Managing IM and P2P Threats in the Enterprise

an Osterman Research white paper
sponsored by

FaceTime™

Osterman Research, Inc. • P.O. Box 1058 • Black Diamond, Washington 98010-1058
Phone: +1 253 630 5839 • Fax: +1 253 630 5928 • info@ostermanresearch.com • www.ostermanresearch.com

Why You Should Read This Report

Instant messaging (IM) and peer-to-peer (P2P) file-sharing networks are finding increasing use within the enterprise, often without the consent – or even knowledge – of the IT department. IM, in particular, is increasingly used as a valuable tool for legitimate business uses even though most use of IM in the enterprise consists of consumer-grade clients that users have downloaded on their own initiative.

Instant messaging (IM) and peer-to-peer (P2P) file-sharing networks are finding increasing use within the enterprise, often without the consent – or even knowledge – of the IT department.

Because most use of IM and P2P in the typical enterprise consists of consumer-grade products that are quite adept at circumventing existing security defenses, an enterprise that permits the use of these tools puts its network, reputation and finances at significant risk from viruses and other malware, as well as potential violations of copyright.

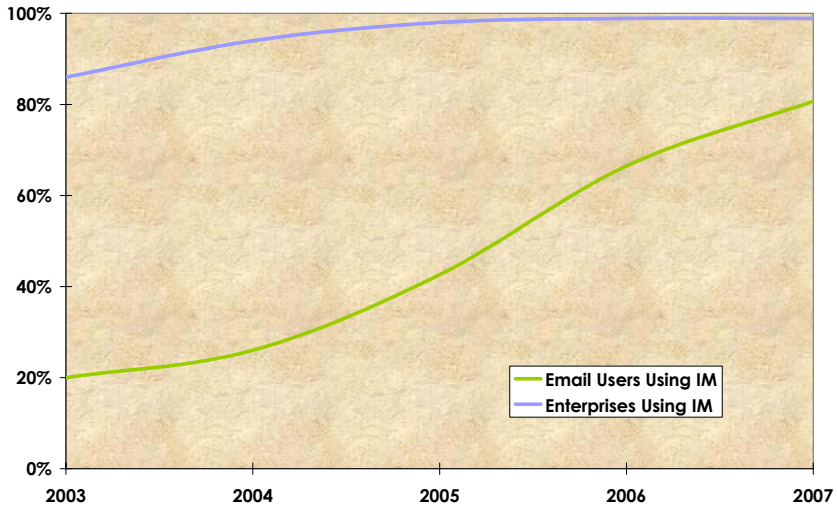
What enterprises need is a) to implement best practices with regard to IM and P2P use in the enterprise and b) a technology solution that will protect their networks from incursions and unauthorized use of IM and P2P. This white paper discusses both.

IM and P2P in the Enterprise

IM is currently used in the vast majority of North American enterprises: as of mid-2004, IM systems are in use in more than 90% of all commercial and non-commercial enterprises. Further, 26% of all enterprise email users now employ IM, a figure that Osterman Research estimates will grow to about 80% of all email users by 2007, as shown in the following figure.

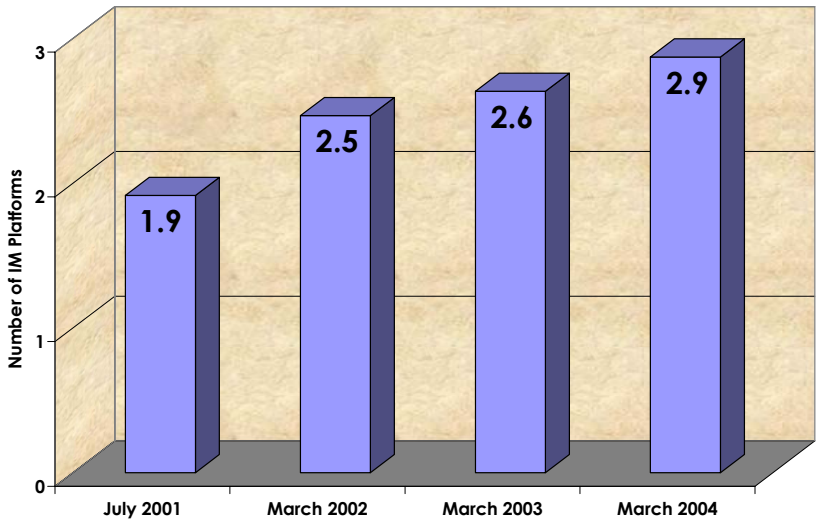
26% of all enterprise email users now employ IM, a figure that Osterman Research estimates will grow to about 80% of all email users by 2007.

