

Introduction

Since the first release of AOL Instant Messaging (AIM) in 1997, the popularity of instant messaging (IM) has never abated and for good reason. IM is easy to use and it facilitates rapid, conversational, communication, making it a very powerful tool for both personal and business use. The business benefits of IM are very clear. These applications enable rapid and efficient communications, allowing employees to easily answer customer questions, find answers to time-sensitive issues and collaborate without using the slightly more formal tools such as a phone or email. The personal benefits are equally obvious. The [Application Usage and Risk Report \(5th Edition, Spring 2010\)](#) confirms the popularity of IM applications by analyzing application traffic on nearly 350 networks around the world. The analysis showed that 60 IM variants were found overall across 97% of the participating organizations. An average of 12 IM variants were found to be consuming 6.7 GB within each of the participating organizations where IM was detected.

Figure 1 shows the ten most commonly used IM applications within nearly 350 organizations around the world. Note that Yahoo IM! is the most commonly used IM application while a variant of the original AIM is still in use in more than 50% of the organizations analyzed.

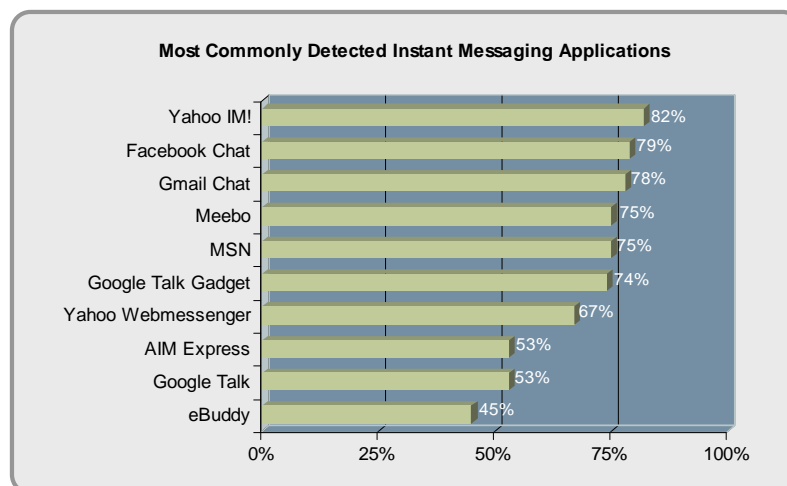


Figure 1: Ten most commonly detected Instant Messaging applications.

No one would dispute the business benefits that IM applications bring to the enterprise – collaboration, increased communications efficiencies and time-to-market are just a few. However, IM applications do pose certain business and security risks. Regulatory compliance within specific industries such as financial services, data loss via file transfer features, malware propagation and vulnerability exploits are the key risks that organizations are exposed to when IM is in use.

An analysis of the underlying technology and the behavioral characteristics for the IM applications found (see table 1) highlights the some of the business and security risks that IM applications pose.

- **Able to easily traverse the firewall using TCP/80, TCP/443, or by hopping ports.** Within the top ten, every variant is capable of traversing the firewall, including those that are client-server based. Within the overall sample 85% (51 of 60) of the IM applications can easily traverse the firewall. A significant risk for industries such as financial services are regulatory compliance violations introduced by unrecorded conversations over unapproved IM applications. Other, more broad-based risks include possible leakage of confidential information that can be introduced by the fact that the traffic looks like common web or SSL traffic.
- **Able to transfer files.** Of the top ten IM applications found, only two of them are capable of transferring files while 28 out of all 60 variants (47%) support file transfer behavior. The risks associated with file transfer include malware delivery and data leakage associated with the unauthorized transfer of files.

Solution Note: Controlling Instant Messaging Usage

Reaping the Business Efficiencies of IM While Mitigating the Risks



- **Malware delivery and have known vulnerabilities.** Both of these risks are well represented within both the top ten and overall sampling. The risks around these behavioral characteristics introduce include propagation of threats, damages to the network resources, data theft and increased expenses associated with fixing the damages inflicted.

