

# Symantec MessageLabs Web Security.cloud

## Mening Van Analisten

“Malware heeft alleen al via websurfen met succes bijna twee derde van de bedrijfsnetwerken geïnfiltrerd.”

*Osterman Research, Messaging and Web Security Market Trends 2010-2013, augustus 2010*

## Het Voordeel Van De Symantec.cloud services zijn

- Informatie over bedreigingen verzameld uit e-mail-, internet- en expresberichtprotocollen voor een nog hogere nauwkeurigheid
- Globale infrastructuur is redundant en voorzien van belastingverspreiding voor hoge beschikbaarheid
- Agressieve Service Level Agreement
- Enkele beheerconsole voor e-mail-, internet- en expresberichtsenservices voor meer overzicht en controle
- Gratis 24/7 wereldwijde ondersteuning in 10 talen van SaaS-specialisten

## Service Level Agreement

U krijgt bij Web Security.cloud een Service Level Agreement met een geld-terug-garantie of andere verhaalsmogelijkheden als niet aan de volgende performance levels wordt voldaan:

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

## De Steeds Grotere Uitdaging Van Veilig En Productief Internetgebruik

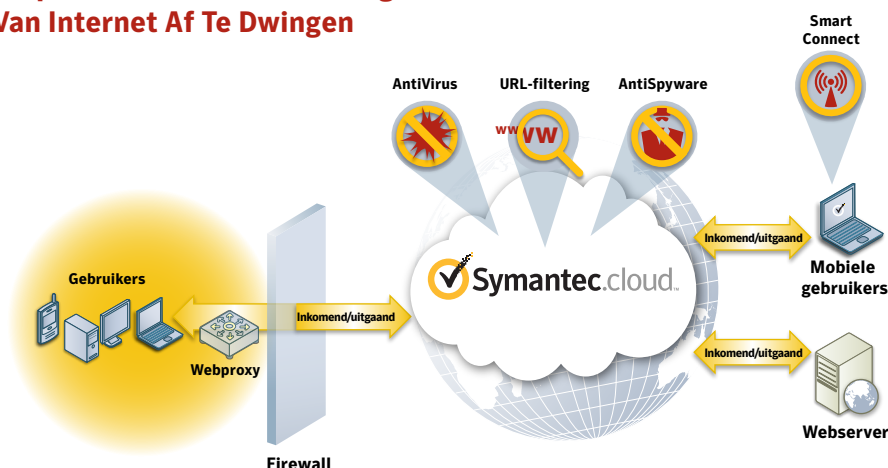
Internet is voor bedrijven een onmisbaar hulpmiddel geworden, maar tegelijk is het surfen op internet nog nooit zo gevaarlijk geweest. Aanvallers gebruiken internet nu als primaire methode voor het verspreiden van virussen en spyware. Gebruikers die besmette sites bezoeken, kunnen ongemerkt malware downloaden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

Ook andere factoren van internetgebruik en -toegang door werknemers kunnen bedrijven aan risico's blootstellen. De toenemende populariteit van sociale netwerken en micro-blogsites kan leiden tot malwarerisico's en misbruik van internet door werknemers. Organisaties beginnen zich te realiseren dat er beleidsregels voor aanvaardbaar internetgebruik nodig zijn om de productiviteit te maximaliseren, gegevensverlies te beperken en wettelijke risico's te verkleinen. En naarmate werknemers vanaf steeds meer locaties op internet gaan, moeten bedrijven erop toezien dat interacties veilig zijn en dat externe en mobiele gebruikers internet op de juiste manier gebruiken.

IT-afdelingen moeten bepalen hoe medewerkers veilig en productief het internet voor hun werk kunnen gebruiken, zonder dat het IT-personeel wordt belast en de werking van het netwerk nadelig wordt beïnvloed.

Web Security.cloud, helpt u uw organisatie tegen internetbedreigingen te beschermen en biedt u de mogelijkheid beleidsregels voor aanvaardbaar internetgebruik te bepalen, ten uitvoer te brengen en te bewaken. Anti-malwarelagen voorkomen dat bedreigingen uw netwerk kunnen binnendringen, terwijl beleid voor URL-filtering en quota voor webverkeer misbruik van internet helpt voorkomen. Bovendien kunt u zo zorgen dat uw bedrijf voldoende bandbreedte houdt.

## Helpt Uw Webverkeer Beveiligen En Een Juist Gebruik Van Internet Af Te Dwingen



Web Security.cloud wordt via ons wereldwijde netwerk van zeer beschikbare en uitgebalanceerde datacentra geleverd. Hierdoor beschikt u over snelle en efficiënte bescherming die altijd aan staat, zonder de productiviteit van uw gebruikers in gevaar te brengen.

Er zijn ook opties voor mobiele en externe gebruikers beschikbaar, zodat u al uw medewerkers kunt beschermen.