Penetration of IM in Enterprises and Among Enterprise Email Users



Further, the number of different IM systems in use in the enterprise continues to grow, as shown in the following figure.

Mean Number of IM Platforms per Enterprise

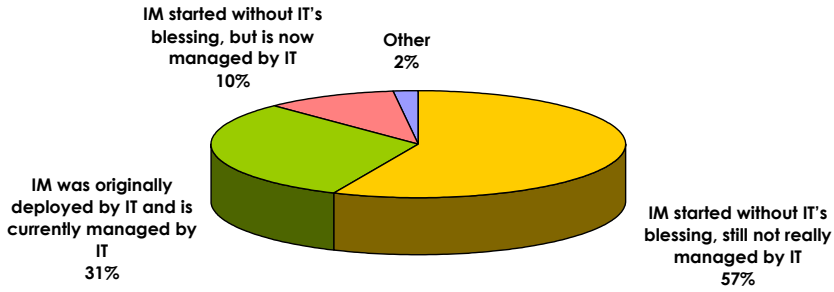


IM Started from the Bottom Up

Unlike virtually any other communications technologies currently in use in the enterprise, IM, in most cases, has developed as a 'bottom up' technology. In other words, most enterprise use of IM started with individual users deploying their own IM client (typically a consumer-grade client freely available from America Online, Microsoft or Yahoo!) outside the auspices of their IT department. In only one-third of enterprises was the deployment of IM initiated by IT, as shown in the following figure.

Most enterprise use of IM started with individual users deploying their own IM client outside the auspices of their IT department.

Methods by Which IM Entered the Enterprise



P2P Growth Has Been Similar

P2P networks – which often are used to share music and other consumer-oriented content – have entered the enterprise in a similar way. One study, conducted earlier in 2004, found that almost 40% of enterprise Internet users have downloaded and/or shared files via P2P networks using a corporate network.

Changing Perceptions About IM and P2P in the Enterprise

The perception of IM as an important business tool is maturing and both IT managers and line-of-business managers are becoming more open to IM's presence and use in the enterprise. What this also means is that enterprises in which users rely solely on consumer-grade IM clients – a significant portion of the use of IM in the enterprise – are opening themselves to a number of problems. As a result, the critical need for these enterprises moving forward will be to implement systems that will protect the network from these hazards, including the deployment of systems to manage the consumer-grade infrastructure currently in place, or implementing a purpose-built enterprise-grade IM system.

P2P networks, on the other hand, have far less – if any – legitimate use in a corporate environment and are unlikely to find nearly as much credible business use as IM[1]. Many are rightly suggesting that access to P2P systems within a corporate environment simply be turned off, as will be discussed later in this paper.

Corporate Risks from IM and P2P

Enterprises are at risk of receiving viruses, worms, rogue protocols and other malicious content through their IM infrastructure.

There are a number of quite serious risks faced by an enterprise that does not properly manage its IM and P2P use.

