

HOSTED WEB SECURITY

MENING VAN ANALISTEN

“Hackers en cybercriminelen geven steeds meer de voorkeur aan internet als middel voor het distribueren van malware en het plegen van identiteitsdiefstal, financiële fraude en bedrijfsspionage.”

IDC Worldwide IT Security Software, Hardware, and Services 2009–2012 Forecast and 2007 Vendor Shares: The Big Picture

HET BIJZONDERE VAN MESSAGELABS

- Geavanceerde architectuur met ongeëvenaarde bescherming en minimale vertraging
- Toonaangevend Service Level Agreement – u krijgt uw geld terug als de servicelevels niet worden gehaald
- Eén enkele beheerconsole plus informatie over bedreigingen die via e-mail, internet en expresberichten worden verstuurd, voor nog meer bescherming en controle en een nog beter overzicht
- Gratis 24/7 wereldwijde ondersteuning van SaaS-specialisten, in 10 talen

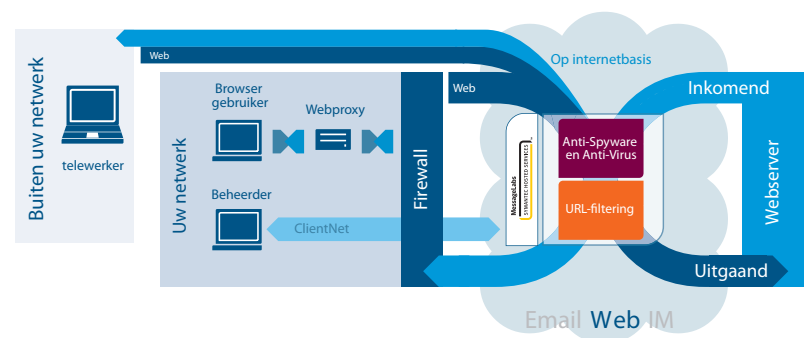
HOE BEWAAKT EN BEVEILIGT U HET WEBVERKEER IN UW ORGANISATIE?

Internet is voor bedrijven een onmisbaar hulpmiddel geworden, maar tegelijk is het surfen op internet nog nooit zo gevaarlijk geweest. Aanvallers gebruiken internet nu als de primaire methode voor het verspreiden van virussen en spyware. Gebruikers die besmette sites bezoeken, kunnen ongemerkt malware downloaden dat als doel heeft om vertrouwelijke informatie te stelen.

Organisaties beginnen zich ook te realiseren dat er beleidsregels voor aanvaardbaar internetgebruik nodig zijn om de productiviteit te maximaliseren, het gegevensverlies te beperken en de wettelijke risico's te verkleinen. De mogelijkheid om internet te misbruiken neemt toe naarmate er steeds meer gebruik wordt gemaakt van Web 2.0 en sociale mediasites.

MessageLabs Web Security blokkeert virussen, spyware en phishing via het web en bewaakt het webverkeer via URL-filtering. Op deze manier kunnen bedrijven hun beleid voor aanvaardbaar internetgebruik afdwingen. MessageLabs Web Security werkt op internetniveau en blokkeert bedreigingen voordat deze uw netwerk kunnen bereiken. De toegang tot internet kan met behulp van URL-filtering per categorie, gebruiker, tijdstip, URL of bestandstype worden geregeld. Dankzij de ondersteuning voor roamende gebruikers strekt de beveiliging en uitvoering van het beleid zich ook uit tot werknemers die buiten het bedrijfsnetwerk op internet gaan.

WEBBEVEILIGING EN CONTROLE – DE OPLOSSING VAN MESSAGELABS



MessageLabs Web Security wordt met minimale vertraging geleverd via ons wereldwijde netwerk van zeer beschikbare datacentra waarin de belasting evenwichtig wordt verdeeld. Hierdoor beschikt u over snelle en efficiënte bescherming die altijd is ingeschakeld, zonder de productiviteit van uw gebruikers te onderbreken. Onze oplossing is gemakkelijk te implementeren en te beheren en wordt ondersteund door de krachtigste SLA in de branche. Bovendien krijgt u gratis wereldwijd 24/7 ondersteuning van SaaS-specialisten (in 10 talen).

