

Symantec MessageLabs Instant Messaging Security.cloud

Analystenstimme

"Mit zunehmender Menge an Instant Messaging-Daten in regulierten Branchen wächst auch die Sorge um Archivierung und Compliance... Unternehmensinterne Richtlinien sollten erstellt werden, damit sich Mitarbeiter ihrer Verantwortung bei der Nutzung von Instant Messaging bewusst sind."

Gartner MarketScope for Enterprise Instant Messaging and Presence von David Mario Smith, 5. Juli 2011

Symantec.cloud – der Unterschied

- Einzigartiger Cloud-basierter Service für die Sicherheit, Kontrolle und Verwaltung von Unified Communications und Instant Messaging mit zuverlässigen Technologien und nachweislichem Expertenwissen.
- Implementierung der von Symantec.cloud entwickelten Skeptic™-Technologie mit mehrschichtigem Schutz vor neuen, künftigen und konvergierenden Bedrohungen.
- Maximale Funktionalität kombiniert mit minimalem Wartungsaufwand.
- Erstklassiger Kundensupport – weltweit rund um die Uhr verfügbar.
- Intuitive Funktion zur Richtlinienerstellung als integrierter Service.
- Niedrige Gesamtbetriebskosten im Vergleich zu internen Software-/Appliance-Lösungen.

Wie können Sie die Vorteile von Unified Communications und Instant Messaging nutzen – und die damit verbundenen Risiken vermeiden?

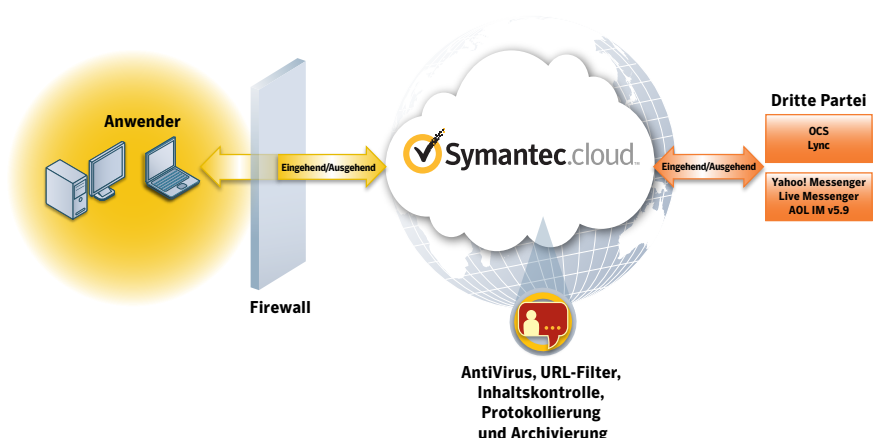
Unified Communications und Instant Messaging sind unmittelbarer als E-Mail und vielseitiger nutzbar als das Telefon. Die Kommunikation in Unternehmen wird damit deutlich schneller, bequemer und effizienter. Aufgrund der zahlreichen Vorteile hat sich Unified Communications als Kommunikationsmittel in Unternehmen fest etabliert, während die Nutzung öffentlicher Instant Messaging-Netzwerke – und insbesondere die unkontrollierte Nutzung – rapide zunimmt.

Die unkontrollierte Nutzung von Unified Communications- und öffentlichen Instant Messaging-Netzwerken setzt Unternehmen Risiken aus, die die Produktivität, Rentabilität und Business Continuity sowie das Kundenvertrauen gefährden können. Dabei geht es nicht nur um potenzielle Störungen durch Unified Communications- und Instant Messaging-Malware. Versehentliche oder vorsätzliche Datenlecks, eine unsachgemäße Nutzung und die Nichteinhaltung gesetzlicher Richtlinien sind weitere ernst zu nehmende Gefahren.

