



HOSTED EMAIL ANTIVIRUS

MENING VAN ANALISTEN

MessageLabs is gepositioneerd in de 'Leader'-kwadrant in de Magic Quadrant voor E-mail Security Boundaries.

Gartner definieert 'leaders' als leveranciers die nu goed presteren, een duidelijke visie op de markttriching hebben en actief op zoek zijn naar bekwaamheden om hun leidende positie in de markt te behouden.

Gartner Magic Quadrant for E-mail Security Boundaries, door Arabella Hallawell, Peter Firstbrook

HET BIJZONDERE VAN MESSAGELABS

- 100% bescherming tegen zowel bekende als onbekende virussen
- Bevat Skeptic™-technologie, die sinds 1999 de weg heeft gebaad voor preventieve detectie.
- Biedt een uitgebreide reeks Service Level Agreements voor de dekking van antivirus, servicebeschikbaarheid, foutrespons en e-mailwachtijd
- Een unieke functie voor koppelingcontrole (het scannen van URL's in e-mails op potentiële koppelingen naar malware) biedt uw bedrijf extra bescherming

**Bron: MessageLabs Intelligence: 2008 Annual Report*

Het Magic Quadrant valt onder het copyright 2008 van Gartner, Inc. en wordt hier met toestemming gebruikt. Het Magic Quadrant is een grafische voorstelling van een marktsegment in en voor een specifieke periode. De uitkomsten zijn het resultaat van een analyse door Gartner van hoe specifieke leveranciers in hun respectievelijke markten presteren volgens criteria die door Gartner zijn opgesteld. Gartner spreekt geen voorkeur uit voor een leverancier, product of service in het Magic Quadrant, noch wordt technologiegebruikers geadviseerd alleen leveranciers te kiezen die in het leiderskwadrant staan. Het Magic Quadrant is uitsluitend bedoeld als leidraad en is geen besluitvormingsinstrument. Gartner wijst alle garanties, zowel expliciet als impliciet, in verband met dit onderzoek af, inclusief alle garanties van verkoopbaarheid of geschiktheid voor een specifiek doel.

HOE WEET U ZEKER DAT UW E-MAIL TEGEN VIRUSSEN IS BESCHERMD?

Het is wel duidelijk dat in het huidige bedrijfsleven e-mail het voornaamste communicatiemiddel is. Dit betekent dat het voor dagelijkse bedrijfsactiviteiten van essentieel belang is dat e-mail veilig en functioneel is. Ondernemingen kunnen elke dag te maken krijgen met onderbrekingen van communicatie en dagelijkse werkzaamheden, en inbreuk op intellectueel eigendom als gevolg van bedreigingen die via e-mail binnenkomen, zoals virussen, Trojaanse paarden, spyware en phishing. Zonder een effectieve verdediging kan dit leiden tot aanzienlijke hogere kosten en ernstige verliezen.

Bedeigingen via e-mail hebben zich verder ontwikkeld en omvatten meer dan alleen virussen en spam. Schrijvers van virussen, spam en spyware maken nu gebruik van elkaars methoden. Zo waren in 2008, botnets (met trojaanse paarden geïnfecteerde computernetwerken) verantwoordelijk voor circa 90% van alle spammails. Tegenwoordig bevat bijna één op de 300 e-mails malware. Sommige aanvallen zijn zo precies gericht, dat deze nooit op de antivirus-industrieradar verschijnen en niet goed worden geïdentificeerd, of door standaard, op handtekeningen gebaseerde antivirusscanners gestopt.

De Email Anti-Virus Service van MessageLabs biedt bescherming voor uw bedrijf tegen bedreigingen die via e-mail binnenkomen en een service level agreement voor 100% bescherming tegen bekende en onbekende virussen. Omdat dit het een hosted service is, vinden continu en automatisch updates plaats. Er is geen software te beheren en de kosten zijn voorspelbaar.

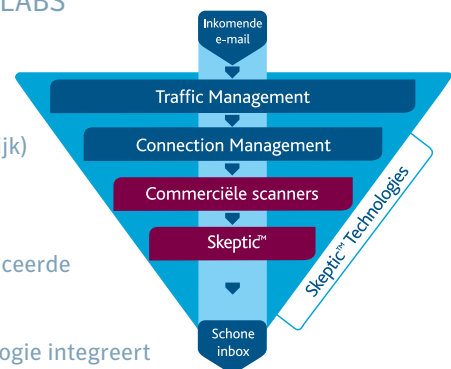
Onze architectuur bevat een combinatie van scanengines van derde partijen en onze eigen Skeptic™-technologieën voor superieure bescherming. Traffic Management vertraagt spam op TCP/IP-niveau, terwijl Connection Management gebruikmaakt van heuristische technieken om ongewenste e-mail op verbindingniveau te blokkeren en aanvallen op het niveau van gebruikersbeheer te voorkomen. Met de informatie over bedreigingen van onze services voor Web Security en IM Security kunnen wij gecombineerde bedreigingen detecteren die meerdere protocollen omvatten en hiertegen bescherming bieden. Het resultaat is meer bandbreedte, verbeterde bescherming tegen gevaren en een schonere verbinding

VERDEDIGING TEGEN MALWARE – DE GELAAGDE OPLOSSING VAN MESSAGELABS

De opties Traffic Management en Connection Management identificeren, vertragen en weigeren e-mails die (vermoedelijk) door een virus zijn geïnfecteerd.

Meerdere commerciële scanners detecteren bekende en geïdentificeerde virussen.

De preventieve Skeptic™-technologie integreert duizenden heuristische regels, slimme handtekeningen, 'fuzzy fingerprinting' en dynamische kopstekstanalyse om onbekende en nieuwe virussen te identificeren.



