

HOSTED INSTANT MESSAGING SECURITY

ANALYTIKERS SYNSPUNKT

“IM har vist sin berettigelse i erhvervslivet i bl.a. call centers eller steder, hvor tid er afgørende, hvor det er et meget effektivt værktøj til hurtig udbredelse af data og hurtig problemløsning”

Gartner MarketScope for Instant Messaging, 2007

“Der er et vedvarende marked for en brugervenlig, offentlig IM-sikkerhedsløsning”.

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

HVAD GØR MESSAGELABS ANDERLEDES?

- Unik, omfattende IM-sikkerheds-, kontrol og administrationstjeneste, udnytter gennemtestet teknologi og ekspertise.
- Opsætning af patenteret Skeptic™-teknologi, giver beskyttelse på benchmark-niveau mod nye, kommende og konvergerede trusler.
- Maksimal funktionalitet kombineret med minimalt behov for vedligeholdelse.
- Markedets førende kundesupport, der er til rådighed i hele verden 24/7.
- Intuitiv, politikopbyggende funktion integreret i tjenesten.
- Lave samlede omkostninger (TCO) sammenlignet med interne løsninger baseret på software eller anordninger.

KAN DU UDNYTTE FORDELENE VED IM - MEN UNDGÅ FARERNE?

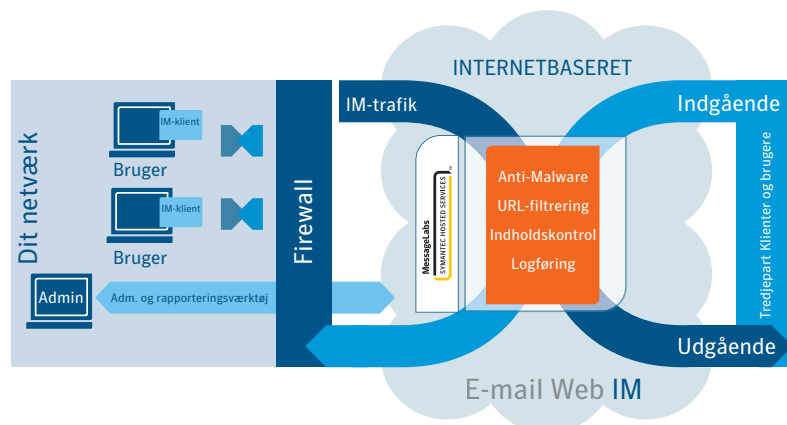
Onlinemeddelelser (IM (Instant Messaging)), der er hurtigere end e-mail og mere alsidige end telefonen, kan få kommunikationen i virksomheder til at køre hurtigere, lettere og mere effektivt. De mange fordele har været med til at gøre IM til et af verdens hurtigst voksende internetmedier, hvor det samlede antal brugere forventes at nå over 1 milliard i 2009. I erhvervslivet er brug - og specielt kontrolleret brug - af IM i kraftig vækst, hvilket sker parallelt med den globale udvikling.

Hvad enten det er autoriseret eller uautoriseret brug af offentlige IM-netværk, udgør det risici for dig, der kan kompromittere produktivitet, overskud, virksomhedens stabilitet og kundernes tillid. Det er ikke kun et spørgsmål om potentielt sammenbrud på grund af IM-båren malware. Utilsigtet eller bevidst data-lækage, upassende brug eller manglende overholdelse af krav er også yderst reelle farer.

MessageLabs' sikkerhedstjeneste til onlinemeddelelser (IMSS) kan hjælpe dine medarbejdere med at bruge offentlige IM-netværk sikkert og trygt. Dens funktioner til beskyttelse og kontrol giver dig mulighed for at udnytte intern og ekstern kommunikation i realtid maksimalt via kompatibel, offentlig IM med øget tryghed og mindre belastning af dit it-team.

Hjælper dig med at undgå omkostninger, kompleksitet og begrænsninger ved interne løsninger baseret på software eller hardware, styrker IMSS's påviselige evner til at opfylde de påtrængende behov virksomheder står overfor i dag for en sikrere, mere kontrolleret og reviderbar brug af offentlig IM.

ONLINEMEDDELELSER SOM ET AKTIV, IKKE EN BELASTNING - MESSAGELABS' SIKKERHEDSLØSNING TIL ONLINEMEDDELELSER (IMSS)



Denne fuldt hostede tjeneste, der helt kan tilpasses, giver en omfattende, omkostningseffektiv pakke af førende funktioner, inkl. anti-malware, URL-filtrering, indholdskontrol, meddelelseslogbog og rapportering. IMSS, der er hurtig og nem at sætte op og bruge, er desuden nem at administrere via en brugervenlig webportal.

IMSS minimerer ganske enkelt IM-relaterede trusler og risici uanset deres kilde eller natur. En primær styrke er tjenestens evne til effektivt at håndtere flodbølgen af konvergerede trusler, der overfører malware-udbredelsesteknikker til IM, e-mail og webprotokoller.

