

Google Message Security



ÜBER GOOGLE SECURITY AND ARCHIVING

Die Google Security and Archiving-Services, bereitgestellt von Postini, sorgen für mehr Sicherheit und Compliance in Ihrem bestehenden E-Mail-System. Diese Produkte befinden sich auf einer gehosteten Service-Plattform und blockieren Spam, Phishing, Malware und andere Eindringlinge, bevor diese Ihr Netzwerk erreichen. Sie bieten außerdem Content-Management und Archivierungsfunktionen an, damit den gesetzlichen Anforderungen besser entsprochen werden kann. Das gehostete Modell von Google bietet verschiedene Vorteile. Dadurch, dass die Google-Technologie den „Netzwerkeffekt“ von zehntausenden E-Mail-Netzwerken wirksam einsetzt, werden neue Bedrohungen in Echtzeit erkannt und im ganzen Google-Sicherheitsnetzwerk blockiert – ohne dass Aktualisierungen vor Ort notwendig sind. Gleichzeitig halten die Größenvorteile beim Speicher, die einfache Bereitstellung und der wartungsfreie Service die Gesamtbetriebskosten niedrig.

Weitere Informationen finden Sie unter www.google.com/postini.

Google Message Security, bereitgestellt von Postini, bietet Unternehmen aller Größen effektive Sicherheit für eingehende und ausgehende E-Mails. Es vereinfacht die Verwaltungsaufgaben in Bezug auf Sicherheit und Compliance von E-Mail-Nachrichten und setzt wertvolle IT-Ressourcen frei. Google Message Security ist immer aktiv und immer aktuell, sodass Unternehmen die Gewissheit haben können, zu jeder Zeit einen effektiven und verlässlichen Schutz für ihre E-Mails zu haben.

Durch die Verwendung einer patentierten On-Demand-Architektur blockiert Google Message Security Spam, Phishing, Viren und andere E-Mail-Bedrohungen, bevor diese Ihr Unternehmen erreichen. Die Software verringert so die Belastung Ihrer E-Mail-Server, spart außerdem Bandbreite und verbessert die Leistung Ihrer bereits vorhandenen Nachrichteninfrastruktur. Google Message Security wird in einer Software-as-a-Service-(SaaS-)Ausführung bereitgestellt. Dadurch, dass keine Software oder Hardware installiert und gewartet werden muss, können Geld und IT-Ressourcen gespart werden.

Google Message Security schont IT-Ressourcen, weil ständiges Patchen und häufige Aktualisierungen, die bei anderen Appliance- oder Software-Lösungen erforderlich sind, nun entfallen. Es senkt außerdem die Belastung Ihrer IT-Abteilung, indem Endnutzer die Berechtigung erhalten, ihre eigenen Nachrichtenquarantänen und -einstellungen mithilfe einer benutzerfreundlichen, webbasierten Oberfläche zu verwalten. Anstatt Ihren Help Desk anzurufen, können Endnutzer ihre Nachrichtenquarantänen überprüfen und sämtliche erwünschten Nachrichten zustellen. Nutzer erhalten regelmäßig einen Quarantäneüberblick per E-Mail mit den Quarantänedetails. Sie können ihre Spam-Schutzeinstellungen auch genau auf ihre bevorzugte Stufe abstimmen. Die Einstellungsfunktionen für Endnutzer können auf Richtlinienebene komplett konfiguriert werden und bieten Ihnen so vollständige Kontrolle über die Berechtigungen der Endnutzer.

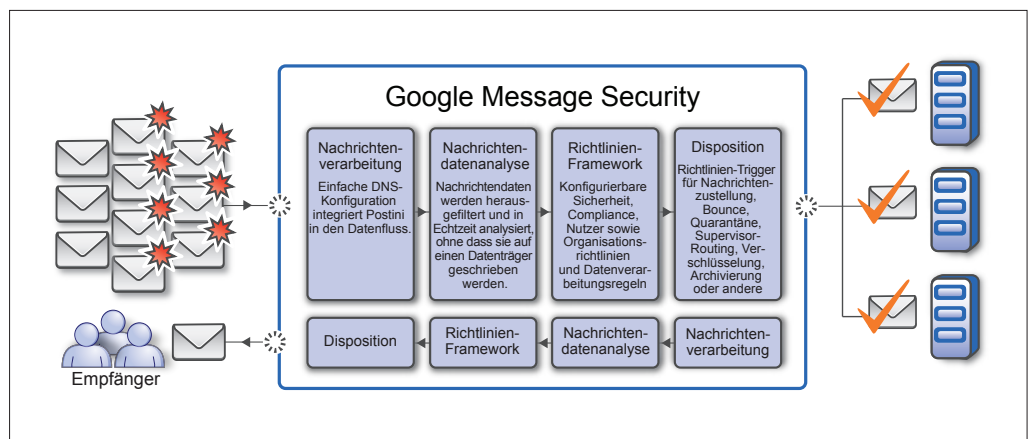


Abbildung 1: Google Message Security bietet Unternehmen aller Größen effektive Sicherheit für eingehende und ausgehende E-Mails.

