

Symantec MessageLabs Instant Messaging Security.cloud

Wat analisten ervan zeggen

“De zorgen over archivering en regelgeving nemen toe nu de hoeveelheid IM-gegevens in gereguleerde bedrijfstakken steeds verder toeneemt. Er moeten beleidsregels voor beheer worden opgesteld, zodat werknemers weten wat hun verantwoordelijkheden zijn met betrekking tot IM.”

Gartner MarketScope for Enterprise Instant Messaging and Presence, door David Mario Smith, 5 juli 2011

Symantec.cloud - Het verschil

- Een unieke cloudservice voor de beveiliging, de controle en het beheer van UC- en IM-beveiliging, met gebruikmaking van bewezen technologie en expertise.
- Bevat de eigen, maatgevende Skeptic™-technologie voor de bescherming tegen nieuwe, opkomende en samengestelde bedreigingen.
- Maximale functionaliteit gecombineerd met minimale onderhoudsvereisten.
- Een toonaangevende klantenondersteuning die wereldwijd 24 uur per dag, 7 dagen per week voor u klaar staat.
- Een intuïtieve mogelijkheid voor het opzetten van beleid is onderdeel van de service.
- Lage totale eigendomskosten vergeleken met interne oplossingen op basis van software of hardware.

Kunt u de voordelen van UC en IM gebruiken en de gevaren ervan vermijden?

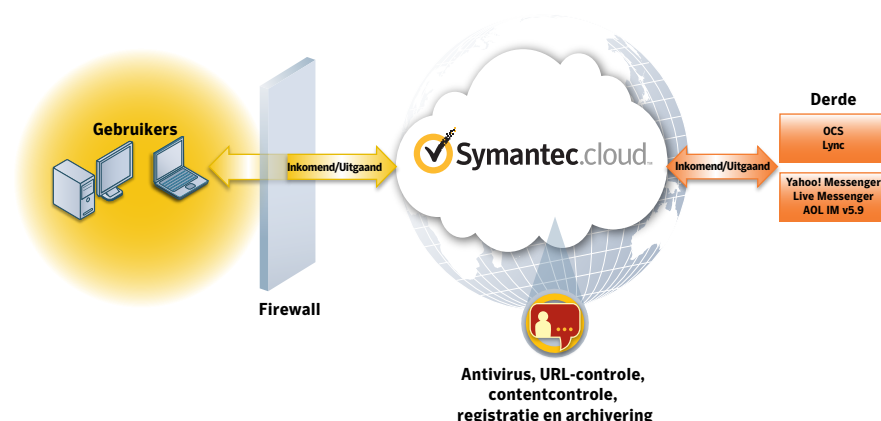
Omdat Unified Communications (UC) en IM (Instant Messaging) directer zijn dan e-mail en veelzijdiger dan de telefoon, kan het de snelheid, het gemak en de efficiency van zakelijke communicatie aanzienlijk verbeteren. Door deze voordelen is het bedrijfsleven UC gaan gebruiken, terwijl het gebruik van openbaar IM, en vooral het ongecontroleerde gebruik ervan, snel groeit, wat overeenkomt met de wereldwijde trend op dit gebied.

Ongecontroleerd gebruik van UC en openbare IM-netwerken stelt u bloot aan risico's die de productiviteit, winstgevendheid, bedrijfscontinuïteit en het klantvertrouwen in gevaar kunnen brengen. Hierbij gaat het niet alleen om potentiële ontwrichting als gevolg van malware die via UC en IM wordt verspreid. Ook onbedoelde of opzettelijke gegevenslekkage en oneigenlijk en onrechtmatig gebruik zijn gevaren waarmee zeker rekening moet worden gehouden.

Instant Messaging Security.cloud (IMS.cloud) kan uw werknemers helpen UC- en openbare IM-netwerken veilig te gebruiken. Door de functionaliteit voor bescherming en beheer kunt u volledig en met meer vertrouwen profiteren van de interne en externe realtimecommunicatie via compatibele UC- en openbare IM-systemen, en de werkdruk van uw IT-team verlichten.

IMS.cloud helpt de kosten, complexiteit en beperkingen van interne oplossingen in de vorm van software en hardware te vermijden. Bovendien biedt het bewezen mogelijkheden om te voldoen aan de urgente behoefte van het moderne bedrijfsleven aan een veiliger, beter beheersbaar en controleerbaar gebruik van UC en openbaar IM.

UC en IM als aanwinst, niet als risico



Deze volledig beheerde en volledig aanpasbare service biedt een uitgebreide reeks kosteneffectieve en geavanceerde functies, waaronder antimalware, detectie van schadelijke URL's, contentcontrole, berichtregistratie, archivering en rapportage. IMS.cloud is snel en handig op te zetten en kan via een gebruikersvriendelijke webportal worden toegepast.

