

## Postini IM Security Service Prevents IM-Borne Threats

“Postini IM Security gives me the peace of mind that users can’t create problems by clicking on or installing something they shouldn’t.”

IT manager  
Professional Hockey Team

Instant messaging (IM) has become a standard business tool, joining email as a core business communications medium. Companies say IM is improving client communications and reducing costs. According to a recent article, analysts are forecasting that 95% of employees will use IM as their de facto tool for voice, video, and text chat by 2013.<sup>1</sup>

However, much of IM usage is frequently “under the radar” of the IT department—because it is easy for employees to download public IM clients without the approval or knowledge of the IT team. Publicly available IM clients are designed to find a way through firewalls, making them difficult to control, secure, and manage. The result is that while IM is broadly in use in many businesses, only 25% manage and protect it.

IM is therefore an enticing target for hackers and spammers (called spimmers in the world of IM), exposing many companies to vulnerabilities. Users can unknowingly activate worms by clicking malicious URLs from spoofed buddies. Hackers can steal company directories by scanning contact lists. Company data can be leaked via unauthorized file transfers, since IM clients don’t check content against policies or have the ability to archive messages for regulatory compliance.

### What Postini IM Security Service Does

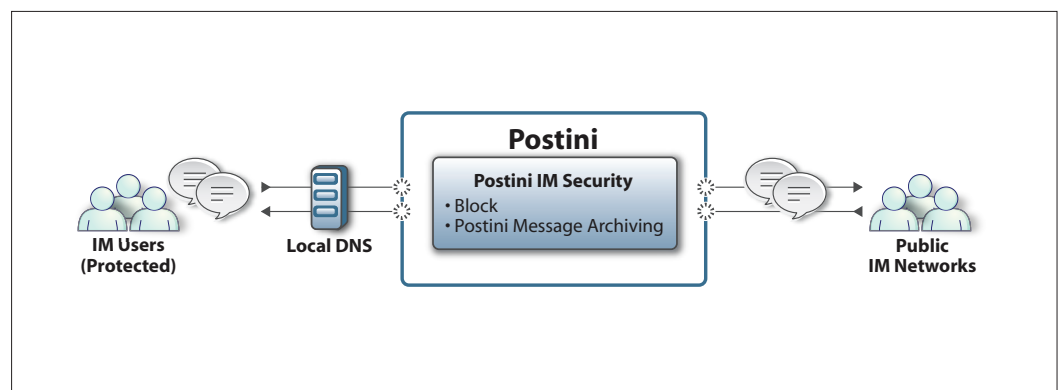
Postini IM Security service prevents IM-borne threats from reaching your network, and enables the monitoring and archiving of IM. Administrators can dynamically set IM access policies, control inbound and outbound IM file transfers, filter conversations for inappropriate or sensitive content, and archive IM sessions for future search and retrieval. Best of all, it’s easy to implement. Postini IM Security service can be activated in a matter of minutes with a simple Domain Name System (DNS) redirect to begin protecting your organization from IM threats.

Additionally, Postini IM Security service brings visibility into enterprise IM usage. With the service, IT now has visibility into usage and can begin planning and management of IM as a corporate resource.

### How Postini IM Security Service Works

#### Threat prevention

IM worms and viruses represent more than 90% of all IM threats. Postini ensures these threats are effectively blocked from ever getting to the recipient and your network.



**Figure 1:** Postini IM Security sits between your corporate firewall and public IM carriers to protect your network and users from IM threats such as IM worms. Public IM traffic is routed to Postini IM Security via changes to your local DNS server or SOCKS server.

1. Source: Gartner—Instant Messaging Reigns Supreme, June 26, 2007

**Content management**

You have the ability to block file transfers, as well as inappropriate content, from being transmitted via IM in order to mitigate the loss of intellectual property and legal liabilities.

**User management**

You can apply granular IM policies to your entire organization, to user groups, or to individual users through the central Administration Console. This gives organizations the control over which users have access to public IM, which public IM network will be used, and whether the conversations will be internal only or to external users as well.

**Compliance**

You can configure policies for archiving IM's according to group or individual user for better record keeping and compliance with corporate and industry regulations. IM conversations can be routed to the Postini Message Archiving service or to a designated corporate email address.

**Visibility**

Public IM screen names are created by end-users. You can now get visibility into what person controls each screen name, their use, and content of their conversations for policy enforcement and archiving.

**No installation. No maintenance.**

Like all Postini services, Postini IM Security service is an on-demand service, making it fast and simple to deploy. No specialized IM expertise is required, or the installation of any hardware or software. There's never any maintenance or updates to worry about.

**Conclusion**

The Postini IM Security service protects your network, your confidential information, and your computing resources while ensuring a productive and compliant workplace. Postini IM Security service controls the use of IM in your workplace, stops IM-borne threats from reaching your network, and enables the monitoring and archiving of IM.

### Postini IM Security Service

Features	Benefits
<b>Global communication policy management</b>	Enables consistent communication policies for email and IM at the organization, sub organization, or individual level. Establishes content and attachment filters to monitor acceptable use and prevent malware infections.
<b>Automatic real-time protection</b>	Proactively keeps threats from ever reaching your network, protecting both IM and non-IM users. Protects users from known and zero-hour threats as well as infected links.
<b>User management</b>	Provides the ability to link IM screen names to an existing corporate email address, thus removing the anonymity of the IM user and enabling unified policy management.
<b>IM archiving</b>	Captures all IM conversations for electronic record retention purposes. Clients subscribed to the Postini Message Archiving service can direct IM conversations into the same message store as their email.
<b>Lower cost</b>	Requires no additional hardware or software to install and maintain on desktops or email servers.

#### Technical Specifications:

##### Services Required

- Postini Email Security

##### System Requirements

- DNS or SOCKS Server
- Any Combination of these public IM carriers:
  - Google Talk
  - Yahoo! Messenger
  - MSN Messenger
  - AOL Instant Messenger (AIM)

### About Postini

Postini, a wholly owned subsidiary of Google, is a global leader in on-demand communications security, compliance, and productivity solutions for email, instant messaging, and the web. Postini's award-winning services are designed to protect customers from viruses, spam, phishing, fraud, and other attacks; encrypt messages to ensure confidentiality and privacy; and archive communications to ensure compliance with regulations and to prepare for e-discovery.

More than 35,000 businesses rely on Postini everyday to protect them from a wide range of threats. Customers can ensure reliable communications, reduce compliance and legal risks, and enable the intelligent management and enforcement of enterprise policies to protect intellectual property, reputations, and business relationships. More than 1,700 business partners worldwide add value to Postini solutions.

For more information please contact Postini at [info@postini.com](mailto:info@postini.com) or visit [www.postini.com](http://www.postini.com).

© Copyright 2007 Postini, Inc. All rights reserved. DS46-0709

Postini, the Postini logo, Postini Perimeter Manager, Postini Threat Identification Network (PTIN), Postini Industry Heuristics, and PREEMPT are trademarks, registered trademarks, or service marks of Postini, Inc. All other trademarks are the property of their respective owners.