Google Message Security kann Ihre E-Mail-Sicherheitsrichtlinien automatisch in Kraft setzen. Dank der Durchsetzung der Richtlinien kann die gesetzliche und behördliche Compliance für eingehende und ausgehende E-Mails in Ihrem Unternehmen sichergestellt werden. Der integrierte Transport Layer Security (TLS)-Support kann sensible E-Mail-Kommunikationen verschlüsseln und automatisch für jegliche Kommunikation zwischen ausgewiesenen E-Mail-Domains angewandt werden. Dadurch ist gewährleistet, dass sensible oder regulierte Kommunikation stets auf einer angemessenen Sicherheitsstufe zugestellt wird.

Google Message Security bietet außerdem eine benutzerfreundliche Web-Konsole zu Administrationszwecken. Diese Konsole ermöglicht Konfigurationen und Richtlinienanpassungen in Echtzeit sowie Benachrichtigungen und umfassende Berichte für Administratoren. Nutzer können in der Konsole definiert werden bzw. Google Message Security kann zur Nutzersynchronisierung in die Verzeichnisstruktur Ihres Unternehmens integriert werden.

Google Message Security umfasst mehrere Komponenten, die zusammengenommen einen effektiven Schutz gegen E-Mail-Bedrohungen bilden. Zu den besonderen Fähigkeiten gehören:

- Die Gefahrenerkennung in Echtzeit basiert auf der Verarbeitung von mehr als zwei Milliarden E-Mail-Nachrichten pro Tag und bietet somit globale Sichtbarkeit bei entstehenden Bedrohungen. Dieser „Netzwerkeffekt“ erkennt und verfolgt automatisch Internet Protocol (IP)-Adressen, die Spam, Viren, Denial-of-Services (DoS) usw. in Umlauf bringen. Sobald die Bedrohung erkannt ist, werden diese Seiten für alle Nutzer von Google Message Security gesperrt. Die Erkennungsfunktion korrigiert sich außerdem selbst. Sobald von den identifizierten IP-Adressen keine Gefahr mehr ausgeht, dürfen sie wieder einfache Simple Mail Transfer Protocol (SMTP)-Verbindungen aufbauen, um seriöse E-Mail-Nachrichten zu versenden.
- Eine patentierte Anti-Spam-Technologie überprüft in Echtzeit tausende Elemente einer E-Mail-Nachricht, um zu bestimmen, ob diese Spam ist. Sie bietet eine äußerst effektive Spam-Filterung und außergewöhnlich niedrige Falsch-Positiv-Raten.
- Der Virenschutz baut auf der Spamerkennung auf und umfasst eine „Nullstunden“-Heuristik sowie eine signaturbasierte Erkennungsmethode, dazu mehrere kommerzielle Anti-Viren-Engines.
- Mit Content-Management können Sie Richtlinien für eingehende und ausgehende E-Mails festlegen und so eine zusätzliche Sicherheitsstufe gegen externe Bedrohungen erreichen. Es bietet außerdem Schutz vor versehentlich oder böswillig verursachten Lecks in Bezug auf vertrauliche Daten bei ausgehenden E-Mail-Nachrichten und deren Anhängen.
- Anhangverwaltungstechnologien ermöglichen es Ihnen, spezielle Richtlinien bezüglich Dateianhängen zu erstellen. Sie ermöglichen außerdem das Blockieren oder Unter-Quarantäne-Stellen von Nachrichten basierend auf dem Typ bzw. der Größe von an die E-Mail-Nachrichten angehängten Dateien. Die Anhangverwaltung überprüft auch archivierte Dateien, wie .zip- oder .rar-Dateien, um deren Inhalt zu bewerten, und ermöglicht es Ihnen, spezielle Richtlinien für die Handhabung von archivierten Dateien festzulegen.

Funktion	Vorteile
Patentierter Pass-through-Architektur	Bietet äußerst effektive Spam-Filterung und niedrige Falsch-Positiv-Raten
Mehrschichtige Virenblockierung, Heuristik und signaturbasierte Erkennung	„Nullstunden“-Schutz vor schnell mutierenden Viren, 100 % Anti-Viren-SLA
Skalierbare, hochverfügbare SaaS-Plattform, SLA zur 99,999 % igen Verfügbarkeit	Bietet einen „Immer aktiv, immer aktuell“-Schutz mit niedrigerem TCO
Webbasierte Administrationskonsole	Ermöglicht Nutzer- und Richtlinienaktualisierungen in Echtzeit, Konfigurationsänderungen und Berichterstattung
Directory Harvest Attack/Denial of Service-Blockierung	Verhindert Angriffe durch patentierte Behavior Analysis
Richtlinienbasierte TLS-Verschlüsselung	Sichere Übermittlung von E-Mails
Anhangfilterung	Inkraftsetzung von Richtlinien für E-Mail-Anhänge
Inhaltsrichtlinienverwaltung	Inkraftsetzung von annehmbaren Nutzungsrichtlinien und Inhalts-Compliance
E-Mail-Spooling	Ununterbrochener Empfang von E-Mail-Nachrichten sogar im Falle eines Serverausfalls

