



„Durch die Kontrolle unserer E-Mails „in the cloud“ [mit Websense Hosted Email Security] werden unsere unternehmensinternen Server entlastet. Damit erübrigen sich die täglichen Verwaltungsarbeiten.“

Terry Kemp

Infrastructure Manager
Nelson Marlborough
District Health Board

Websense®

Hosted Email Security

Die heutige E-Mail-Bedrohungslandschaft wird von konvergierten E-Mail- und Web-Attacken beherrscht. Inzwischen enthalten über 85 Prozent der unerwünschten E-Mails eine eingebettete URL. Außerdem sind Unternehmen immer mehr Gefahren ausgesetzt, die mit Datenverlusten und Verstößen gegen E-Mail-Nutzungsrichtlinien zusammenhängen. Aber nur weil die E-Mail-Bedrohungen immer komplexer werden, muss das noch lange nicht für das Management der E-Mail-Security gelten.

Die als Websense® security-as-a-service (SaaS) lieferbare E-Mail-Security beinhaltet die besten Internet- und Datensicherheitstechnologien und bietet dadurch eine beispiellose Transparenz der auftretenden Bedrohungen und einen optimalen Schutz vor ein- und ausgehenden E-Mail-Security-Risiken. Dieser leicht zu verwaltende Service bietet einen sehr zuverlässigen Schutz vor Spam, Viren, Spyware, Phishing sowie konvergierten E-Mail- und Internet-Bedrohungen. Vordefinierte Content-Verzeichnisse erleichtern die Umsetzung von E-Mail-Nutzungsrichtlinien, verhindern Datenverluste und entsprechen den gesetzlichen Anforderungen.

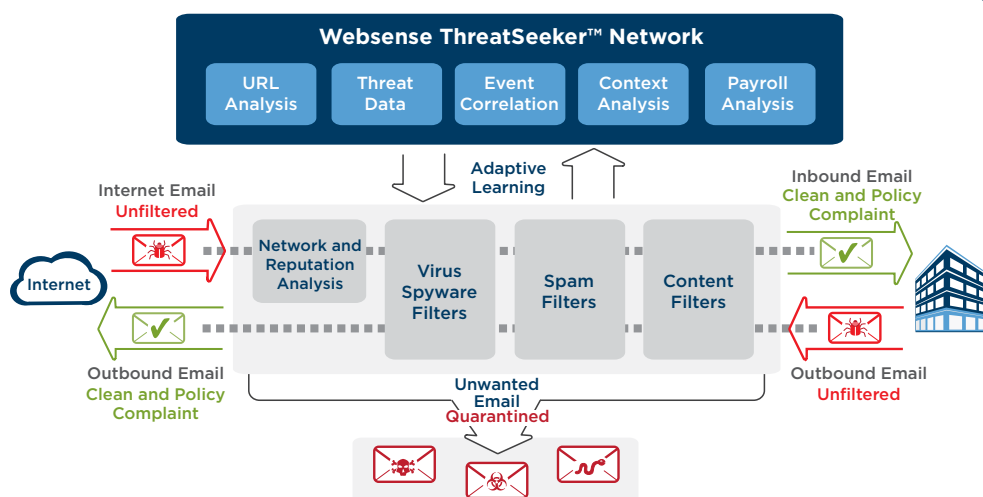
Funktionsweise:

Das Netzwerk ist durch Websense Hosted Email Security leicht zu schützen. Stellen Sie die MX-Einträge einfach auf das Websense Datacenter, dann wird jede E-Mail gefiltert, bevor sie das Netzwerk erreicht, so dass erheblich an Bandbreite und Speicherplatz gespart wird. Die Websense Datacenter verfügen über eine Lastverteilung und sind redundante, hochverfügbare Cluster, die sich

an 10 geographisch unterschiedlichen Standorten weltweit befinden. Der Service bietet eine SLA-gestützte Verfügbarkeit von 99,999 Prozent. Um das höchstmögliche Maß an globaler und lokaler Sicherheit, Datenschutz und Vertraulichkeit zu gewährleisten, ist der gehostete Service gemäß ISO 27001 zertifiziert.

Mit der SaaS E-Mail Security von Websense können Kunden:

- **Geschäftskosten und Komplexität reduzieren**, da kein Equipment vor Ort installiert oder instand gehalten werden muss, Bandbreite und Speicherplatz eingespart werden, keine unerwarteten Ausgaben anfallen und der administrative Aufwand gering ist.
- **den Schutz** vor konvergierten E-Mail- und Web-Bedrohungen dank branchenführender SLAs und der Leistungsstärke des Websense ThreatSeeker™ Network erhöhen.
- **die Kontrolle behalten** durch den Zugriff rund um die Uhr und die flexible, kundenorientierte Anpassung von Richtlinien, Konfigurationseinstellungen, Quarantäne-Management und Reporting.