WERKING VAN DE SERVICE

- MessageLabs-clients verwijzen hun Mail Exchange-records (MX) door naar MessageLabs
- Inkomende en uitgaande e-mail wordt via MessageLabs geleid, waar het wordt gescand
- Skeptic™ biedt een onmisbare beveiligingslaag, waarbij nieuwe of onbekende bedreigingen worden geïdentificeerd en geblokkeerd
- E-mail met een virus wordt geblokkeerd en gedurende 30 dagen in quarantaine gehouden. De ontvanger ontvangt hiervan bericht
- De functie voor koppelingcontrole controleert alle webpagina's die in een e-mail worden vermeld, op virussen en andere gevaren. Als op die websites malware wordt aangetroffen, wordt die e-mail geblokkeerd.
- Als een verdachte koppeling inderdaad een virus blijkt te zijn, wordt een handtekening gemaakt en worden volgende e-mails die deze koppeling bevatten, behandeld als zijnde geïnfecteerd met een virus. Alle e-mails met een viruskoppeling worden in quarantaine geplaatst.

SERVICE LEVEL AGREEMENTS

- Antivirusbescherming - 100% bescherming tegen bekende en onbekende virussen
- Valse positieven bij virussen - onderschepping valse positieven van 0,0001%
- Aflevering - gegarandeerde e-mailaflevering van 100%
- Vertraging - gemiddelde retourtijd van e-mailaflevering is minder dan 60 seconden
- Beschikbaarheid van de service - 100% beschikbaar
- Technische ondersteuning/ foutrespons - gegarandeerde responstijden voor kritieke, belangrijke en minder belangrijke oproepen

DE VOLGENDE STAP

Contact met een productspecialist:
Nederland: +31 (0)20 799 7929
info@messagelabs.com



Confidence in a connected world.

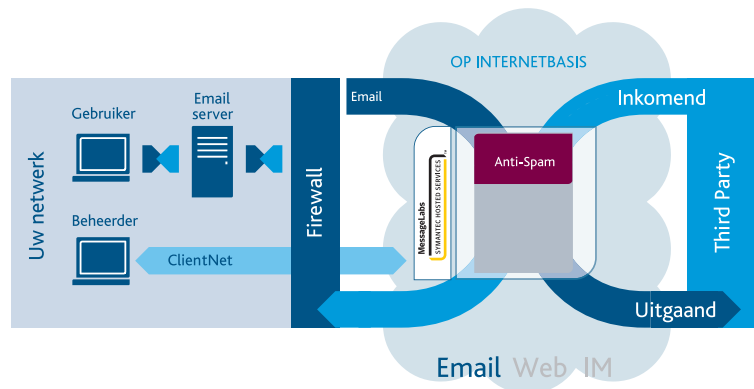
Deze service op internetsniveau combineert meerdere toonaangevende commerciële scanners met onze eigen preventieve Skeptic™-technologie, om bescherming te bieden tegen nieuwe bedreigingen voordat deze uw netwerk in gevaar kunnen brengen.

MessageLabs scant ruim 3 miljard e-mailverbindingen per week. Met de informatie die via dit venster over het wereldwijde e-mailverkeer wordt verzameld, krijgen klanten ongeëvenaarde bescherming tegen nieuwe bedreigingen.

Via de functie voor koppelingcontrole biedt de Email Anti-Virus Service ook bescherming tegen geïdentificeerde, met virussen geïnfecteerde URL-koppelingen in e-mails.

Via de globale architectuur voor databasereplicatie worden continu en automatisch updates op ons netwerk uitgevoerd. Het resultaat is uitgebreide bescherming op het moment van de verschijning van een bedreiging, nog lang voordat traditionele antivirushandtekeningen beschikbaar zijn.

MessageLabs wordt ondersteund door een uitgebreide Service Level Agreement. U krijgt uw geld terug als de volgende servicelevels niet worden gehaald: beschikbaarheid van service, valse positieven bij virussen, e-mailvertraging en onderschepping van virussen voor e-mail die via onze service loopt. Email Anti-Virus wordt 24 uur per dag in een wereldwijde infrastructuur onderhouden en biedt een veilige, flexibele en betrouwbare hosted oplossing.



FUNCTIES	VOORDELEN
Meerlaagse verdedigingstechnologieën, waarbij bedreigingen die via e-mail binnenkomen, buiten uw netwerk worden afgehandeld	Bespaart de tijd en middelen die nodig zijn voor het afhandelen van uitbraken en de gevolgen hiervan, en houdt bandbreedte in het bedrijf vrij voor het web, VoIP en andere kritieke systemen
Eigen heuristische Skeptic™-technologieën	Garandeert effectieve bescherming tegen nieuwe en ongeïdentificeerde bedreigingen
De technologie voor koppelingcontrole controleert elke URL in e-mails op bedreigingen	Biedt uitgebreide bescherming tegen samengestelde bedreigingen en technieken
Volledig instelbaar met een reeks mogelijke acties voor geïdentificeerde bedreigingen	Biedt beheerders de mogelijkheid aangepaste beleidsregels af te dwingen of te delegeren op basis van de specifieke behoeften van uw bedrijf
Agressieve Service Level Agreement	Stelt u gerust waardoor u zich kunt concentreren op het uitbreiden van uw business
Dashboard, samenvatting, gedetailleerde en geplande rapportages.	Biedt overzicht en verantwoording van, en vertrouwen in de effectiviteit van de service, met gedetailleerde rapporten over virusvolume en gestopte aanvallen.