HVORDAN TJENESTEN FUNGERER

- Hver onlinemeddelelse sendt til eller der kommer fra din virksomhed, sendes gennem vores infrastruktur.
- Indgående meddelelser (inkl. alle tekstfiler eller andre vedhæftede filer) bliver straks og omhyggeligt scannet for:
 - kendte og ukendte vira, orme, trojanere og anden malware
 - weblinks, der fører til websteder, der er inficeret med malware
- Alle ind- og udgående meddelelser sammenholdes med din indholdskontrol og godkendte politikker for brug af IM.
- Meddelelser, der er skadelige, mistænkelige eller overtræder dine politikker, bliver automatisk blokeret.
- Alle andre meddelelser fortsætter til modtagerens IM-indbakke uden mærkbar forsinkelse.
- Alle meddelelser logges i vores sikre infrastruktur.

MESSAGELABS' TJENESTER I PRAKSIS

- IM-brugere: MessageLabs' tjeneste vil ikke medføre nogen mærkbar forsinkelse i levering af IM'er eller forstyrrelser i IM-funktioner
- It-chefer: IMSS giver fuld kontrol over (og forståelse af) IM-brug på tværs af din virksomhed; tjenesten kører desuden uproblematisk sammen med vores e-mail-/websikkerheds og IM-tjenester til virksomheder.
- Administratorer af tjenesten: IMSS administreres nemt via en enkelt webportal; via Client Net kan der genereres en omfattende række rapporter

NÆSTE TRIN

Kontakt en produktspecialist:
Danmark: +45 3332 3718
info@messagelabs.com

Gå ind på www.messagelabs.dk/contact for at se kontorer og kontaktnumre i andre lande



Confidence in a connected world.

IMSS, der grundlæggende er fleksibel, alsidig og anvendelig til mange formål, sætter en prop i det nuværende eller potentielle IM-sikkerhedshul i din virksomheds kerne ved at beskytte dit omdømme og din bundlinje.

IMSS kører på vores gennemtestede, globale websikkerhedsplatform til store virksomheder. Hver af dine indgående, udgående og interne onlinemeddelelser (inkl. vedhæftede filer) sendes gennem en avanceret, belastningsafbalanceret infrastruktur, der yder den bedst mulige sikkerhed og kontrol. Det er også enkelt at introducere firewall-regler, der forhindrer dine medarbejdere i at omgå denne tjeneste.

Enhver meddelelse/vedhæftet fil, der indeholder malware, blokeres af vores scannere, før den overhovedet når den ydre grænse for den tiltænkte modtagers netværk. En central rolle spilles af Skeptic™, der er vores unikke forudsigelsesteknologi, der lærer af hver IM, e-mail og webside, den scanner og hele tiden styrker sin suveræne evne til at opdage trusler.

Enhver meddelelse/vedhæftet fil, som mistænkes for at indeholde et link til et inficeret eller upassende websted, eller som indeholder nøgleord eller udtryk, som du har angivet i dine regler for indholdskontrol, blokeres automatisk. Det hjælper med at beskytte dit netværk mod infektioner, skærmer dine medarbejdere mod upassende materiale, der stammer udefra og beskytter dig både mod utilsigtet eller bevidst datalækage og mod dine medarbejders upassende brug af IM.

Alle onlinemeddelelser logges og kan sendes til din eksisterende arkivløsning for at hjælpe med at spore al din offentlige IM-kommunikation, så du overholder alle juridiske krav til genfindning og overholder andre krav og regler.

FUNKTIONER	FORDELE
Fungerer med AOL's AIM, Yahoo! Mail og Microsoft MSN.	Giver sikrere, kontrolleret brug af markedets førende, offentlige IM-netværk.
Yder multilagdelte beskyttelse mod kendte, nye og konvergerede trusler, der spredes via offentlige IM-netværk.	Lukker et sikkerhedshul i din virksomheds netværk og forhindrer malware i at komme ind via IM.
Har indbygget, intuitiv politikopbyggende funktion, inkl. stabling af forskellige regler.	Muliggør hurtig skabelse af en godkendt brugerpolitik for IM-brug på gruppe-niveau eller for individuelle brugere.
Fuldt integreret med adressebøger, der overholder LDAP.	Sikrer, at grupperes data altid er opdateret, hvilket sparer administrator tid/ressourcer.
Inkorporerer konfigurerbare/tilpasningsvenlige regler og meddelelser.	Sikrer, at dine særlige behov kan opfyldes, uden at det går ud over brugeroplevelsen.
Kræver ikke download af en agent eller software til dit netværk.	Nem at sætte op, bruge og administrere.
Inkluderer instrumentpanel, oversigt og detaljeret rapportering.	Giver gennemsikuelighed, ansvarlighed og tillid til tjenestens effektivitet.