Gehosteter Email-Security-Service im Überblick

„Kaum verfügten wir vor Ort über die Websense Hosted Email Security, da blieben Spams fast auf der Stelle aus.“

Lee Smith
IT Operations Manager
Harvey Nichols

Funktionen der gehosteten E-Mail-Security

Module mit gehosteter E-Mail-Security	Antispam	Antivirenprogramme	Content Filter	Verschlüsselung
Hosted Antispam	●			
Hosted Email Security	●	●		
Hosted Email Security und Content Control	●	●	●	●

Antispam

Websense bietet einen äußerst präzisen Spam-Schutz mit sehr wenigen False Positives und wird durch ein Service Level Agreement mit 99%iger Spam-Erkennung unterstützt. Bei der Identifizierung von Spam kommen verschiedene Technologien wie Absender-Reputation, adaptives Lernen, URL-Analysen, Heuristiken, digitales Fingerprinting und die optische Erkennung von Bild-Spam zum Einsatz. Sie ist die einzige Lösung, in die die marktführende Web-Security-Technologie von Websense zum Schutz vor Phishing und konvergierten E-Mail- und Web-Bedrohungen integriert ist. Jeder E-Mail wird eine Score zugeordnet, der mit einem kundendefinierten Schwellenwert verglichen wird, so dass festgelegt werden kann, welche Maßnahmen zu ergreifen sind.

Antivirenprogramme

Ein- und ausgehende E-Mails werden mit Hilfe eines vielschichtigen Ansatzes mit drei verschiedenen kommerziellen Antiviren-Engines und dem Websense Threat-Seeker Network zum Schutz vor bekannten und unbekanntem Bedrohungen auf Viren, Spyware und anderen Formen von Malware gescannt. ThreatSeeker bietet einen Zero-Hour-Schutz, indem es E-Mails und Webseiten kontinuierlich überprüft, um Trends und Muster zu ermitteln, die auftretende Bedrohungen erkennen lassen, und das Gefährdungszeitfenster zwischen einem neuen Malware-Ausbruch und der Verfügbarkeit einer Erkennungssignatur zu schließen. Dieser Service wird durch eine 100%ige SLA-Erkennung der bekannten Viren unterstützt.

Content-Filter

Durch die integrierte Technik der marktführenden Websense Data-Security-Lösungen ist es einfach, Datenverluste zu verhindern, gesetzliche Anforderungen zu erfüllen und E-Mail-Nutzungsrichtlinien umzusetzen. Mit Hilfe vordefinierter Wörterbücher, die 20 Topics in 12 Sprachen umfassen, und integrierter PCI-DSS und Datenschutzzurichtlinien können die Unternehmen Verstöße gegen E-Mail-Nutzungsrichtlinien schnell identifizieren und stoppen. Mit modernen regulären Ausdrücken und flexiblen Richtlinien sind auch sehr spezifische Kontrollanforderungen leicht zu erfüllen. Durch eine eingehende Kontrolle der E-Mail-Nachricht und des Inhalts im Attachment werden Verstöße identifiziert. Die Nachrichten können auch aufgrund des True-File-Typs des Anhangs in Quarantäne verschoben und aufgrund ihrer Größe zur späteren Auslieferung zurückgestellt werden.

Verschlüsselung

Mit der Websense-Verschlüsselung wird die E-Mail-Kommunikation geschützt, ohne dass auf die Möglichkeit verzichtet werden müsste, verschlüsselte E-Mails auf Malware und Content-Verletzungen zu überprüfen. Websense unterstützt die Server-to-Server-Verschlüsselung mit Hilfe der branchenüblichen Transport-Layer-Security (TLS) und der Ad-hoc-Park-and-Pull-Verschlüsselung für die individuelle Kommunikation. Zur Verschlüsselung der Kommunikation können je nach Absender, Empfänger, den Empfindlichkeitseinstellungen von Outlook oder einem Schlüsselwort im Betreff Verschlüsselungsrichtlinien erstellt werden. Die Verschlüsselung kann, wie gewohnt, zusammen mit dem Content-Filtering erfolgen, so dass E-Mails verschlüsselt werden, die einen spezifischen Content enthalten, wie z. B. sensible oder vertrauliche Daten.