Instant Messaging Security.cloud (IMS.cloud) trägt dazu bei, dass Mitarbeiter Unified Communications- und öffentliche Instant Messaging-Netzwerke sicher nutzen können. Die integrierten Schutz- und Kontrollfunktionen ermöglichen eine optimale Nutzung der Geschäftskommunikation in Echtzeit. Damit werden kompatible Unified Communications- und öffentliche Instant Messaging-Netzwerke sicherer, mit minimalem Aufwand für IT-Teams.

IMS.cloud nutzt bewährte Funktionen, um den dringenden Bedarf von Unternehmen nach einer sichereren, besser kontrollierten und nachprüfbarer Nutzung von Unified Communications öffentlichem Instant Messaging zu decken. Unternehmen vermeiden so die Kosten, Komplexität und Einschränkungen, die mit unternehmensinternen Software- oder Appliance-Lösungen verbunden sind.

Unified Communications und Instant Messaging – Vorteile nutzen und Risiken ausschalten



Dieser komplett verwaltete und anpassbare Service ist eine umfassende und kostengünstige Paketlösung mit innovativen Technologien zum Schutz vor Malware und zur Erkennung bössartiger URLs sowie für die Nachrichtenprotokollierung, Archivierung und Berichterstattung. Die Einrichtung und Bedienung von IMS.cloud ist mit minimalem Aufwand verbunden und äußerst bequem. Die Verwaltung erfolgt über ein benutzerfreundliches Web-Portal.

Wie funktioniert der Service?

- Alle Unified Communications- oder Instant Messaging-Nachrichten, die an ein Unternehmen gesendet werden oder aus dem Unternehmen stammen, fließen durch die Symantec.cloud-Infrastruktur.
- Eingehende Nachrichten (einschließlich Textdateien oder andere Anhänge) werden umgehend und gründlich gescannt. Gesucht wird nach:
 - Viren, Würmern, Trojanern und anderer Malware
 - Bösartige URL-Links, die zu infizierten Websites führen
- Eingehende und ausgehende Nachrichten werden mit den für die Content-Kontrolle sowie Unified Communications- und Instant Messaging-Nutzungsregeln festgelegten Richtlinien abgeglichen
- Nachrichten, die bösartig oder verdächtig sind bzw. gegen die aufgestellten Richtlinien verstoßen, werden automatisch blockiert
- Alle anderen Nachrichten werden praktisch ohne Verzögerung an den angegebenen Empfänger weitergeleitet.
- Jede Nachricht kann sicher in unserer abgesicherten Infrastruktur protokolliert werden.

Der Symantec.cloud-Service in der Praxis

- **Instant Messaging-Benutzer:** Der Symantec.cloud-Service verursacht keine merklichen Verzögerungen bei der Zustellung von Unified Communications- und Instant Messaging-Nachrichten; die Nutzung wird nicht beeinträchtigt.
- **IT-Manager:** IMS.cloud ermöglicht die vollständige Kontrolle (und genaue Kenntnis) über die unternehmensweite Unified Communications- und Instant Messaging-Nutzung. Der Service lässt sich zudem nahtlos mit den E-Mail- und Internetsicherheitsservices sowie den Kontroll- und Archivierungsservices von Symantec.cloud kombinieren.
- **Serviceadministratoren:** IMS.cloud lässt sich problemlos über ein gemeinsames Web-Portal verwalten. Zudem kann eine große Auswahl an Berichten erstellt werden.

Nächste Schritte

Sprechen Sie mit einem Produktspezialisten:
DACH: +49 800 66 47 453
cloud_info@symantec.com
www.symanteccloud.com

Mit dieser flexiblen, vielseitigen und anpassbaren Lösung sind Unternehmen in der Lage, aktuelle oder potenzielle Unified Communications- und Instant Messaging-Sicherheitslücken in ihrem Unternehmensumfeld zu schließen. So bewahren sie ihren Ruf und Geschäftserfolg.