The Risks of Unmanaged IM Use

The informal, non-business nature of much IM use in the enterprise – which is dominated by consumer-grade IM systems – has created several problems for corporate IT departments:

- **Lack of namespace control**
  Because most enterprise IM users employ their IM client independently from a corporate directory, enterprises have little control over the IM identities of their employees. This has two important ramifications:
  - Operation independent of a corporate directory means that IM identities may not reflect the naming policies of an enterprise and so could be injurious to the reputation of the enterprise.
  - When an IM user leaves his or her employer, there is no way to prevent continued use of that user's IM handle, resulting in significant potential liabilities for an employer.
- **Lack of security**
  Because consumer-grade IM clients and their associated networks do not provide end-to-end encryption, local routing or other secure messaging capabilities; and because these clients can often penetrate corporate firewalls; enterprises are at risk of receiving viruses, worms, rogue protocols and other malicious content through their IM infrastructure, not to mention the lack of protection for sensitive content

[1] One of the few legitimate uses of P2P in an enterprise is file sharing which can be more efficient than downloading content from a central server, although enterprises should be extremely careful about using P2P for this application.

transmitted via IM. Consumer-grade IM systems can also create buffer overflow vulnerabilities in a corporate network.

- **Lack of auditing and logging capabilities**
  Consumer-grade IM clients typically do not provide any sort of logging of IM conversations – when the parties to an IM conversation leave the session, the content of their conversation is lost unless the text thread is manually copied and saved. This can result in significant problems for an enterprise that archives employees' electronic communications, particularly for those that are required by statute to do so. Further, it leaves an enterprise vulnerable if the archived content of an IM conversation is modified after the fact. This risk is a particularly important consideration in the context of increased corporate scrutiny imposed by regulations like the 'Books and Records' regulations from the SEC, the Health Insurance Portability and Accountability Act (HIPAA) and Sarbanes-Oxley.

[Lack of native IM archiving] leaves an enterprise vulnerable if the archived content of an IM conversation is modified after the fact.

- **Potential for incursion by viruses and worms**
  Because consumer-grade IM systems can easily bypass corporate defenses like anti-virus systems and firewalls, unmanaged IM represents a key avenue through which viruses, worms and other malware can enter a corporate network.

Based on a study that Osterman Research conducted early in 2004, the key concerns that enterprises have with business applications of IM (other than viruses and worms, which is a leading concern with consumer-grade IM systems in an enterprise setting), as well as the leading attributes that enterprises would like to have in their enterprise IM system, are shown in the following tables.

Concerns that Enterprises Have About the Use of Instant Messaging

Problem	% That Rated Problem a Significant or Major Concern
Security of information sent via IM	64%
Too much personal use	57%
Additional IT time required to manage	42%
Lack of interoperability between IM systems	35%
Cost of maintaining the IM infrastructure	33%
IM reduces user productivity	33%
Cost of implementing the IM infrastructure	31%

Importance of Various Enterprise IM Attributes

Attribute	% That Rated Attribute Very or Extremely Important
The ability to authenticate IM users against a corporate directory	82%
The ability to encrypt IM traffic between users	72%
The ability to block IM traffic for some users	70%
Maintaining complete ownership and control of your IM directory	69%
The ability to encrypt IM traffic between servers	69%
Maintaining complete, in-house control of your IM infrastructure	68%
The ability to enable or disable certain IM features for some users	66%
Ease of use and familiarity of the IM client	65%
Having IM meet compliance requirements from regulatory agencies	62%

Traffic from P2P networks can create enormous bandwidth drains on corporate networks. For example, some ISPs report that P2P traffic constitutes as much as 70% of the traffic on their networks.

The Risks Associated with P2P

P2P presents enormous security risks to an enterprise on a number of fronts.

- Downloading content from P2P networks bypasses corporate messaging security systems, leaving an enterprise network susceptible to viruses, worms, Trojans, buffer overflow vulnerabilities, spyware, adware and similar threats. Interestingly, FaceTime has found that exploits of a corporate network by P2P systems start *inside* an enterprise about 80% of the time, make egress concerns just as critical as ingress of malware and the like.