WERKING VAN DE SERVICE

- Webverkeerverzoeken worden via MessageLabs geleid en met uw beleid voor aanvaardbaar gebruik vergeleken.
- Wanneer geen beleidsregel wordt geactiveerd, wordt het verzoek doorgelaten.
- Wanneer wel een beleidsregel wordt geactiveerd, wordt het verzoek gelogd en doorgelaten of wordt de toegang tot de webpagina geweigerd.
- Verzoeken tot het openen van webpagina's worden voordat deze op uw netwerk worden afgeleverd, door MessageLabs opgevangen en op bekende en nieuwe webbedreigingen gescand.
- Nieuwe en gekoppelde malwarebedreigingen worden door Skeptic™ geïdentificeerd, terwijl bekende bedreigingen door meerdere malware-engines worden herkend.
- Wanneer een bedreiging is geïdentificeerd, wordt de toegang tot de gevraagde webpagina geweigerd.
- Wanneer geen bedreiging is geïdentificeerd, wordt de pagina zonder merkbare vertraging bij de gebruiker afgeleverd.

SERVICE LEVEL AGREEMENTS

MessageLabs Web Security wordt door de volgende SLA-niveaus ondersteund:

- Antivirusbescherming op internet - 100% bescherming tegen bekende virussen
- Vertraging - Gemiddelde scantijd van webcontent duurt hoogstens 100 milliseconden
- Beschikbaarheid van de service - 100% beschikbaar
- Technische ondersteuning - responstijden voor kritieke, belangrijke en minder belangrijke oproepen

DE VOLGENDE STAP

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

Voor andere vestigingen en telefoonnummers gaat u naar:
www.messagelabs.nl/contact



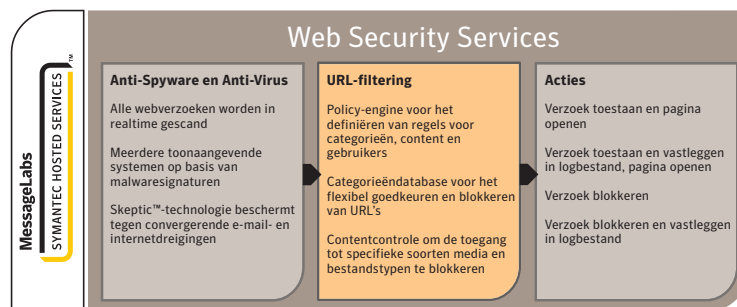
Confidence in a connected world.

MessageLabs Web Security bestaat uit twee kernonderdelen:

Meerlaagse beveiliging – meerdere commerciële antispyware- en antivirusescannen webinhoud op malware. Deze engines worden voortdurend door MessageLabs bijgewerkt, wat een nauwkeurige detectie van bekende bedreigingen garandeert. Bovendien beschermt de heuristische Skeptic™-technologie van MessageLabs tegen nieuwe en gekoppelde bedreigingen, die zich via andere protocollen, zoals e-mail en expresberichten, op webgebruikers kunnen richten.

URL-filtering - alle webverzoeken worden met een geavanceerde beleid-engine en database voor URL-categorisatie vergeleken om te zorgen dat geschikte content toegankelijk blijft, terwijl ongeschikte content nauwkeurig in de gaten wordt gehouden. De beleid-engine is zeer flexibel en intuïtief, waardoor organisaties voor specifieke gebruikers en groepen beleidsregels kunnen opzetten en gedrag kunnen bewaken.

MessageLabs heeft een enkele, geïntegreerde beheerconsole voor e-mail, internet en expresberichten. Deze zorgt voor eenvoudiger beheer en minder totale eigendomskosten, terwijl meer inzicht wordt geboden op het gedrag van gebruikers. Informatie over bedreigingen wordt over verschillende communicatieprotocollen gedeeld voor betere bescherming.



FUNCTIES	VOORDELEN
Meerlaagse verdediging tegen virussen en spyware op internetsniveau.	Blokkeert virussen en spyware voordat deze uw netwerk kunnen bereiken.
Eigen heuristische Skeptic™-technologie met gridverwerking.	Beschermt tegen nieuwe en gekoppelde malwarebedreigingen die via e-mail, internet en expresberichten lopen.
Wereldwijd verspreide architectuur met minimale vertraging.	Biedt de mogelijkheid zonder merkbare vertragingen veilig te surfen.
Gedetailleerd instelbare engine voor beleidsopzet met URL-filtering.	Stelt ondernemingen in staat internetmisbruik te voorkomen door de toegang tot ongepaste sites en content te beperken.
Ondersteuning voor roamende gebruikers	Uitvoering van regels voor bescherming en beleid ook toe te passen op werknemers buiten het bedrijfsnetwerk.
Cachefiltering van zoekengine.	Identificeert de oorsprong van gecacheerde content en past de juiste controleregels toe.
Dashboard, samenvatting, gedetailleerde en geplande rapportages.	Biedt overzicht en verantwoording van, en vertrouwen in de effectiviteit van de service.
Enkele beheerconsole voor de beveiliging van e-mail, internet en expresberichten.	Vereenvoudigt het beheer maar biedt tegelijk uitgebreide mogelijkheden voor bescherming, controle en overzicht.