

# HOSTED INSTANT MESSAGING SECURITY

## ANALYSTENSTIMME

“Instant Messaging hat sich in Geschäftsumgebungen wie Call Centern oder in denen der Zeitfaktor eine wichtige Rolle spielt, als effektives Tools für die schnelle Informationsübermittlung und Problemlösung erwiesen.”

Gartner MarketScope für Instant Messaging, 2007

“Es gibt einen Markt für benutzerfreundliche Instant Messaging-Sicherheitslösungen.”

Osterman Research, Presence, IM and Real Time Communication Trends, 2007-2010, 2007

## DER MESSAGELABS-UNTERSCHIED

- Einzigartiger und umfassender Service für die Sicherheit, Kontrolle und Verwaltung von Instant Messaging mit zuverlässigen Technologien und nachweislichem Expertenwissen.
- Implementierung der von MessageLabs 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.

## KÖNNEN SIE DIE VORTEILE VON INSTANT MESSAGING NUTZEN – UND DOCH DIE RISIKEN VERMEIDEN?

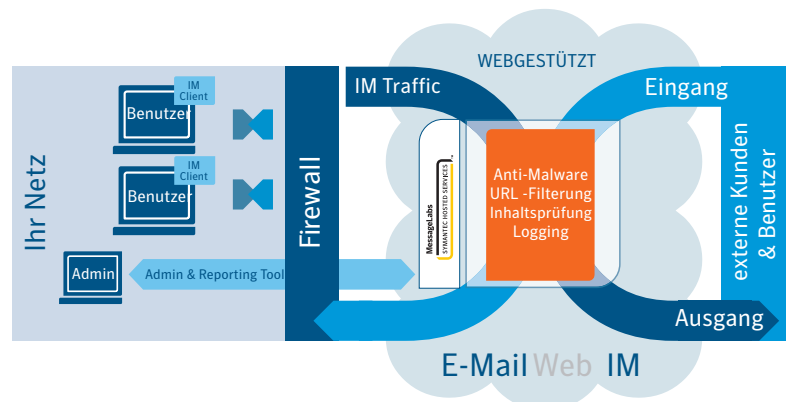
Instant Messaging ist unmittelbarer als E-Mail und vielseitiger nutzbar als das Telefon. Die Kommunikation in Unternehmen wird damit deutlich schneller, bequemer und effizienter. Aufgrund der zahlreichen Vorteile hat sich Instant Messaging zu einem der weltweit am schnellsten wachsenden Kommunikationsmittel im Internet entwickelt – mit voraussichtlich über 1 Milliarde Nutzern in 2009. Dieser weltweite Trend macht auch vor Unternehmen nicht halt. Die Instant Messaging-Nutzung in Unternehmen – und insbesondere die unkontrollierte Nutzung – nimmt rapide zu.

Die unkontrollierte Nutzung von öffentlichen Instant Messaging-Netzwerken – ob befugt oder unbefugt – 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 Instant Messaging-Schadprogramme. Versehentliche oder vorsätzliche Datenlecks, eine unsachgemäße Nutzung und die Nichteinhaltung gesetzlicher Richtlinien sind weitere ernst zu nehmende Gefahren.

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

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

## INSTANT MESSAGING – VORTEILE NUTZEN UND RISIKEN AUSSCHALTEN MESSAGELABS INSTANT MESSAGING SECURITY SOLUTION



Dieser komplett verwaltete und anpassbare Service bietet Unternehmen eine umfassende und kostengünstige Paketlösung mit innovativen Technologien zum Schutz vor Malware sowie für URL-Filterung, Inhaltskontrolle, Nachrichtenprotokollierung und Berichterstattung. Die Einrichtung und Bedienung von IMSS ist mit minimalem Aufwand verbunden und äußerst bequem. Die Verwaltung erfolgt über ein benutzerfreundliches Web-Portal.

