

Britain's Open University Switches to FaceTime for Instant Messaging Management

CASE STUDY



ABOUT FACETIME IMAUDITOR™

- Enforce usage policy for all IM in the organization
- Prevent loss of intellectual property and other confidential information over IM
- Scan file transfers using existing anti-virus with no additional cost
- Zero-day defense against IM-based virus and worm attacks
- Automatically protect against IM and P2P threats
- Block SPIM to reduce the spread of viruses and worms across the network
- Sophisticated workflow process for regulatory compliance monitoring
- Guaranteed 100% accurate binary archiving of all IM
- Intuitive web-based administration and reporting
- Integrates with common email archiving and WORM storage systems
- Platform-neutral architecture with flexible enterprise deployment options

“ FaceTime’s IMAuditor does everything we need an IM security solution to do. It scans file transfers for viruses using our existing anti-virus. It can be deployed on Linux. It logs the IP addresses of clients. The database structures are well-documented, enabling us to do our own custom reporting. And the challenge-response mechanism prevents IM worms and SPIM before they do damage. ”

Chris Wigglesworth, Senior Systems Programmer, The Open University
FaceTime customer since August 2005

Overview

The Open University (OU) was the world's first successful distance teaching university. Born in 1969, the OU was founded on the belief that communications technology could bring high quality degree-level learning to people who had not had the opportunity to attend campus universities. Today, more than 180,000 students interact with the OU online from home around the world; they are supported by more than 4,000 academic and administrative staff at the main site in Milton Keynes, 13 UK regional centers, two warehouses, and European offices in Dublin and Brussels.

The OU has a complex IT environment encompassing Windows, Macintosh, Linux and Unix desktops, workstations and servers. There is a firewall cluster, extensive VPN infrastructure, and anti-virus is in place at mail gateways and on the desktops.

Challenge

The OU uses the Internet for almost every aspect of its business, and is the world's leading e-university. While the OU does not yet use instant messaging (IM) in its core business or officially support its use, the organization recognizes that students and staff alike use public IM services in their daily interactions and when collaborating with outside contractors. The sheer size and scale of the OU community, as well as its ever-changing population, renders its IT systems vulnerable to malware infections, so IT staff needed to prevent worms and viruses from using this new channel to invade and exploit the network. There was also a need to provide a record of IM conversations – who talked to whom using which IM system and when - but not their content.

The biggest concern regarding virus infections was the file-transfer capabilities of the IM clients. Early on, the clients used peer-to-peer techniques that could be controlled through the firewall, but newer clients include the ability to use the IM service as an intermediary which was less easy to block with a firewall. Comments OU Senior Systems Programmer Chris Wigglesworth, “While our desktop anti-virus strategy will for the most part cope with this newer approach, there will always be machines on the network with a faulty anti-virus install. An IM worm outbreak is our nightmare scenario - the nature of instant messaging means worms can propagate extremely quickly.” IM spam (SPIM) is also regarded as a risk for malware infections.



The OU also needed to be able to log instant messaging conversations in case of the need to, for example, investigate allegations of abuse or harassment using or involving IM. As IM conversations use a central server, without protocol inspection it was only possible to log that a client is using instant messaging, not to whom they are sending messages. At the same time, the UK's Data Protection Act requires that the privacy of instant message conversations be respected as personal communications despite their use of university resources.

In 2004, the OU took its first steps to address the problem by installing an IM management product available from a FaceTime competitor. While the SPIM and worm protection were adequate, the product required the use of a specific anti-virus solution – different from that used at the OU - and its reporting and management proved less flexible than the university needed. As client IP addresses were not recorded, staff had to manually map buddy names to users, which made deployment difficult, and attempts to upgrade were fraught with support problems.

Solution

At this point, Wigglesworth turned to JX Solutions, the OU's security reseller – who had been providing much of the support for the IM management product's installation – for alternatives. They had no hesitation in recommending FaceTime's IMAuditor. "FaceTime is the only company that recognizes IM cannot be isolated from P2P and spyware." Says JX Solutions Managing Director Toby Sparrow: "FaceTime solutions enable us to offer our customers a reliable solution that is based on safely permitting IM use rather than risk handicapping the business process by preventing its use."

Working with JX, the OU conducted an evaluation of FaceTime's IMAuditor, which provides virus, worm and SPIM protection through pattern-matching rules, augmented with a challenge-response mechanism that requires new buddies to enter a phrase to confirm they are real people and not a worm or bot. Wigglesworth was pleased to note that IMAuditor could be used with almost any anti-virus program, and that it could be deployed on Linux as well as Windows.

"Perhaps the most impressive aspect of IMAuditor is its flexibility," says Wigglesworth. "FaceTime clearly has a good understanding of the needs of mixed-platform, highly distrib-

uted IT environments. IMAuditor logs the IP addresses of clients. Full specification of the database structures are provided, allowing the information to be easily retrieved. This meant we did not need to map buddy names to user accounts, which greatly simplified deployment and helped reassure users."

Results

The OU uses IMAuditor to scan file transfers for viruses, block IM worms and SPIM, and to record IM message headers without recording content. Viruses and worms are prevented from spreading through IM to the internal network and users are unable to anonymously misuse IM on the network, significantly mitigating the potential for loss of reputation or legal liability. The ability to tailor the settings to respect users' privacy is very important in an educational environment, and the low maintenance and ease of integration with existing infrastructure keep the costs down for limited-resource environments.

Wigglesworth couldn't be happier with his decision. "IM threats are clearly growing, and it gives us considerable peace of mind to have IMAuditor in place now. We feel that we're ahead of the game. Importantly, it also allows us to investigate any claims of harassment, abuse or other improper use of IM on our network. In the future we see it as becoming more important as IM use grows.

"It has been simple to deploy and upgrade and simple to use. It has done exactly what we wanted it to. The technical support has been excellent with quick and detailed responses. The final deployment went smoothly and IMAuditor now regularly serves about 400 users a day."

Would he recommend IMAuditor to other higher-education establishments facing a growing threat from IM and other real-time communications protocols?

"Absolutely. It's easy to deploy and is available on both Windows and Linux, allowing you to choose the platform most appropriate to your organization. It uses your existing anti-virus solution, reducing costs, complexity, and support issues. It's reliable and needs little maintenance. It has granular reporting options that can be changed to address privacy concerns, and the database structures are open and documented, easily allowing custom reporting of your own."