Ten Most Commonly Detected IM Applications Found Within the Participating Organizations					
Underlying Technology	IM Variants Identified	Can use TCP/80, TCP/443, or hop ports	Can Transfer Files	Used to Deliver Malware	Have Known Vulnerabilities
Browser-based	70%	70%	10%	30%	70%
Client-Server	30%	30%	10%	20%	30%
Peer-to-peer	0	0	0	0	0
Total	100%	100%	20%	50%	100%
All 60 Variants Found Within the Participating Organizations					
Underlying Technology	IM Variants Identified	Can use TCP/80, TCP/443, or hop ports	Can Transfer Files	Used to Deliver Malware	Have Known Vulnerabilities
Browser-based	50%	48%	17%	5%	47%
Client-Server	42%	33%	22%	23%	27%
Peer-to-peer	8%	5%	8%	5%	5%
Total	100%	85%	47%	33%	62%

Table 1: Breakdown of the technology and behavioral characteristics for the IM applications found.

In order to strike the appropriate balance between enabling the business benefits that IM applications represent and their associated risks, organizations must take a systematic approach.

The Challenge: Enabling IM and its' Associated Business Efficiencies

Instant messaging applications enable more efficient communications so the benefits are very clear. They are easy to use and can simplify communications to friends, family and co-workers around the world. The challenge for IT is to maintain network security while enabling a set of applications that most people would view as being used more for personal, not professional, purposes.

The business benefits of IM make the unreasonable “block all IM” an inappropriate response while the “head in the sand, allow all” approach is equally inappropriate due to the business and security risks described earlier. Organizations need to follow a systematic process to develop, enable and enforce policies that allow the use of IM in a secure manner.

1. **Find out which IM applications are in use and who the users are.** The ubiquitous nature of IM applications (an average of 12 variants in 97% of the participating organizations), means that it is not a question of “are they in use”, but more a matter of how many variants and how heavily. Key questions to answer include which IM variants are in use; do they support other features such as file transfer or VoIP; are they browser-based or client-server; and how much of a security threat do they pose (malware delivery and known vulnerabilities). Knowing who the users are will allow IT to have a meaningful discussion with the business groups and agree upon the common company goals. Equally important, is that this step can help IT move past the image of “always saying no” and towards the role of business enabler.
2. **Develop an IM application usage policy.** Once visibility into IM usage patterns are determined, organizations should engage in discussions around which IM applications and which functions should and should not allowed on the network. In some cases, LotusSametime or Microsoft MCS (detected 7% and 3% of the time respectively) may be the approved corporate IM application. These applications are corporate-based IM solutions and may not be well suited for personal, so a secondary IM such as MSN may be allowed and defined in the policy. If a corporate IM is not in place, then an IM variant that ties multiple IM networks together may be worth considering to ensure flexibility. Meebo, one of the more popular IM variants is an excellent example of an IM application that enables a single client to “talk” across a range of IM networks including AIM, Yahoo!, Windows Live Messenger, Google Talk, ICQ, and Jabber.

3. Additional considerations will revolve around possible compliance issues such as those within the financial service industry where there are strict rules around both the use and archiving of IM conversations. The results of these discussions, including which IM applications are or are not allowed should be well documented and shared with users.
4. **Use Technology to Monitor and Enforce Policy.** The outcome of each of these discussions should be documented with an explanation of how IT will apply security policies to enable the secure use of IM across the organization.

Documenting and enforcing a policy around IM can help organizations improve communications, productivity, and the bottom line while boosting employee morale while reducing risks. An added benefit is that it can help bridge the chasm that commonly exists between the IT department and the business groups.

The Solution: Apply Policy Control Over IM Usage, Block Threats

Palo Alto Networks next-generation firewalls allow organizations to take a very systematic approach to enabling the secure use of IM applications by determining usage patterns, matching them with business objectives and then establishing (and enforcing) policies that enable business objectives achievement in a secure manner.