## Werking Van De Service

- Webverkeerverzoeken worden via Symantec.cloud geleid en vergeleken met uw beleid voor aanvaardbaar gebruik
- 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 door Symantec opgepikt voordat deze op uw netwerk worden afgeleverd 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

## Over Symantec.cloud

Symantec.cloud's werelds toonaangevende leverancier van hosted services voor het beveiligen en beheren van e-mail, internet en expresberichten (of communicaties).

Meer dan 30.000 organisaties en meer dan 9 miljoen eindgebruikers in 99 landen maken gebruik van Symantec.cloud voor de bescherming tegen virussen, spam, phishing, onjuist internetgebruik, spionage en andere bedreigingen die schadelijk zijn voor bedrijven.

## Volgende stappen

Neem contact op met een productspecialist:  
Nederland: +31 (0) 307670700  
Cloud\_Info@Symantec.com  
www.symanteccloud.com

## Uw Internetbeveiliging Naar De Cloud Brengen

Web Security.cloud helpt u uw webverkeer op internetniveau te beschermen met gebruikmaking van:

**Uitgebreide verdedigingsmechanismen** – Meerdere commerciële en bedrijfseigen antispyspionage- en antivirusengines scannen internetcontent op malware voordat dit op uw netwerk wordt afgeleverd. De commerciële engines worden constant door Symantec.cloud bijgewerkt, waardoor u verzekerd bent van een nauwkeurige detectie van bekende bedreigingen en uw personeel minder wordt belast met onderhoud en beheer. Onze eigen heuristische Skeptic™-technologie verdedigt tegen de allernieuwste bedreigingen.

Zodra uit een protocol nieuwe informatie is verzameld, deelt Skeptic dit automatisch met alle andere protocollen. Hierdoor kunnen wij bedreigingen vinden die van meerdere leveringsmethode gebruikmaken.

**URL-filtering en internetbeleidsengine** - Alle webverzoeken worden met een geavanceerde beleidsengine en database voor URL-categorisatie vergeleken om te zorgen dat geschikte content toegankelijk blijft, terwijl ongeschikte content nauwkeurig in de gaten wordt gehouden. De beleidsengine geeft beheerders de mogelijkheid om aangepaste regels voor bepaalde gebruikers, groepen, tijdsperiodes of niveaus van bandbreedteverbruik in te stellen. Om de configuratie van de service voor u gemakkelijker te maken is onze URL-filtering al voorzien van standaardregels voor best practices die veel geblokkeerde websitecategorieën omvatten.

**Voorspelbare kosten en vereenvoudigd beheer:** wordt geleverd op basis van een abonnement, waardoor geen hoge aanschafkosten nodig zijn en de kosten betaalbaar en voorspelbaar blijven. De eenvoudig in te stellen en gebruiksvriendelijke service kan doeltreffend via een centrale console op het web worden beheerd. Upgrades vinden automatisch plaats. U krijgt er 24/7 wereldwijde technische ondersteuning bij om zo de administratieve werklast te verlagen en de productiviteit van uw personeel te verhogen.

Functie	Voordelen
<b>Beveiliging op alle niveaus</b>	<ul style="list-style-type: none"><li>• De voorspellende technologieën van Skeptic™, gecombineerd met meerdere commerciële scanners, helpen uw organisatie tegen zero-hour en bekende internetbedreigingen beschermen door deze van uw netwerk vandaan te leiden</li></ul>
<b>URL-filtering en uitvoering van internetbeleid</b>	<ul style="list-style-type: none"><li>• Biedt u de mogelijkheid beleid voor aanvaardbaar internetgebruik op te stellen en ten uitvoer te brengen, met regels op basis van websitecategorieën, contenttypen en het maximaal aantal webverzoeken per gebruiker.</li><li>• Helpt de bandbreedte en productiviteit van een bedrijf te beschermen door downloads van bepaalde bestandstypen te blokkeren of te beperken en tijds- en volumebeperkingen op het gebruik van internet op te leggen.</li></ul>
<b>Minimale latentie</b>	<ul style="list-style-type: none"><li>• Een scan van webcontent vindt gemiddeld binnen 100 milliseconden plaats en wordt ondersteund door een SLA, waarin de verwachtingen wat betreft prestaties zijn vastgelegd en zo meer vertrouwen biedt.</li><li>• De wereldwijd verspreide, redundante en schaalbare architectuur biedt eindgebruikers een consistente en veilige browse-ervaring en beperkt vertragingen tot een minimum.</li></ul>
<b>Uitgebreide rapportage</b>	<ul style="list-style-type: none"><li>• Het dashboard, samenvattingen en de gedetailleerde en geplande rapportage bieden overzicht, verantwoording en vertrouwen in de effectiviteit van de service</li></ul>
<b>Ondersteuning voor mobiele en externe medewerkers</b>	<ul style="list-style-type: none"><li>• Biedt opties voor de uitvoering van beleidsregels en het beschermen van gebruikers die buiten het bedrijfsnetwerk op internet gaan</li></ul>