- Traffic from P2P networks can create enormous bandwidth drains on corporate networks. For example, some ISPs report that P2P traffic constitutes as much as 70% of the traffic on their networks.

- Perhaps the greatest P2P-related risk to an enterprise is that much of the content downloaded and shared via these networks consists of copyrighted material, the illegal sharing of which can expose an enterprise to charges of copyright violations. According to U.S. copyright law, anyone who infringes a copyrighted work is liable for damages for each work for which copyright has been violated – if a copyright owner can prove willful infringement, that amount can be increased dramatically.

  In late August 2004, the US Department of Justice began a crackdown on illegal P2P file-sharing known as Operation Digital Gridlock, highlighting the risk that enterprises face if they permit unauthorized P2P capabilities to operate over the corporate network.

- P2P clients open up the corporate network to file sharing.

P2P Networks and Their Capabilities

There are a large number of P2P networks that currently operate in corporate environments – a sampling of these networks and their capabilities are shown in the following figure.

Leading P2P-Related Networks and Capabilities

Network	P2P	Chat	IRC	VoIP	Other
Anonymizer					●
BearShare	●				
eDonkey	●	●			
eMule	●		●		
Gnucleus	●	●			
Grokster	●	●			
Hopster					●
Kazaa	●				
LimeWire	●	●			
Morpheus	●		●	●	
Shareaza	●	●			
Skype		●		●	
Xolox	●				

Examples of IM and P2P Threats

Among the many threats that can be introduced into a corporate network through unmanaged consumer-grade IM systems and P2P networks are the following:

- The w32.choke.worm uses Microsoft MSN Messenger to send itself as a reply to incoming messages.
- The Aplore worm spreads via AOL Instant Messenger by asking users to click a link to a worm residing on a remote server.
- The Goner worm, which is capable of deleting computer programs, distributes itself through ICQ.
- Attackers can trigger a buffer overrun on machines running Yahoo! Messenger by sending a long stream of data in the form of a Web page URL to a vulnerable function in yauto.dll, crashing the application or allowing the attacker to place his or her own malicious code on the machine.
- A buffer overflow vulnerability in an ActiveX control for MSN Messenger could allow an attacker to supply arbitrary code and have it executed under the privilege of the current user.
- Although the fizzerworm enters a network through email, it uses IM as a backup for its email infection and can spread through IM via user's IM contact list.
- When a user transfers files via P2P or uses IM-based file-sharing or voice chat features, that user's IP address is revealed, making it easier for a hacker to attack the user's system.

Despite the best attempts at blocking IM and P2P traffic, some of this traffic will continue to make its way through traditional defenses.

IM and P2P Security and Management Basics

Many organizations attempt to block IM and/or P2P traffic through a variety of methods, although Osterman Research has found that a significant percentage of IT staff believes that adequate blocking, at least of IM, is not even possible. Why? Simply because IM and P2P clients tend to be quite agile at finding ports through which they communicate with the outside world and because many of these systems use native and third-party tunneling mechanisms. In short, despite the best attempts at blocking IM and P2P traffic,

some of this traffic will continue to make its way through traditional firewall, IDS/IPS and URL-blocking defenses.

Complicating the issue is the fact that there are many legitimate business uses for IM in the enterprise. Osterman Research has found that more than 40% of enterprises currently use IM for legitimate applications. Further, blocking IM can create problems for employees who have grown to rely on IM for doing their work. By contrast, because there are very few, if any, business uses for P2P in the workplace, the social and productivity ramifications of blocking P2P are far less extensive than for blocking IM.

Why IM and P2P are Outpacing Traditional Security Tools

As an IM application tries new sockets and protocol tunneling techniques, firewalls are generally unable to discern common evasion techniques that exploit these well known vulnerabilities.

