



Der Einsatz
hybrider Messaging
Security führt zu
erhöhter Effizienz
und mehr Schutz
und maximiert
Investitionen.

Durch einen größeren Überblick kann bessere Messaging Security erreicht werden. Websense Hybrid Messaging Security bietet umfangreichen Schutz vor hybriden Web- und E-Mail-Bedrohungen.

Websense[®]

Hybrid Messaging Security

Heutige E-Mail-Bedrohungen sind wesentlich invasiver und heftiger als je zuvor und die Art und Weise dieser Angriffe ändert sich ständig. Das moderne Business muss Security-Lösungen im Einsatz haben, die mehr können, als Spam zu blockieren. Eine gute Messaging Security-Lösung bietet klare Standards zur Risikominderung und unterstützt zudem Corporate Compliance und Governance-Richtlinien.

Websense Hybrid Messaging Security verbindet Websense Hosted Email Security, die auf Internet-Level ansetzt und Websense Email Security, die am Gateway eingesetzt wird. Durch den mehrstufigen und hybriden Einsatz dieser Lösung, sind Unternehmen noch besser geschützt und können im Gegensatz zu einer einzigen Anwendung, eine Vielzahl von Sicherheitsanforderungen erfüllen.

Unternehmen und Analysten schätzen es zunehmend, Schutz dort zu gewährleisten, wo es am meisten Sinn macht. Mit dem Einsatz von mehrstufiger Messaging Security wird höhere Effizienz und mehr Schutz erzielt, während Investitionen in Netzwerk-Ressourcen maximiert werden können.

Wie es funktioniert

Websense Hosted Email Security filtert Spam und Viren auf Internet-Level. Dadurch wird Bandbreite und Zeit für die Verwaltung und System-Ressourcen eingespart.

On-premise: Websense Email Security sitzt am Gateway und bietet granularen Schutz bei ausgehenden E-Mails. Unternehmen haben so die Möglichkeit, fein abgestimmte Richtlinien für das Filtern von ausgehenden E-Mails zu konfigurieren. Hinzu kommt eine

optionale zweite Schutzschicht beim Filtern von eingehenden E-Mails. Leistungsstarke Reporting Tools sind für ausgewählte Nutzer zugänglich und bieten zudem tiefgreifende Kontrolle von Anhängen, um regulative Compliance zu unterstützen.

Nur ein hybrider Einsatz bietet die Kosteneinsparung eines Hosted Services, der mit On-premise Richtlinienkontrollen für granulares E-Mail Content Filtering verbunden ist.

Hauptvorteile

- **Verbesserte Netzwerk- und Kosten-Effizienz**

Profitieren Sie von den Vorteilen beider Lösungen: Websense Hosted Email Security und On-premise Websense Email Security. Spam und Viren werden blockiert, bevor sie das Netzwerk erreichen. Dadurch steht mehr Bandbreite, Ressourcen und eine verbesserte Leistung zur Verfügung, während gleichzeitig gewährleistet ist, dass vertrauliche und sensible Nachrichten innerhalb des Netzwerks bleiben.

- **Minderung des Risikos und des Gefährdungspotentials mit nachgewiesenem ROI**

Websense Hosted Email Security bietet klare Schutzlevel für E-Mail und Viren. Diese gewährleisten SLA-gestützte Betriebszeit und Einsehbarkeit in entstehende Bedrohungstrends und -aktivitäten. Mit der On-premise Websense Email Security steht verschiedenartigstes, delegiertes Richtlinien- und Nutzer-basiertes Reporting mit einmaliger Einsehbarkeit in ausgehende E-Mail-Bedrohungen zur Verfügung.

- **Reduzierte TCO (Total Cost of Ownership)**

Websense Hosted Email Security verringert Bandbreitenkosten, die durch Spam verursacht wurden und es stehen mehr Zeit und System-Ressourcen zur Verfügung. Unternehmen erhalten wertvolle Hardware- und Management-Zeit zurück und können sich somit auf andere Teilbereiche der Messaging Security konzentrieren. Dazu gehört auch die Richtlinienumsetzung und Compliance für ausgehende E-Mails.

- **Reduzierte Komplexität durch eine einheitliche Lösung**

Konsolidierter E-Mail-Bedrohungsschutz, Compliance und Leak Prevention durch eine einheitliche Messaging Security-Lösung, die verschiedene Arten von E-Mail-basierten Bedrohungen am Ort ihrer Entstehung eliminiert.

Fazit

Websense Hybrid Messaging Security verbindet Websense Hosted Email Security und Websense Email Security (Einsatz am Gateway).

Durch den mehrschichtigen und kombinierten Einsatz dieser Lösungen, erhalten Unternehmen umfassenderen Schutz, als mit einer einzelnen Lösung.

Diese Kombination von Security-Kompetenz und dem Websense ThreatSeeker™-Netzwerk gewährleistet proaktiven Schutz gegen E-Mail und webbasierte Bedrohungen. Angriffe werden gestoppt, bevor sie Ihr Netzwerk erreichen. Die Websense ThreatSeeker™-Technologie bietet höchste Genauigkeit, verbunden mit der niedrigsten Anzahl an False Positives, da es gegen die heutigen zahlreichen, bösartigen Bedrohungen umfassend schützt.

