

FaceTime Delivers IM Security, Productivity for Fortune 100 Communications Company

CASE STUDY



BACKGROUND

- 90,000 user organization with 20 facilities in 18 countries

CHALLENGE

- Guarantee security against malware infections entering the organization through public IM channels

RESULTS

- Higher employee productivity and morale through risk-free usage of public and enterprise IM networks
- Spyware visibility and prevention - 20,000 spyware infections detected in the first 80 minutes of deployment
- Simple solution to deploy and manage – 55,000 users protected in the first three months

“From initial evaluation to laboratory tests to deployment, this was a collaborative effort. We were extremely impressed with the FaceTime team’s desire to understand our needs and deliver a solution that enables our users around the world to make productive use of instant messaging without impacting corporate security.”

IT Manager, Global Communications Corporation

FaceTime customer since July 2005

Overview

Instant Messaging (IM) usage in business, whether sanctioned or not, is growing rapidly, especially in fast-moving global enterprises; FaceTime Security Labs report an increase in IM use in excess of 2000% in 2005 over 2004. While there’s no doubt that its use can be a significant productivity boost, IM also opens up unsecured channels into the organization, and so the hacking community has wasted no time in exploiting this growth.

IM, particularly the ‘public’ IM applications such as MSN, Yahoo!, and AOL, can create major risks to network security and integrity because they fly below the radar of traditional corporate security measures. They expose vulnerabilities that can become vectors for malware distribution, allow monitored information leakage, and breach privacy legislation compliance. A disturbing new trend being recorded by FaceTime Security Labs researchers is the propagation via IM of worms that carry a rootkit as a payload. These worms automatically send themselves to buddy lists and chat room participants, downloading the rootkit to each infected PC. The rootkit then attempts to shut down conventional security applications and opens up a back door on the PC to attack and infect the entire network.

Traditional security measures simply are not broad enough to manage IM vulnerabilities, and have the potential to cause additional problems through false alarms, resource-intensive scanning, and incomplete cleansing.

Challenge

For one global communications giant, the unprotected use of IM had been causing major security and productivity problems. While the company was using Microsoft Exchange 2000 as its officially sanctioned and monitored internal enterprise IM system, individual employees across the corporation were also using MSN and other unmonitored public IM clients. Whenever a worm infected someone’s public IM client, the infection almost immediately hopped over to the enterprise IM system and from there spread throughout the Exchange network. While corporate policy did not sanction the use of public IM networks, the policy proved impossible to enforce, and attempts to block access to public IM resulted in a deluge of complaints to the helpdesk.

Without any practicable way to scan public IM networks for malware or any realistic hope of preventing employees from using them, the company was forced to shut

down the entire IM network for days at a time whenever a worm struck in order to clean out the infection and restore the system to normal operation. Over time, this was having a significant effect on employee productivity, as well as wasting IT resources that could be more productively deployed.

According to research from IBM, the use of instant messaging reduces telephone usage by more than four percent and saves around \$13 per month per employee in travel expenses. For a corporation with 70,000 employees, it's clear that significant operational cost increases will be incurred when IM becomes unavailable for an extended period of time.

Solution

Early in 2005, the company began an extensive review of potential solutions, including FaceTime's IMAuditor and Real-Time Guardian (RTG).

The award-winning IMAuditor™ is a scalable, enterprise-class application for the management and control of IM in the enterprise. Deployed behind the firewall, IMAuditor supports all public and enterprise IM clients, providing a single enterprise-wide IM management solution that enables IT to gain control of all IM communications through a single user interface.

Real-Time Guardian™ (RTG) is the industry's first multi-channel anti-malware perimeter security solution, enabling corporations to prevent unauthorized IM connections, block high-risk features, and create a standardized profile of IM use. Additionally, RTG enables corporations to block and prevent spyware infection as well as gain insight into bandwidth abuse, source and destination IP addresses, and port abuse.

IMAuditor maintains an integrated trust relationship with RTG for complete end-to-end security, management and control of IM in the enterprise.

The products were subjected to several rounds of extensive lab testing to determine compatibility with existing networks and ability to detect and report on both inbound and outbound security breaches. In July, the company awarded the contract for IM security protection to FaceTime, and has been delighted with the results thus far.

"With 70,000 users and 90,000 user accounts in 18 countries around the world, we really needed a solution that would not only enable employees to safely use public IM networks

but also be easy to manage from an IT perspective. By combining a central installation of IMAuditor in the U.S. with RTG perimeter protection in 20 regional IT facilities around the world, we have a solution that works well for everyone." – IT Manager, Global Communications Corporation.

Results

In the four months since it purchased the FaceTime solution, this organization has deployed enterprise IM protection to 55,000 of its 70,000 users around the world – in itself a testimony to the products' ease of use. The results from a security perspective are even more impressive:

"FaceTime's solutions blocked more than 20,000 malware hits in the first 80 minutes after installation. Everyone involved in the decision to put this protection in place, from the executive team to the helpdesk staff, couldn't help but be convinced that they'd made a good decision. We'll be deploying Live Communications Server shortly, and we plan to use FaceTime technology to protect that environment, as well as extending our use of FaceTime's anti-spyware solutions."
- IT Manager, Global Communications Corporation

Not only has the company been able to significantly improve their network security, but they are also able to track who the high-volume public IM network users are, and take appropriate action to educate and redirect the activities of those users.

About FaceTime Communications

Founded in 1998, FaceTime Communications is the leading provider of security solutions for the management and control of greynet applications such as adware/spyware, instant messaging, webmail, P2P file sharing, web conferencing and instant voice. FaceTime delivers the industry's first IMPact Index, which assesses "point-in-time" risks posed by viruses, worms and other malware propagating through greynet applications. FaceTime's award-winning solutions are used by over 500 customers, among them seven of the eight largest U.S. financial institutions. FaceTime supports or has strategic partnerships with all leading public and private IM network providers, including AOL, Google, Microsoft, Yahoo!, IBM, Bloomberg, Jabber and Reuters.

