten. Schließlich ist eine richtlinienbasierte Verschlüsselung als Symantec Content Encryption-Add-on verfügbar.

Flexibilität bei der Bereitstellung

Die SMG-Software ist auf verschiedenen Plattformen verfügbar und kann in flexiblen Rollen eingesetzt werden. Sie bietet eine modulare und skalierbare Architektur, die den Anforderungen des Unternehmens entspricht.

Funktion	Beschreibung
Plattform Support	VMware, HyperV, KVM, Microsoft Azure, Symantec Messaging Gateway Appliance 8390 Hardware
Einsatzrollen	Nur All-in-One-Scanner, Kontrollzentrum und Quarantäne-Scanner; nur Quarantäne
Formfaktor des Geräts	1U rack mount
CPU	Dual 20 Core processor
Memory: Hard Drive/RAID	192-GB RAM, 6 x 2.4-TB hard drive (RAID 10)
NIC	Dual port 1-Gb onboard, dual port 10GbE Base-T adapter

Zusammenfassung

SMG bietet eine umfassende Reihe von Funktionen zur Erkennung von Bedrohungen, die ein- und ausgehende E-Mail-Nachrichten schützen. Diese Funktionen verhindern heimtückische E-Mail-Bedrohungen wie die Kompromittierung von Geschäfts-E-Mails, Ransomware und Spam und stellen sicher, dass Ihre Benutzer nicht versehentlich vertrauliche Daten versenden. Die Lösung lässt sich auch in andere führende Symantec-Sicherheitslösungen integrieren, um zusätzlichen Schutz vor Messaging-Bedrohungen zu bieten.

Für weitere Informationen besuchen Sie bitte: broadcom.com/symantec-smg