## WIE FUNKTIONIERT DER SERVICE?

- Alle Instant Messages, die an ein Unternehmen gesendet werden oder aus dem Unternehmen stammen, fließen durch die MessageLabs-Infrastruktur.
- Eingehende Nachrichten (einschließlich Textdateien oder andere Anhänge) werden umgehend und gründlich gescannt. Gesucht wird nach:
  - Bekannten und unbekanntem Viren, Würmern, Trojanern und anderen Schadprogrammen.
  - Web-Links zu Websites, die mit Schadprogrammen infiziert sind.
- Eingehende und ausgehende Nachrichten werden mit den für die Content-Kontrolle 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 in den Instant Messaging-Posteingang des angegebenen Empfängers weitergeleitet.
- Jede Nachricht wird sicher in unserer abgesicherten Infrastruktur protokolliert.

## DER MESSAGELABS-SERVICE IN DER PRAXIS

- Instant Messaging-Benutzer: Der MessageLabs-Service verursacht praktisch keine merklichen Verzögerungen bei der Zustellung von Instant Messages; die Instant Messaging-Nutzung wird nicht beeinträchtigt.
- IT-Manager: IMSS ermöglicht die vollständige Kontrolle (und genaue Kenntnis) über die unternehmensweite Instant Messaging-Nutzung. Der Service lässt sich zudem nahtlos mit den E-Mail-/Web Security-Services und Instant Messaging- Unternehmensservices von MessageLabs integrieren.
- Serviceadministratoren: IMSS lässt sich problemlos über ein gemeinsames Web-Portal verwalten. Eine große Auswahl an Berichten kann direkt über ClientNet erstellt werden.

## DER NÄCHSTE SCHRITT

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



Confidence in a connected world.

Unternehmen erhalten mit IMSS eine unkomplizierte Lösung, die Instant Messaging-Bedrohungen und -Risiken deutlich reduziert. Unabhängig davon, woher sie stammen und in welcher Form sie auftreten. Eine der Hauptstärken des Service besteht darin, die wachsende Flut konvergierender Bedrohungen effektiv abzuwehren. Diese neuartige Form von Bedrohungen kombiniert Techniken zur Verbreitung von Schadprogrammen auf Instant Messaging-, E-Mail- und Internetprotokollplattformen.

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

IMSS ist dank der globalen und permanent geschützten MessageLabs-Infrastruktur ein zuverlässiges Kommunikations-Tool. Sämtliche eingehenden, ausgehenden und internen 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 oder Anhänge, die einen verdächtigen Link zu einer infizierten oder ungeeigneten Website bzw. Schlüsselworte oder Ausdrücke enthalten, die in den Regeln für die Inhaltskontrolle 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 und Instant Messaging unsachgemäß nutzen.

Sämtliche Instant Messages werden aufgezeichnet und können an eine im Unternehmen bereits vorhandene Archivierungslösung weitergeleitet werden. Dies trägt dazu bei, dass sich sämtliche öffentlichen Instant Messaging-Kommunikationen nachverfolgen lassen. Ein wichtiger Aspekt, um Anforderungen an die rechtliche Offenlegung zu erfüllen und die Einhaltung relevanter gesetzlicher Regelungen zu gewährleisten.

FUNKTIONEN	VORTEILE
Unterstützt AOL AIM, Yahoo! Mail und Microsoft MSN.	Ermöglicht eine sicherere und besser kontrollierte Nutzung von marktführenden öffentlichen Instant Messaging-Netzwerken.
Bietet mehrschichtigen Schutz vor bekannten, neuen und konvergierenden Bedrohungen, die über öffentliche Instant Messaging-Netzwerke verbreitet werden.	Schließt eine Sicherheitslücke im Unternehmensnetzwerk, indem es das Eindringen von Schadprogrammen über Instant Messaging verhindert.
Integriert eine intuitive Funktion zur Erstellung von Richtlinien, einschließlich der Stapelverarbeitung mehrerer Regeln.	Ermöglicht ein schnelles Erstellen von Nutzungsregeln für die 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 spezifische Unternehmensanforderungen erfüllt werden können, ohne dass der Benutzerkomfort beeinträchtigt wird.
Macht das Herunterladen eines Agenten oder einer Software in das Unternehmensnetzwerk überflüssig.	Einfache Einrichtung, Verwendung und Verwaltung.
Enthält Dashboard-, Übersichts- und Detailberichte.	Bietet eine bessere Übersicht und Kontrolle über die Effektivität des Service.