

Symantec MessageLabs Enterprise Instant Messenger.cloud

Analystenstimme

“Unternehmen, die bisher auf Instant Messaging verzichteten, sollten sich mit dem Geschäftsszenario für EIM vertraut machen. Es zeigt, dass Instant Messaging die Kommunikation in Unternehmen verbessern kann, da ein Unternehmen mithilfe von Instant Messaging flexibler und schneller reagieren kann.”

“Allerdings müssen auch Sicherheitsrisiken berücksichtigt werden, da Instant Messaging ähnlich wie E-Mail anfällig für Malware, Viren und SPIM ist.”

Instant Messaging: The Real Value of Real-Time Communication, Burton Group, April 2009.

Symantec.cloud - Der Unterschied

- Kosteneffizienter Service, der eine schnelle und effektive Geschäftskommunikation ermöglicht
- Erstellt ein sicheres, nicht-öffentliches Netzwerk, das Mitarbeiter, Partner und Kunden über TLS verschlüsselte Kommunikation miteinander verbindet
- Ermöglicht Instant Messaging-Benutzern die Kommunikation und den Datenaustausch in Echtzeit bei vollständiger Sicherheit und umfassendem Datenschutz
- Integration mit ausgewählten öffentlichen Instant Messaging-Services
- Für Endbenutzer intuitiv und leicht zu bedienen und für IT-Administratoren über ein anwenderfreundliches, webbasiertes Verwaltungs- und Berichts-Tool schnell anpassbar

Ist die Nutzung von Instant Messaging in Ihrem Unternehmen sicher?

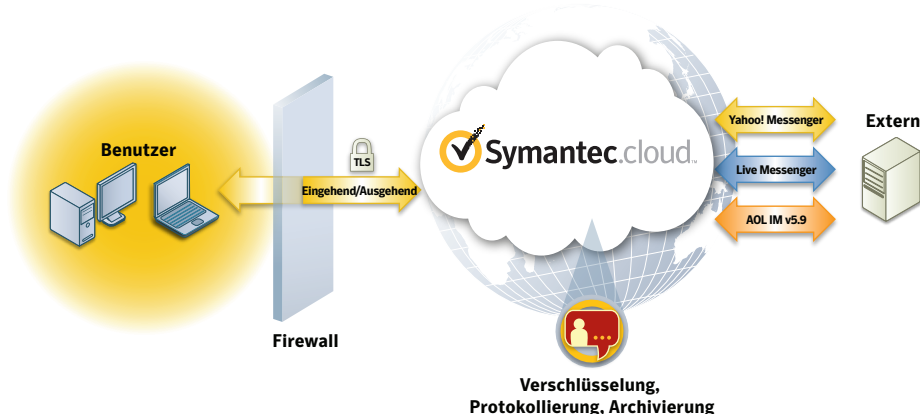
Instant Messaging ist eine benutzerfreundliche Alternative zu E-Mail. Dank seiner Geschwindigkeit und Unmittelbarkeit vereinfacht es die Echtzeitkommunikation sowie die Zusammenarbeit und die gemeinsame Nutzung von Informationen. Diese Vorteile schlagen sich in größerer Effizienz und Produktivität nieder.

Doch gerade weil es so unmittelbar und informell ist, kann Instant Messaging auch eine Quelle für potenziell ernsthafte Risiken sein. Umsatz- und imageschädigende Viren, Würmer und Trojaner sowie SPIM (Spam über IM) können über öffentliche Instant Messaging-Netzwerke wie AOL, Windows Live Messenger und Yahoo! leicht in Ihr Unternehmen eindringen. Bei unkontrollierter Nutzung besteht zudem ein erhebliches Risiko der Preisgabe vertraulicher Daten und die Gefahr von Verstößen gegen geltende Vorschriften wie beispielsweise zur Aufzeichnung und Aufbewahrung von Instant Messaging-Protokollen. Trotz der Sicherheitsrisiken haben bisher nur wenige Unternehmen Maßnahmen für einen adäquaten Schutz getroffen.

Der Enterprise Instant Messenger.cloud (EIM.cloud) Service ermöglicht es Unternehmen, die Vorteile des Instant Messaging zu nutzen und gleichzeitig die Risiken zu begrenzen. EIM.cloud schafft ein sicheres, nicht-öffentliches Instant Messaging-Netzwerk für die Kommunikation und Zusammenarbeit zwischen unternehmensinternen Mitarbeitern, mobilen Mitarbeitern und Geschäftspartnern. Ergänzt wird dieser Service durch Verwaltungs- und Überwachungsfunktionen sowie eine umfassende Nachrichtenprotokollierung.

Der Service lässt sich leicht einrichten und bedienen, ist vollständig mit ausgewählten öffentlichen Instant Messaging-Netzwerken kompatibel und über jeden internetfähigen PC zugänglich. Durch die sichere Verschlüsselung des Kommunikationsaustausches zwischen Benutzern bietet der Service ein hohes Maß an Sicherheit und schafft Vertrauen in die Instant Messaging-Plattform.

Sichere und produktive Nutzung von Instant Messaging



Wie funktioniert der Service

- Auf den Desktops von Benutzern wird ein sicherer EIM-Unternehmensclient (Professional Online Desktop – POD) installiert.
- Autorisierte Benutzer haben Zugang zu einem sicheren, privaten Instant Messaging-Netzwerk mit TLS-verschlüsselten Tunneln.
- Alle über das Netzwerk ausgetauschten Nachrichten und Dateianhänge sind vollständig verschlüsselt und können nicht abgefangen oder manipuliert werden.
- Alle über das Netzwerk ausgetauschten Dateianhänge werden auf Viren, Würmer, Trojaner und andere Malware gescannt.
- Administratoren können den Service über ein umfangreiches Berichts-Tool, das über ein anwenderfreundliches, webbasiertes Portal zur Verfügung steht, überwachen.

