Instant Messaging: Security, Control And Compliance

Melanie Turek

IM vendors are refining their solutions for protecting networks and meeting regulatory requirements.

There's no doubt about it: Instant messaging (IM) is a fact of life in the enterprise. More than three-quarters of IT executives report that employees in their companies use IM on the job, and countless vendors—from small start-ups to large enterprise stalwarts—are making it easier for companies to deploy a single IM client or service across the organization.

Instant messaging has the potential to change the way people work, especially in this increasingly virtual workplace. With more than 90 percent of employees working away from headquarters, and up to two-thirds working in a location separate from their managers', employees need a way to get in touch quickly and easily—right when they need to. The presence capability that powers instant messaging assures users that they can contact their co-workers or partners whenever those people are available, speeding information delivery and ultimately boosting productivity (no more phone tag, no more endless email threads).

What's more, vendors are branching out with their IM clients, enabling industry- and job-specific capabilities (such as trade orders or contact center support), as well as productivity enhancements (for instance, Microsoft embedding its Communicator IM client into the rest of its Office applications, for one-click messaging capabilities within a Word or Excel document).

But IM is also a potentially risky technology, opening up enterprises to threats from viruses, spam and other malware, much the way email does today. It also requires that rules and policies be set and maintained to ensure compliance with regulations.

The big difference is that while most IT executives are not only aware of the risks posed by email, but also take action against them, too few are protecting their networks from IM-borne threats, or their companies from IM-related compliance breaches. Indeed, only about one third of companies report using secure, manageable enterprise IM (EIM), and among those, two-thirds still allow their employees to also use (unprotected) public IM (PIM) services such as AOL's AIM and Microsoft's MSN.

On the other hand, some IT executives are so worried about the risks of IM, they ban it altogether—indeed, Nemertes saw the use of IM in the enterprise decrease between 2004 and 2005, as more companies clamped down on the threats by disallowing the use of instant messaging, period. It's hardly an effective strategy—throwing the baby out with the bathwater—especially these days, as more and more knowledge workers expect to be able to message not just co-workers, but partners, customers and suppliers, too.

Instead, companies should develop a clear IM strategy that includes deploying a secure enterprise IM client; applying the necessary security and management controls for compliance purposes; and enabling interoperability with other EIM and PIM services.

Security: Start Here

The first order of business is security—protecting enterprise networks and infrastructure from viruses, and end users from spam, spyware and other malware that comes along with unprotected IM.

Several vendors, from small startups (Antepo, Bantu, Omnipod, WiredRed, and others) to large enterprise players (Microsoft, IBM Lotus), have deployed a variety of security tools and features as part of their enterprise IM products. These closed systems may not be a threat if you keep them behind the firewall and use them only with your employees. But many companies are wary even of their EIM systems—users don't have to be intentionally malicious to cause havoc—and want to protect them from threat.

Even more important, of course, is protecting any public IM services in use in the enterprise, as it's on these consumer-oriented, completely open systems that most threats arise. Some EIM vendors extend a basic level of security to PIMs, but for the best protection many companies deploy

Melanie Turek, Nemertes senior vice president and founding partner, covers collaboration and virtual workplace tools for Nemertes.

software from one of the three so-called IM gateway players, which have traditionally enabled enterprises to add security and control to public and private IM: Akonix, FaceTime and IMlogic (now owned by Symantec).

Interestingly, much of the news in recent months has centered on product trends also emerging in the email world: appliances, real-time monitoring and all-in-one solutions.

For instance, Akonix recently released a line of IM security and compliance hardware appliances, all-in-one solutions optimized for instant messaging security and management for up to tens of thousands of users. The appliances are Akonix L7 Enterprise v5.1 and Akonix L7 Enforcer v5.1 (the latter product is designed to detect and block the unauthorized use of IM and peer-to-peer file sharing applications). The appliances are powered by AkOS, a hardened operating system developed by Akonix for real-time messaging environments.

Akonix also recently announced its new L7 IM Sentry application, which can be added to each user's buddy list upon login. When the IM Sentry receives a message containing an unknown URL, it alerts the IT administrator and puts the URL on a list of disallowed Web addresses, preventing any further propagation of the message. Any future IM traffic containing the URL is then automatically blocked.

Only fifty percent of companies include messaging as part of their compliance efforts

Another trend is the real-time monitoring of viruses and other threats. IMlogic's Real-Time Threat Protection System (RTTPS) was developed to predict and combat "zero-day" attacks on IM networks. Integrated with IMlogic IM Manager and the IMlogic Threat Center, RTTPS creates a global, networked community to exchange threat detection information and block IM security attacks, before anti-virus signature file updates are available. RTTPS automatically detects and quarantines suspicious or dangerous enterprise IM traffic. Similarly, the Akonix Security Center provides the latest information about worms, viruses and other vulnerabilities that are targeting IM and P2P networks.

Finally, general security vendors are getting into the IM game. For instance, early this year Symantec acquired IMlogic. Symantec and IMlogic partnered in the past: Enterprise Vault, Symantec's email and content archiving product, has been integrated with IMlogic's IM Manager since 2002. Now the companies will expand on that relationship, integrating IMlogic's threat detection and remediation capabilities into Symantec's early warning and response system, and ultimately delivering a product that works with email and IM. This trend is especially good news for IT executives, who want integrated messaging-management solutions for which they can set universal policies and controls.