Perimeter security solutions are designed to keep hosts beyond the firewall from connecting to resources inside the firewall. These solutions have been optimized to protect from ingress into a corporate network and, for the most part, are quite good at preventing intrusions. By contrast, selective egress enforcement becomes a much more difficult problem than the relatively simple task of complete ingress blocking. In other words, it is much simpler to keep everything out of a network than to allow only certain internal applications to communicate with the outside world.

Egress connections established by users on an internal network are targeted for specific and well-known application ports (e.g., Web browsing on ports 80 or 443). These ports are the default open and allowed egress points for a variety of legitimate corporate applications. While blocking egress is technically quite simple, outbound port blocking is an all-or-nothing proposition: once certain outbound access points are permitted for legitimate applications, they are easily abused. This is why IM and P2P systems so easily circumvent traditional security infrastructures.

The Problem with Firewalls

Firewalls are used to block specific ports and IP addresses (sockets) from ingress and egress attempts. By default, most firewalls are configured to accept few, if any, ingress connection attempts (e.g., to accept only VPN attempts on specific ports and to establish pass-through only after authentication has successfully occurred). Further, most firewalls are configured to allow a number of egress connections based on port and protocol adherence – for example, certain application-aware firewalls will inspect

protocol flows to make sure that port 80 traffic is, indeed, HTTP traffic. As an IM application tries new sockets and protocol-tunneling techniques, firewalls are generally unable to discern common evasion techniques that exploit these well-known vulnerabilities. This is because the exploits typically do a good job of mimicking protocol and/or adherence. Furthermore, when firewalls are application-aware and are conducting deep packet protocol analysis, their inline performance degrades to a point that significantly impacts network performance.

Why Web and Application Proxies Provide an Inadequate Defense

Web and application proxies are deployed inline with firewalls to inspect protocol-specific traffic. The concept behind these defenses is that the proxy performs a more rigorous inspection of protocol-specific messages. URL filtering and protocol spoofing can usually be accomplished with these systems. However, these systems typically fall short because IM and P2P traffic evade these filters through protocol adherence and the use of multiple destination addresses.

These methods leave enterprise network defenses open to circumvention by IM and P2P systems. The only practical way to detect and prevent these techniques is to deploy egress enforcement solutions that are targeted specifically at IM and P2P.

A security scan, if nothing else, can educate IT managers about what is actually running on the corporate network.

Signature-based deep packet inspection is required to catch all of the evasion methods. The ideal solution looks like a reverse IPS that is targeted specifically at IM and P2P. It is also important to note that if some IM use is allowed, the solution that is implemented will have to be able to discriminate between IM traffic that is within policy and that which is circumventing policies. Firewalls, proxies and URL blocking solutions cannot accommodate these scenarios.

Why a Proactive IM and P2P Security/Vulnerability Analysis is Necessary

A security scan of a corporate network is a good idea for a number of reasons. First, many IT managers are simply unaware of the extent to which IM and P2P exists on their corporate network. A security scan, if nothing else, can educate IT managers about what is *actually* running on the corporate network. Secondly, if an IT manager considers the network to be safe, then a security scan, by finding new applications that can successfully penetrate existing

corporate defenses, can illustrate where there are holes in the existing infrastructure. For managers who already acknowledge that their users could be employing IM and/or P2P tools, the goal of a scan might be to inform them of the extent of the risk they face.

Best Practices

There are a variety of best practices with regard to IM and P2P use within an enterprise:

- P2P should be blocked in almost all cases. While there might be an occasional legitimate use of P2P, the uncontrolled use of these systems puts an enterprise's network at serious risk of being infected with malware and related content. Further, P2P systems can create significant legal liabilities because of the common distribution of content in violation of copyright.

- IM monitoring should be implemented at the perimeter of a network using an IM gateway or proxy server. A monitoring system should be deployed that can detect all IM traffic occurring on a network.

- IM sessions should be archived for three reasons:

    - Because of increasing government scrutiny, exemplified by legislation like Sarbanes-Oxley, there is a growing need to archive electronic communications of all types, including email and IM.