Unternehmensführung

- Mit dem Symantec.cloud EIM Service können Unternehmen die Gefahren vermeiden, die entstehen, wenn Mitarbeiter – meist ohne Beteiligung der IT-Abteilung – öffentliche Instant Messaging-Anwendungen installieren und verwenden.
- Der Service ermöglicht Unternehmen die Verwaltung und Überwachung der Instant Messaging-Nutzung auf der Unternehmensebene. Unternehmen können so Best Practices-Richtlinien zur Instant Messaging-Nutzung definieren und durchsetzen.
- Da der Zugang nur auf autorisierte Benutzer beschränkt ist, können ehemalige Mitarbeiter nicht mehr auf das Netzwerk zugreifen. Die dadurch verursachten Risiken werden so vermieden.

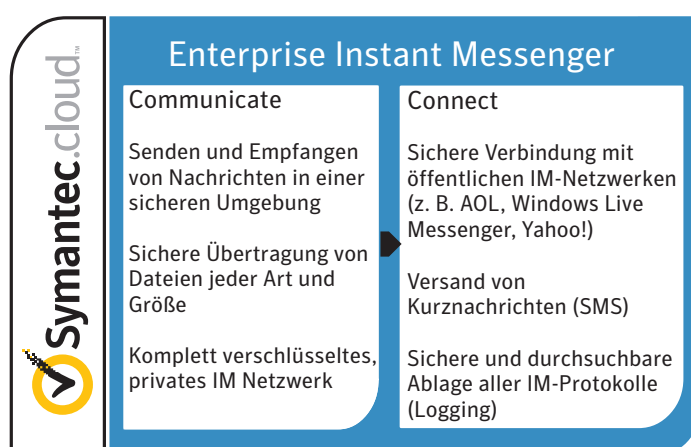
Der nächste Schritt

Sprechen Sie mit einem Produktspezialisten:
DACH: +49 800 66 47 453
info@messagelabs.com
www.messagelabs.com

Mit dem Symantec.cloud EIM Service erhalten Unternehmen eine bewährte und äußerst zuverlässige Möglichkeit, die Instant Messaging-Nutzung zu verwalten und zu optimieren. Für den Service stehen zwei Pakete zur Auswahl:

EIM Communicate – Mit Symantec.cloud POD (Professional Online Desktop), einem Online-Desktop, können Benutzer Mitteilungen auf sichere Weise senden und empfangen, Instant Messaging-Sitzungen speichern und durchsuchen sowie Mitteilungen und Dateien gleichzeitig austauschen. Mit EIM File Sharing können Benutzer Dateien jeder Art und Größe übertragen, unabhängig davon, ob der Empfänger online oder offline ist.

EIM Connect – Enthält zusätzlich zu den Leistungen von EIM Communicate die folgenden Services: Mit EIM Interoperate können Benutzer eine sichere Verbindung mit den großen öffentlichen Instant Messaging-Netzwerken herstellen und einen Puffer gegen Viren, Würmer, Trojaner und andere Bedrohungen erstellen. Mit EIM Logging werden Protokolle aller Instant Messaging-Gespräche an einem zentralen Ort gespeichert. Mit EIM SMS können Benutzer Kurznachrichten (SMS) direkt von ihrer POD-Benutzeroberfläche aus senden.



Funktion	Vorteil
Weltweit von jedem Standort mit einem internetverbundenen PC aus zugänglich	Ermöglicht die Unternehmenskommunikation in Echtzeit und erleichtert damit effektive Entscheidungs- und Handlungsprozesse
TLS-verschlüsselte Instant Messaging-Kommunikation zwischen befugten Netzwerkbenutzern	Steigert die Sicherheit vertraulicher Informationen und schafft Vertrauen bei Partnern und Kunden
Besserer Schutz vor Viren, SPIM und anderen über Instant Messaging übertragenen Bedrohungen und Verhinderung ihrer Ausbreitung durch die Sperrung von Buddy-Listen	Minimiert durch Instant Messaging-Bedrohungen verursachte Störungen und senkt die Kosten ihrer Erkennung und Beseitigung
Robustes, flexibles System, das sich durch eine einfache Installation und intuitive Bedienung auszeichnet und praktisch wartungsfrei ist	Vermeidet unnötige Investitionen in die Infrastruktur und mindert die Belastung des internen IT-Supports
Zentrale Speicherung und Protokollierung, plus detailliertes Berichtssystem mit schnellem Zugriff auf Instant Messaging-Gesprächsprotokolle sowie Aktivitäts- und Nutzungsberichte	Gewährleistet die Einhaltung gesetzlicher Vorschriften, beispielsweise dadurch, dass Instant Messaging-Protokolle für eine rechtliche Offenlegung jederzeit schnell abgerufen werden können
Alle Dateifreigabetransaktionen finden auf dem zentralen Server statt	Verringert die Anforderungen an die interne Bandbreite
Umfassendes Verwaltungs-Tool ermöglicht die Verwaltung von Domänenstrukturen und Benutzern über eine webbasierte Konsole	Ermöglicht die unternehmensweite Instant Messaging-Verwaltung durch Kontrolle von Kontakten und Funktionsrechten