Die Websense SaaS Email Security arbeitet auch mit der Websense SaaS Web Security Hand in Hand und sorgt damit für einen integrierten E-Mail- und Web-Schutz. Dadurch haben die Unternehmen die Möglichkeit der Konsolidierung von Management und Reporting für die Web- und die E-Mail-Security.

Funktionen	Nutzen
Spam und Virenschutz	Höchst präziser SLA-gestützter Schutz vor Spam, Viren, Spyware, Phishing und konvergierten E-Mail- und Web-Bedrohungen.
Zero-Hour-Erkennung von Bedrohungen	Dank der Schutzfunktion des ThreatSeeker Netzwerks werden neu entstehende Bedrohungen erkannt und gestoppt. Potenzielle Risiken werden dadurch ausgeschlossen.
Schutz vor Datenverlust	Die marktführenden Data-Security-Lösungen von Websense schützen dank integrierter Technologien vor Datenverlust und erleichtern die Einhaltung gesetzlicher Anforderungen.
Content-Filtering	Mit Hilfe vordefinierter Content-Verzeichnisse, die 20 Topics in 12 Sprachen umfassen, lassen sich Verstöße gegen E-Mail Richtlinien leicht identifizieren.
Verschlüsselung	Schützt sensible, regulierte Daten durch sichere E-Mail-Kommunikation mit Geschäftspartnern und Einzelpersonen
Bereitstellung als security-as-a-service	Spart Zeit und Geld, da kein Equipment installiert oder instand gehalten werden muss; integrierte Elastizität, vorhersehbare Kosten und reduzierter Administrationsaufwand.
Infrastruktur des globalen Top-Tier Data Center	Zehn Datacenter weltweit mit voll redundanter Stromversorgung, Kühlung und Internet-Konnektivität gewährleisten eine hohe Verfügbarkeit mit SLA für eine 99,999%ige Betriebszeit.
Security-Zertifizierungen	Mit Hilfe einer unabhängigen Überprüfung und Zertifizierung der Security-Praktiken gemäß ISO27001 wird der höchstmögliche Level an Sicherheit, Datenschutz und Vertraulichkeit gewährleistet
Zugriff und Support rund um die Uhr	Zugriff auf die Dienste und Management über ein Web-basiertes Portal, das jederzeit und überall im Internet verfügbar ist und Support rund um die Uhr bietet. So erhalten Sie jederzeit Hilfe, wenn Sie sie benötigen sollten.
E-Mail-Spooling für die Notfallplanung	Durch integrierte Redundanz und E-Mail-Spooling wird sichergestellt, dass E-Mails auch nach einem Ausfall des Netzwerk- oder Mailservers des Kunden nie verloren gehen.
Quarantäne-Management	Eine leistungsfähige Nachrichten-Suchmaschine sorgt für absolute Transparenz und Zugriff auf in Quarantäne verschobene Nachrichten und Logs.
Selfservice für Endanwender	Geplanter und bedarfsorientierter Zugriff zur Ansicht und Freigabe von in Quarantäne verschobenen Nachrichten; eine Whitelist/Blacklist der Absender reduziert den Verwaltungsaufwand.
Verzeichnisdienst-Integration	Automatische Synchronisierung von E-Mail-Adressen und -Gruppen mit Active Directory und LDAP erleichtert das Richtlinien-Management.
Rollenbasierte Verwaltung	Separate Zugriffskontrollen für das Quarantäne-Management, Report-Anzeige, Zugriff auf Audit-Protokoll und weitere Schlüsselfunktionen ermöglichen eine delegierte Verwaltung.
Directory-Harvest-Prevention	Durch integrierten Schutz werden Spammer daran gehindert, gültige E-Mail-Adressen zu erfassen.
Reporting	Über 40 verschiedene Report-Typen mit Zusammenfassung und detaillierter Drilldown-Forensik bietet 360-Grad-Transparenz der Bedrohungstypen und -umfänge, der bearbeiteten Mitteilungen, Richtlinienverletzungen u.a.

Websense ThreatSeeker™ Network

Die adaptive Security-Technologie des Websense ThreatSeeker Network nutzt über 50 Millionen Echtzeit-Datensammelsysteme, die auch neuen und dynamischen Internet-Content kontinuierlich überwachen und einen Zero-Hour-Schutz vor neu entstehenden Bedrohungen bieten. Diese Forschungen und Informationen fließen in Echtzeit in das Lösungsportfolio von Websense ein.