- **Identify IM Usage Patterns.** As stated earlier, it is highly likely that IM is already in use due to its ubiquitous nature. Palo Alto Networks identifies 80 different IM applications (see list [here](#)), with new variants added on a regular basis via a weekly content update. The goal of this phase is to determine which variants are in use, by whom, how heavily and for what purpose. Once the variants in use are found, the behavioral characteristics (file transfer, evasiveness, malware vector, known vulnerabilities) can be used to further determine the level of risk associated with the application.
- **Define and Enforce Appropriate Usage Policies.** After determining the usage patterns and business requirements, administrators can apply appropriate usage policies that support the organization's goals and objectives. The ability to delineate which IM applications are popular and who is using them means that appropriate enablement policies can be deployed. The identity of the application tied to the user information from enterprise directory services (Active Directory, LDAP, eDirectory) enables administrators to apply policies that go beyond the traditional allow or deny:
 - Allow or deny
 - Allow based on schedule
 - Allow and apply traffic shaping (QoS)
 - Allow certain application functions
 - Allow but scan
 - Decrypt and inspect
 - Allow for certain users or groups
 - Any combination of the above

Using a policy editor that carries a familiar look and feel, experienced firewall administrators can quickly create a firewall policies that:

- Allows only AIM, YahooIM! and MSN for all users and scans the allowed traffic for specific types of malware and vulnerabilities to protect the network.
- Allows AIM, YahooIM! and MSN for all users but blocks the ability to transfer files.
- Allows Meebo but applies traffic shaping to ensure it does not rob business critical applications of precious bandwidth.
- Allow any IM that does not transfer files.
- Allow MSN, AIM and YahooIM! but look for and block the transfer of specific file types.
- Allows IM usage based on a specific schedule and scan the traffic and alert on SSN data patterns.
- Denies IM use and presents the user with a notification as to why the application has been blocked.

The use of IM brings clear business benefits to the company so it is important to enable the use while managing the business and security risks.

Solution Note: Controlling Instant Messaging Usage

Reaping the Business Efficiencies of IM While Mitigating the Risks



- **Protect the Network From Malware and Vulnerability Exploit Attempts.** The ubiquitous nature of IM applications makes them a very common delivery mechanism for viruses, Trojans and worms. More often than not, the malware first installs itself, then is propagated across the unsuspecting users buddy list. The key to protecting the network against threats is to first determine which IM applications are allowed on the network, while blocking all others, as described earlier. Blocking unwanted IM applications can help reduce the attack surface and the application characteristics are an invaluable resource to assist in this decision making process. Then, once the *allowed* list is determined, specific malware and vulnerability profiles can be assigned to look for, and block the propagation of threats.
- **Monitor and Control Unauthorized File and Data Transfers:** As part of the balancing act between personal and professional IM usage, organizations must also evaluate how best to implement policies that are designed to limit unauthorized transfer of files and data. Taking advantage of the Palo Alto Networks data filtering and file transfer control capabilities, administrators can apply policies to limit the transfer of confidential data.
 - **File transfer function control.** Palo Alto Networks can exert file transfer control on multiple levels. First, using the application characteristics, administrators can block the use of applications that exhibit are capable of transferring files. The second control mechanism is at the functional level where the IM application itself is allowed, yet the file transfer function is blocked. The key differences between the two are that one is at the application level, the other at the function level.
 - **Block files types:** More than 50 different file types are identified and can be controlled with response options that include outright blocking, block and send the user a warning message or log and send an alert to the administrator.
 - **Data filtering:** Detect the flow of confidential data patterns (credit card numbers, social security numbers and custom patterns) with varied response options (block, alert, log) depending on the policy.

Summary

The response to the use of ubiquitous, consumer-oriented applications like instant messaging can take one of two forms. Blindly blocking, which may result in lost productivity and business opportunities or blindly allowing, which can expose the business to unnecessary business and security risks. The recommended approach to managing the use of these types of applications is for IT departments to work with the business groups to determine key business requirements and how they can enable the secure use without hindering workflow. With a Palo Alto Networks next-generation firewall, the IT department can achieve the best of both worlds by enabling usage while protecting users and the company from a wide range of business and security risks.