IMS.cloud ist dank der globalen und permanent geschützten Symantec.cloud-Infrastruktur ein zuverlässiges Kommunikations-Tool. Sämtliche eingehenden, ausgehenden und internen Unified Communications und Instant Messages (einschließlich Anhänge) werden über eine hochmoderne Infrastruktur mit Lastverteilung weitergeleitet, die ein Höchstmaß an Sicherheit und Kontrolle ermöglicht. Firewall-Regeln lassen sich problemlos hinzufügen. Mitarbeiter werden so daran gehindert, den Service zu umgehen.

Nachrichten bzw. Anhänge, die ein Schadprogramm enthalten, werden von unseren Scansystemen blockiert, bevor sie überhaupt den Netzwerkperimeter des angegebenen Empfängers erreichen. Die von MessageLabs entwickelte Prognosetechnologie Skeptic™ spielt dabei eine entscheidende Rolle. Die Technologie lernt mit jeder gescannten Instant Messaging-Nachricht, E-Mail oder Webseite und verbessert so fortlaufend ihre einzigartigen Erkennungsfähigkeiten.

Nachrichten, die einen verdächtigen Link zu einer infizierten oder ungeeigneten Website bzw. Schlüsselwörter oder Ausdrücke enthalten, die in den Regeln für die Content-Kontrolle definiert sind, werden automatisch blockiert. Unternehmen können damit ihr Netzwerk vor Infektionen schützen sowie versehentliche oder vorsätzliche Datenlecks verhindern. Zudem lässt sich so vermeiden, dass Mitarbeiter ungeeignetes Material aus externen Quellen in das Unternehmen einbringen sowie Unified Communications und Instant Messaging unsachgemäß nutzen.

Sämtliche Unified Communications und Instant Messages werden aufgezeichnet. Ein wichtiger Aspekt, um Anforderungen an die rechtliche Offenlegung zu erfüllen und die Einhaltung relevanter gesetzlicher Regelungen zu gewährleisten. Für Unternehmen mit sehr hohen Compliance-Anforderungen steht ein optionaler Cloud-basierter Archivierungsservice mit fortschrittlichen E-Discovery-Funktionen zur Verfügung.

Funktionen	Vorteile
Unterstützt Microsoft OCS und Lync sowie AOL AIM, Yahoo! Mail und Microsoft Live Messenger	Ermöglicht die sicherere und kontrollierte Nutzung von marktführenden Unified Communications- und öffentlichen Instant Messaging-Netzwerken
Bietet Schutz vor einer Vielzahl von bekannten, neuen und konvergierenden Bedrohungen, die über Unified Communications- und öffentliche Instant Messaging-Netzwerke verbreitet werden	Beendet eine Sicherheitsproblem im Unternehmensnetzwerk, indem es das Eindringen von Schadprogrammen über Unified Communications und Instant Messaging verhindert
Integriert eine intuitive Funktion zur Erstellung von Richtlinien, einschließlich der Stapelverarbeitung mehrerer Regeln	Ermöglicht ein schnelles Erstellen von Nutzungsregeln für die Unified Communications- und Instant Messaging-Nutzung – sowohl für Benutzergruppen als auch für einzelne Benutzer
Vollständige Integration mit LDAP-kompatiblen Verzeichnissen	Sorgt dafür, dass Gruppendaten immer auf dem neuesten Stand sind – und reduziert so den Zeit- und Arbeitsaufwand von Administratoren
Enthält konfigurierbare/anpassbare Regeln und Benachrichtigungen	Stellt sicher, dass spezielle Anforderungen Unternehmen aller Art erfüllt werden, ohne dass der Benutzerkomfort beeinträchtigt wird
Keine Hardware vor Ort und überschaubare Software	Einfache Einrichtung, Verwendung und Verwaltung
Enthält Dashboard-, Übersichts- und Detailberichte	Bietet eine bessere Übersicht und Kontrolle über die Effektivität des Service.