Compliance: Messaging Matters

Another key issue for IT executives when it comes to IM is compliance. Just as more companies are archiving email messages for compliance purposes, many will need to do the same with IMs—whether because those, too, are regulated, or because they see doing so as part of a larger best-practices effort or hedge against legal discovery requests.

Many IT executives say they aren't sure how the regulations by which they're governed affect messaging—very often, they're waiting for the case law to define the parameters of the issue. Indeed, it can be difficult to assess whether certain rules apply to email and IM, and to what extent.

Sarbanes-Oxley (SOX), for instance, doesn't mention messaging. But SEC rule 17a-4 requires financial companies to retain, monitor and analyze electronic communications. HIPAA (the Health Insurance Portability and Accountability Act) allows doctors and other health care providers to communicate with patients via email so long as they use reasonable and appropriate safeguards to "ensure the confidentiality, integrity and availability" of any health information transmitted electronically, and "protect against any reasonably anticipated threats" to the security of such data. And government agencies tasked with sharing information with the public are often required to keep email messages (and other official correspondence) seemingly forever.

When asked, 90 percent of IT executives say they consider email and IM messages to be corporate information. On the other hand, only 50 percent of companies include messaging as part of their compliance efforts—and then, very often, they only include email and not IM.

What's more, many IT executives say they purposely don't "officially" deploy IM so that they aren't legally responsible for managing it. "By matter of policy we consider email to be corporate data, because we provide that system," said the director of IT at a mid-size consulting firm. "We have been required to produce email information, but we don't officially use IM, and policy is, it isn't supposed to be used for corporate information."

IT executives consider interoperability to be vital

We stress that if they aren't already, companies should include messaging—email and IM—in any compliance discussions and policies they have. At the very least, any company regulated by HIPAA or SEC rule 17a-4 should use a third-party archiving tool for email (available from vendors such as C2C, Orchestria and Symantec, through its Veritas/KVS acquisition) and IM (such as those available from Akonix, FaceTime or IM Logic), or an enterprise-class IM system that can provide those capabilities.

Interoperability: Gateway To The Future

One of the biggest drawbacks of real-time communications today is the fact that the different technologies can't interact with one another out of the box. That doesn't sit well with IT executives who want to extend IM to users outside their organizations. "Having them talk to each other is essential—not being able to talk to others because of the business decision [vendors] make is crazy," said one CEO who extends his professional-services company's IM service to clients.

Today, standards exist to make such open architectures a reality, but they don't measure up—many vendors base their tools on standards they then tweak for maximum performance. And the partnerships and deals in place to enable interoperability, while a good start, require too much forethought on the part of IT executives—as well as more money to pay for it.

The most common standards for real-time communications are Session Initiation Protocol (SIP) and SIP for Instant Messaging and Presence Leveraging Extensions (SIMPLE). Most major telephony and applications vendors, including Microsoft, back SIP and SIMPLE.

XMPP is a more open protocol that drives the Jabber IM client and which is supported by many in the open-source community, who consider it better, more mature and easier to work with. Some applications vendors, such as Oracle, have backed XMPP; others, such as IBM, are openly supporting it even as they build their own technology on SIP, SIMPLE and/or proprietary standards.

One of the biggest goals for vendors going forward should be to solve this problem. In an ideal world, presence would work the way the telephone and email do today. Any given presence server or services could pull presence from a variety of sources, aggregate and clean it, and then send it out to the desired applications, as well as other presence servers inside and outside the firewall. The applications themselves should be built on open standards, so that they can tap that same presence information, as well as offer IT managers relatively easy integration on the back end.

Why is this important? Because IT executives say it is. When we asked participants to tell us the most important issue or feature for collaboration vendors to focus on in the next 12 months, "interoperability" was critical; 70 percent of IT executives placed it at the top of their lists. And when asked to rate the importance of interoperability on a scale of 1 to 5, with 1 being unimportant and 5 being vital, 83 percent of IT executives said it's "vital" and the remaining 17 percent considered it "very important."

"We have had, for some time, basic interoperability requirements in all our RFPs," said one local government CIO. "We are somewhat in a federated enterprise, because we extend interactions to other organizations in the state government and the federal government."

Many vendors, including IBM Lotus and Microsoft, are delivering interoperability with the public IM services from AOL, Microsoft and Yahoo—as well as federated IM between select EIM vendors—via business partnerships. This allows users who pay for the service to message contacts on other IM systems and services, but only if they opt for the capability—and not all features associated with their IM products will also extend to the other systems.

Other companies have turned to hosted services to help them with their interoperability needs. "If we have a client and want to put a secure IM on their system we give them a license and they can talk to us through IM securely," said the CEO of a small professional services firm using Omnipod's hosted IM service. "Clients love it."

Conclusion

Instant messaging is already changing the way employees communicate—but it's also changing the way IT executives design and protect their networks. Ignoring the new technology, while tempting for some, isn't a solution. Instead, companies should look for an enterprise IM product that will deliver the security, control and interoperability they need to make the most out of this presence-driven communications tool□

Companies Mentioned In This Article

Akonix	(www.akonix.com)
Antepo	(www.antepo.com)
AOL	(www.aol.com)
Bantu	(www.bantu.com)
C2C	(www.c2c.com)
FaceTime	(www.facetime.com)
IBM Lotus	(www.lotus.com)
IMLogic	(www.imlogic.com)
Microsoft	(www.microsoft.com)
Omnipod	(www.omnipod.com)
Orchestria	(www.orchestria.com)
Symantec	(www.symantec.com)
WiredRed	(www.wiredred.com)
Yahoo	(www.yahoo.com)