Hoe de service werkt

- Elk UC- of IM-bericht naar of afkomstig van uw organisatie wordt door onze infrastructuur geleid.
- Inkomende berichten (inclusief tekstbestanden of andere bijlagen) worden onmiddellijk en uitgebreid gescand op:
 - virussen, wormen, Trojaanse paarden en andere malware,
 - URL's die u opzettelijk naar geïnfecteerde websites proberen te leiden.
- Alle inkomende en uitgaande berichten worden eerste gecontroleerd op basis van uw beleid voor contentcontrole en aanvaardbaar gebruik van UC en IM.
- Berichten die schadelijk of verdacht zijn, of de beleidsregels schenden, worden automatisch geblokkeerd.
- Alle andere berichten gaan zonder merkbare vertraging naar de beoogde ontvanger.
- Elk bericht wordt veilig in een logbestand in onze beveiligde infrastructuur geregistreerd.

De Symantec.cloud-ervaring

- **IM-gebruikers:** De Symantec.cloud-service veroorzaakt geen merkbare vertraging in de aflevering van UC- en IM-berichten en heeft geen nadelige invloed op de functionaliteit
- **IT-beheerders:** IMS.cloud biedt volledige controle over (en volledig inzicht in) het gebruik van UC en IM in uw bedrijf. De service werkt ook naadloos samen met onze beveiligings-, controle- en archiveringservices voor e-mail- en webverkeer
- **Servicebeheerders:** IMS.cloud is eenvoudig te beheren via één webportal en voorziet in uitgebreide functionaliteit voor het genereren van rapporten

Volgende stappen

Neem contact op met een productspecialist:
Nederland: +31 (0) 307670700
cloud_info@symantec.com

Het fundamenteel flexibele, veelzijdige en aanpasbare IMS.cloud dicht huidige of potentiële UC- en IM-beveiligingsgaten in de kern van uw bedrijf en beschermt daarmee uw reputatie en bedrijfsdoelstellingen.

IMS.cloud draait op ons bewezen, ondernemingsgerichte, wereldwijde webbeveiligingsplatform. Al uw inkomende en uitgaande UC- en IM-berichten (inclusief bijlagen) worden door een ultramoderne en uitgebalanceerde infrastructuur geleid, die de best mogelijk beveiliging en controle mogelijkheden biedt. U kunt ook heel eenvoudig firewallregels toevoegen die voorkomen dat uw medewerkers de service kunnen ontwijken.

Berichten en bijlagen met malware worden door onze scantorens geblokkeerd nog voordat ze zelfs maar de grens van het netwerk van de beoogde ontvangers bereiken. Een belangrijke rol hierin is weggelegd voor Skeptic™, onze unieke voorspellingstechnologie die van elk IM-bericht, elke e-mail en webpagina die het scant, leert en zo constant zijn ongeëvenaarde detectiemogelijkheden verder uitbreidt.

Wanneer een bericht een link naar een geïnfecteerde of ongeschikte website lijkt te bevatten, of als er trefwoorden of uitdrukkingen in zijn opgenomen die u in uw controleregels opgeeft, wordt het bericht automatisch geblokkeerd. Hierdoor kunt u uw netwerk tegen infectie beschermen en uw medewerkers afschermen van ongeschikt materiaal dat van buiten uw organisatie afkomstig is. Bovendien bent u beschermd tegen onbedoelde of opzettelijke gegevenslekage en tegen ongewenst gebruik van UC en IM door uw medewerkers.

Alle UC- en IM-berichten worden in een logbestand vastgelegd, waarmee u een middel in handen hebt om te voldoen aan de wettelijke vereisten ten aanzien van de opvraagbaarheid van gegevens en naleving van relevante voorschriften te bewerkstelligen. Voor degenen die te maken hebben met een nog strakkere regelgeving, is een optionele cloudservice voor archivering beschikbaar met geavanceerde functies voor e-Discovery.

Functie	Voordelen
Werkt met Microsoft OCS and Lync evenals met AIM van AOL, Yahoo! Mail en Microsoft Live Messenger	Biedt veiliger en gecontroleerd gebruik van toonaangevende UC- en openbare IM-netwerken
Biedt bescherming tegen bekende, nieuwe en samengestelde bedreigingen die via UC- en openbare IM-netwerken worden verspreid	Dicht beveiligingsgaten in uw bedrijfsnetwerk door te voorkomen dat malware via UC- en IM-berichten kan binnenkomen
Bevat intuïtieve functionaliteit voor het opzetten van beleid, inclusief het stapelen van meerdere regels	Maakt het snel opzetten van beleid voor aanvaardbaar gebruik van UC en IM op groepsniveau of per gebruiker mogelijk
Kan volledig worden geïntegreerd met directory's die aan LDAP voldoen	Zorgt dat groepsgegevens altijd up-to-date zijn waardoor er minder beheertaken zijn
Bevat instelbare/aanpasbare regels en meldingen	Voldoet aan uw specifieke behoeften zonder nadelige gevolgen voor de gebruikerservaring
Geen hardware op locatie nodig, en slechts een minimum aan software	Eenvoudig in te stellen, te gebruiken en toe te passen
Omvat een dashboard, samenvatting en gedetailleerde rapportage	Biedt overzicht en verantwoording van, en vertrouwen in de effectiviteit van de service