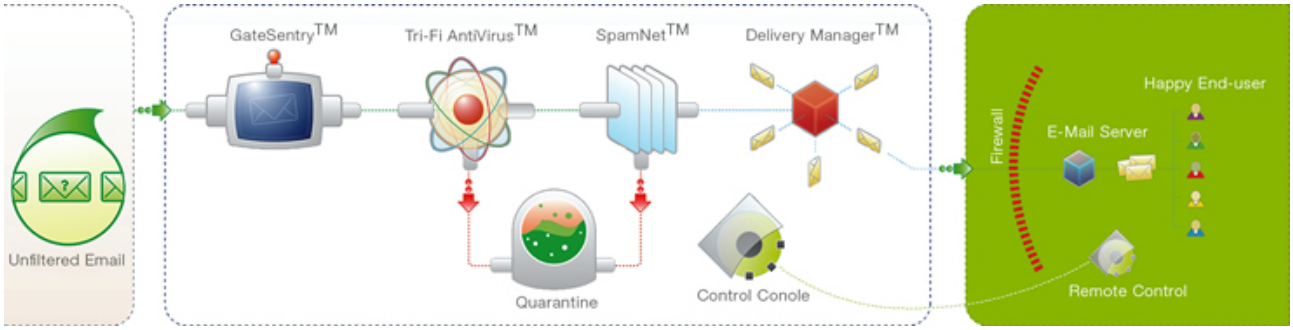
Antispam & Antivirus

Factsheet

	M	L
Features		
Schutz im Posteingang	ja	ja
Schutz im Postausgang	-	ja
Anzahl E-Mail Konten	5 – 5'000	5 – 5'000
Vertragliches		
Vertragslaufzeit	12, 24, 36 Monate	12, 24, 36 Monate
Abrechnungsperiode	3 Monate	3 Monate
Einmalige Aufschaltgebühr	CHF 270.–	CHF 270.–

Wichtiges im Überblick



GateSentry:
Der Zugang zum SpamLab wird mit höchster Sicherheit überwacht, damit unser SpamLab nicht von Attacken oder Hackern blockiert werden kann. Im Einsatz steht nur das beste Equipment, welches redundant ausgelegt ist.

Tri-Fi AntiVirus:
Die drei Virenscanner (McAfee, SOPHOS und FPROT) reinigen Ihre E-Mails von Viren, Trojanern, Würmern und anderen gefährlichen Inhalten. Die Aktualisierung der Virenscanner geschieht in Real-Time alle 10 Minuten.

SpamNet:
Der SpamNet untersucht jedes einzelne E-Mail auf diverse Spam-Eigenschaften. Unsere derzeitige Spam-Identifikation kann zusammenfassend wie folgt beschrieben werden:

- Header, Subject, Lexical, Signatures Analyse
- Multi-hop Detections
- URL Screening
- Heuristik-Methode
- Image Decoding and Detection
- Anti-Spoofing
- HTML Tag Parsing
- Campaingn Tracking Analysis
- Internal and External Block Lists

Delivery Manager:
Der Delivery Manager erhöht dank seiner Architektur die Stabilität und Verfügbarkeit des SpamLab. Die «echten» E-Mails werden nun an den Kundenserver ausgeliefert.

Quarantäne (Quarantine):
In der Quarantäne werden alle verdächtigen E-Mails aufgehalten. Somit geht kein E-Mail ungewollt verloren.

Webinterface (Control Console):
Das Webinterface dient als Login. Es können alle in der Quarantäne befindlichen E-Mails angeschaut werden, ohne gefährliche Inhalte herunter zu laden. Zusätzlich sind alle Einstellungen und Details ersichtlich und können kundenseitig angepasst werden.

So arbeitet die Antispam-Lösung

Analyse der Betreffzeile (Subject)
Viele Spam-Mails verfügen über einschlägig bekannte Betreffzeilen anhand der neuen versandte Spam-Mails gezielt gefiltert werden können.

Anti-Relay Funktion
Schutz des Mailservers, damit dieser nicht als Spam-Versender missbraucht werden kann. Damit wird eine Auflistung in den Real-Time Black-Lists verhindert.

Antispam-Datenbank
Datenbanken im Internet, welche Beispiele von bekannten Spam-Mails enthalten. Mailserver können sich mit diesen Datenbanken abgleichen und lassen E-Mails, welche sich in den Datenbanken befinden nicht zu.

Anti-Spoofing
Erkennung von Spammern, welche E-Mails offiziell von externen Domains aber zur Tarnung mit internen Absender-Adressen versenden.

Header-Analyse
Überprüfung der E-Mail-Header, um Abweichungen von festgelegten E-Mail-Standards zu ermitteln.

Heuristische Analyse
Regelbasierende Scanmethode, die bestimmte Merkmale eines E-Mails erkennt. Merkmale wie «Removelink» und bestimmte Wörter wie «VIAGRA» deuten auf Spam hin und werden «Schlecht-punkten» zugeordnet. Nach der Analyse werden die Punkte addiert und ab einem definiertem Grenzwert gilt ein E-Mail als klassifizierter Spam.

Internal Black Lists und White Lists
Liste mit Domain-Namen und Adressen, welche eindeutig gesperrt sind. White Lists sind das Gegenstück, also klare Spezifierungen von erwünschten E-Mails.

Lexikalische Textanalyse
Untersuchung nach ganzen Textstellen und Verknüpfung mittels Operatoren OR, AND, NOT, etc., beispielsweise Verkaufsangebote und die Aufforderung zum Besuch von Webseiten.

Real-Time Black-Lists (RBL)
Listen im Internet welche IP-Adressen von Mail-Server enthalten, von welchen Spam versandt wurde. Mit RBL akzeptiert der Firmenserver keine E-Mails von solchen einschlägig bekannten IP-Adressen. Es kommt aber vor, dass Mail-Server irrtümlich auf dieser Liste enthalten sind, wenn Firmenserver ungewollt zum Spam-Versand missbraucht wurden.

Schutz vor Mail-Bombing
Massive Zustellung von automatisch generierten E-Mails auf einen Mailserver (DoS, Denial of Service). Dieser Schutz reguliert den E-Mail-Fluss um eine Überlastung zu verhindern.

Unterbindung von «Directory Harvesting Attacken»
Spammer versuchen direkt über den SMTP Server an gültige E-Mail-Adresse zu kommen, dies wird unterbunden.

Vorteile der Lösung

- Kinderleichtes Installieren mittels Umleitung des Mailverkehrs (MX-Record)
- Keine eigene Antispam/Antivirus Infrastruktur notwendig
- Antispam überprüft und sortiert Ihre E-Mails
- Kein lästiges Sortieren mehr von unerwünschten E-Mails
- Spam, Viren und Trojaner bleiben in unserer Quarantäne
- Bessere Produktivität und erhöhte Sicherheit
- Eigene Infrastruktur bleibt von gefährlichen E-Mails verschont
- Keine unnötige Belastung Ihrer Infrastruktur durch unnötigen Datenverkehr