    - IM archival is useful to comply with internal corporate policies, HR regulations, knowledge management needs and other organization-specific requirements.

    - Archiving is useful for disaster recovery. If there is a major security-related event associated with an IM system, archival can be extremely valuable in rebuilding lost data stores.

Unlike spam, SpIM is sent primarily via rogue protocols and related malware-types of incursions.

- Anti-SpIM capabilities (designed to protect a network from spam sent via IM) should be deployed. Because, unlike spam, SpIM is sent primarily via rogue protocols and related malware-types of incursions, it is

important to protect a network against these protocols to prevent unauthorized access to 'buddy lists' for purposes of distributing commercial messages or other unwanted content.

- IM systems should at all times be integrated with corporate anti-virus capabilities because of the significant potential for viruses to enter through IM.

- Content filtering in IM systems is important to guard against violations of corporate policy and the like. Systems that can monitor outgoing IM messages for a variety of keywords and other sensitive content, like Social Security numbers, are part of a best-practices approach to IM management.

- Inserting disclaimers in outgoing IMs is important for two reasons:

    - At least one court has found that archival of IM conversations without the consent of all parties constitutes a violation of wiretap laws[2]. While such decisions are unlikely to stand, notification through disclaimers can mitigate against potential claims of wrongdoing.

    - Disclaimers can eliminate most out-of-policy behavior. In other words, employees using IM are far less likely to violate corporate policy if these policies are spelled out in disclaimers that are automatically attached to each message.

Any best practice must protect the corporate network at its perimeter and manage internal use of IM so that corporate policies are followed.

Defense-in-Depth

In short, any best practice for the management of IM in an enterprise must include two essential elements:

1. Protect the corporate network at its perimeter by preventing users from circumventing anti-virus, firewall and other defenses through the use of consumer-grade and other 'public' IM and P2P systems. This includes protecting the network from internal

[2] In February 2004, a New Hampshire judge ruled that copying and pasting the content of an IM conversation without the consent of all parties involved violates that state's wiretap laws. Several other US states require that all parties to a conversation provide consent before a conversation can be recorded.

applications, such as P2P systems, from initiating communication with the outside world.

2. Manage internal use of IM systems so that corporate policies are followed and so that key corporate resources – applications, storage, data and other elements – are protected from unauthorized access.

This strategy – known as 'Defense-in-Depth' – is essential to ensure that the productivity and other benefits of IM are realized while at the same time protecting the corporate network from threats and policy violations.

The FaceTime Solution

Use of IM in the workplace is introducing new challenges and severe corporate and security risks into the enterprise. Management and control of IM and P2P can no longer be ignored. The need for a higher level of security for a real-time messaging infrastructure is imperative.

Only FaceTime offers a complete 'Defense-in-Depth' approach–a comprehensive strategy for end-to-end security and management of IM and P2P. This approach consists of two key components:

1. RTG500™ in the DMZ to block unauthorized IM and P2P usage and protect against sophisticated workarounds and enforce compliant, authorized use.

2. IMAuditor™ in the LAN to enable user policy management, hygiene (anti-SPIM, anti-virus), regulatory and corporate compliance, archiving and logging, and identity management.

Our proven two-point approach, based on secure and reliable code, has passed rigorous certification and is in use today by the largest financial institutions in the world.

Founded in 1998, FaceTime Communications is the leading provider of extensible real-time management solutions that address network and information security and regulatory and corporate compliance.

FaceTime has built the industry's most comprehensive ecosystem of partners to provide the best solutions available for the security, management and control of real-time

applications. FaceTime has strategic partnerships with all leading public and private IM network providers, including AOL, Microsoft, Yahoo!, IBM, Bloomberg, Jabber and Reuters, as well as with a wide range of leading technology partners that complement and extend our solutions in the enterprise.

FaceTime is headquartered in Foster City, California. For more information on FaceTime, visit http://www.facetime.com or call 888-349-FACE.