Aus diesem Grund ist Websense in der Lage, sich dem schnell verändernden Internet mit einer Geschwindigkeit anzupassen, mit der herkömmliche Sicherheitslösungen nicht Schritt halten können.

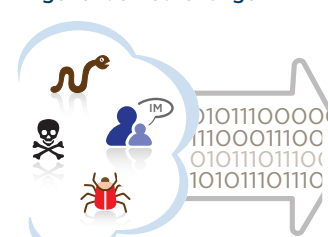
Websense, Inc.
 San Diego, CA USA
 tel 800.723.1166
 tel 858.320.8000
 www.websense.com

Websense UK, Ltd.
 Reading, Berkshire UK
 tel 0118.938.8600
 fax 0118.938.8697
 www.websense.co.uk

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

Australien websense.com.au	Italien websense.it
Brasilien websense.com/brasil	Japan websense.jp
Kolumbien websense.com/latam	Malaysia websense.com
Frankreich websense.fr	Mexiko websense.com/latam
Deutschland websense.de	China prc.websense.com
Hong Kong websense.cn	Singapur websense.com
Indien websense.com	Spanien websense.com.es
Irland websense.co.uk	Taiwan websense.cn
Israel websense.co.uk	UAE websense.com

Eingehende Bedrohungen



- Spam
- Viren
- Bösartige URLs

Integrierte Internet- und Datensicherheitsintelligenz

- | | |
|-------------------------|---|
| ✓ ThreatSeeker | ✓ Vordefinierte Wörterbücher |
| ✓ Zero-Hour-Intelligenz | ✓ Deep-Content-Kontrolle |
| ✓ URL-Analyse | ✓ Hoch entwickelte Mustererkennungsfunktion |

Ausgehende Risiken



- Datenverluste
- Nutzungsrichtlinien
- Compliance

Intelligente E-Mail-Security

Schutz der E-Mail-Privatsphäre

ISO 27001

Die Websense SaaS Email Security ist von unabhängigen Stellen gemäß der Norm ISO 27001 geprüft und zertifiziert, so dass der höchste Level an Sicherheit, Datenschutz und Vertraulichkeit sichergestellt ist. ISO 27001 ist eine im Oktober 2005 von der Internationalen Organisation für Normung veröffentlichte Norm für Informationssicherheits-Managementsysteme. Diese Zertifizierung ist der allgemein anerkannte Qualitätsnachweis für das Security-Programm eines Unternehmens und die strengste Sicherheitsnorm in der Branche: Sie geht über die Anforderungen gemäß der SAS 70-Zertifizierung hinaus, die viele Wettbewerber als Zertifizierungsmaßstab zugrunde legen.

Sicherheit der Datacenter

Zu den sichersten Stellen, zu denen Sie Ihre E-Mails routen können, zählen die Websense Datacenter. Websense hat für das Bereitstellungsnetz der Datacenter strenge Sicherheits- und Datenschutzmaßnahmen getroffen. Saubere E-Mails werden nicht abgefangen, und andere E-Mails sind nur für diejenigen sichtbar, die über Administratorenrechte für Ihr System verfügen – insbesondere Ihre Netzwerkadministratoren und diejenigen, denen Sie Zugriffsrechte auf Ihren Account erteilt haben. Die Datacenter von Websense halten darüber hinaus strenge physische Sicherheitsvorkehrungen ein, zu denen u.a. die folgenden zählen:

- an 365 Tagen im Jahr rund um die Uhr besetzt
- Systeme zur Erkennung von physischen Zugriffen
- Videoüberwachung
- Zugriffsbeschränkungslisten
- photo- und biometrische Verifizierung

Zusammenfassung des Service Level Agreement

Websense bietet branchenführende SLAs an, die einen Service auf höchstem Niveau sicherstellen.

- **Verfügbarkeit** - zu 99,999 %
- **Spam** - die Erkennungsrate beträgt 99 Prozent oder mehr
- **Viren** - 100%ige Erkennung bekannter Viren
- **Bearbeitungswartezeit** – 60 Sekunden oder weniger für Nicht-Spam-Mails unter zwei Megabyte
- **E-Mail-Logs und Quarantäne** – spätestens fünf Minuten nach Erhalt einer E-Mail verfügbar

Alle SLAs unterliegen den in der Kundendienstvereinbarung ausgeführten Bedingungen.

Weitere Informationen, ein Testversion der Websense E-Mail-Lösung sowie eine Online-Demo finden Sie unter www.websense.com/evaluations/Default.aspx?l=de.