Corporate Kontakte:

Websense, Inc.
 San Diego, CA USA
 tel +1 800 723 1166
 fax +1 858 458 2950
 www.websense.com

Websense UK Ltd.
 Reading, Berkshire UK
 tel +44 118 938 8600
 fax +44 118 938 8698
 www.websense.co.uk

Websense Deutschland GmbH
 München, Deutschland
 tel +49 89 5908 2357
 fax +49 89 5908 1361
 www.websense.de

Alle anderen Adressen
 www.websense.com/international

Office Lokationen:

Australien websense.com.au
 Israel websense.com

China prc.websense.com
 Italien websense.it

Frankreich websense.fr
 Japan websense.jp

Deutschland websense.de
 Niederlande websense.com

Hong Kong websense.cn
 Singapur websense.com

Indien websense.com
 Spanien websense.com.es

Irland websense.co.uk
 UAE websense.com

• Konsolidierung durch einen einzigen Anbieter ihre Vertrauens

Websense sichert Unternehmen weltweit in den Bereichen Web Security, Messaging Security und Data Security. Durch die Konsolidierung der eingehenden und ausgehenden Messaging Security durch Websense, erhalten Firmen Unterstützung von einem einzigen Ansprechpartner. Unternehmen haben zudem die Möglichkeit, ihren Schutz auch auf Websense Web und Data Security auszuweiten und erhalten dadurch Websense Essential Information Protection™ - den Schutz der essentiellen Informationen.

Anwenderszenarien

Die folgenden Beispiele zeigen, wie Unternehmen vom Einsatz einer hybriden Lösung profitieren können.

Anwenderszenario 1: Mit Hybrid Messaging Security bleiben eingehende und ausgehende Bedrohungen da, wo sie hingehören.

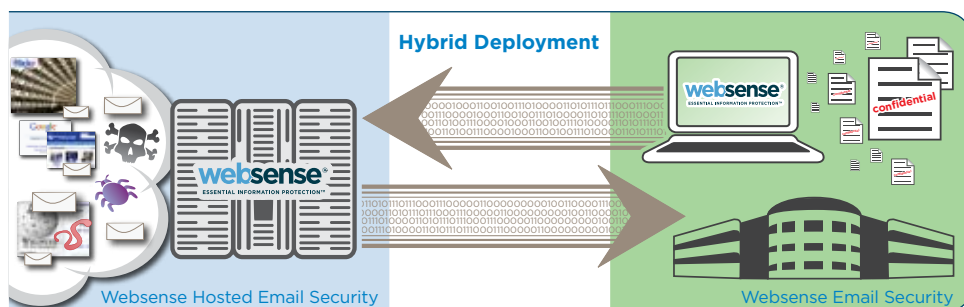
Schafft man es, bestimmte Arten von Nachrichten da zu belassen, wo sie hingehören, erhält man einen logischen Vorteil: schädliche Nachrichten sollten außerhalb, sensible und vertrauliche Nachrichten sollten innerhalb des Netzwerks bleiben. Hybrid Messaging Security hält schädliche E-Mails in Schach.

Bei diesem Szenario eliminiert Websense Hosted Email Security Viren, Malware, Würmer, Spam und andere Bedrohungen, bevor diese das Netzwerk erreichen. On-premise Websense Email Security schützt sensible Daten davor, das Netzwerk via E-Mail zu verlassen. Für viele Kunden, besonders für kleine und mittelgroße Unternehmen ist dies der erste richtige Schritt hin zur Implementierung einer umfassenden Data Leak Prevention-Lösung.

Anwenderszenario 2: Hybrid Messaging Security verbessert die Netzwerk- und Kosteneffizienz.

Websense Hosted Email Security kann ungefähr 90% des eingehenden E-Mail-Verkehrs eliminieren. Das liegt daran, dass ca. 90% aller E-Mails, Spam sind. Durch das Blockieren von Spam und Viren, bevor diese das Netzwerk erreichen, wird die Belastung dessen, was mit Websense Email Security bearbeitet werden muss, stark reduziert. Ist einmal die Masse der Spams beseitigt, kann Websense Email Security eine weitere Selektion der E-Mails durchführen, mit einem zweiten Satz von Technologien, was einen weiteren Vorteil bedeutet und sicherstellt, dass die E-Mails wirklich sauber sind.

In diesem Szenario verbessern Unternehmen die Effizienz ihrer E-Mail-Bearbeitung und erhalten einen höheren Schutz durch hybride Messaging Security.



Websense Hybrid Messaging Security verbindet Websense Hosted Email Security und Websense Email Security (Einsatz am Gateway).

Für weitere Informationen und um eine Testversion der Websense Email-Lösung zu erhalten oder um sich eine Online-Demo anzusehen, besuchen Sie www.websense.com/evaluations.