

# Zone Labs Integrity IM Security



---

## Product Sheet

---

### The First Endpoint Security Solution for Instant Messaging Safety

Instant Messaging (IM) can significantly boost corporate productivity, allowing users to exchange information more quickly than ever. But along with convenience and efficiency, IM also carries a serious security threat. Similar to email, IM creates an ingress point that hackers can compromise as a conduit to enterprise systems and data.

The threat is real and is growing extremely fast; 19 of the top 50 malicious code threats in the first half of 2003 used IM and peer-to-peer platforms to propagate and penetrate company defenses.\* Once inside the firewall, hackers and malware such as Smibag and Coolnow can wreak havoc on IT assets, taking advantage of:

- Client vulnerabilities such as buffer overflow, malicious scripting and "social engineering" by mischievous, malevolent hackers
- Network exposure including open, persistent connections that can be exploited by worms and other bandwidth-clogging malware
- Traffic vulnerabilities that can result in breaches of confidentiality and loss of intellectual property.

#### IM Security: A Must-Have for Total Endpoint Security

The reality is, endpoint security without an IM-specific element is not complete. Zone Labs® provides an ideal solution with Zone Labs Integrity™ IM Security, the first comprehensive IM security solution that keeps IM conversations private and

secure, regardless of the IM service used. With it, endpoint PCs are protected from the spammers, social engineers, hackers and malware that can exploit vulnerable IM connections. While other endpoint vendors point out the threat, none provide the same level of comprehensive IM security.

A product module that is seamlessly integrated with Zone Labs Integrity, Zone Labs' IM solution offers policy-based endpoint security that is superior to other types of IM security. Unlike port-level protection, which is easily bypassed by portable IM programs and clever end-users, Zone Labs offers protocol-level protection to all incoming and outgoing traffic. And unlike IM protection at the gateway, which doesn't protect remote or external mobile users, can't encrypt messages and adds a single point of failure, Zone Lab provides full security and encryption to all users without having to maintain an additional server. Zone Labs also complements proprietary internal solutions like Lotus® Sametime™ by allowing employees to safely use IM to communicate outside the enterprise.

---

**"A review of the top 50 virus and worms over the past six months shows 19 malicious code submissions used P2P and IM applications. This is an increase of almost 400% in only one year."**

**-Symantec Internet Security Threat Report,  
October 1, 2003**



A Check Point Company

---

\* Symantec Internet Security Threat Report

## Zone Labs Delivers Comprehensive Endpoint IM Security

Until now, IT managers and administrators have had three choices in handling IM security risks: ignore IM and remain susceptible to its increasing security risks; attempt to block IM and realize that existing mechanisms are easily bypassed; or replace it with a private IM system that jeopardizes IT's productivity and doesn't allow safe external communication.

Integrity IM Security filters, blocks and analyzes network traffic, defending the enterprise from the risks of public IM usage with "client-agnostic" protection. Regardless of the IM client used – such as ICQ, IRC, AOL, MSN, Yahoo! or third party clients such as Trillian – endpoint PCs are instantly protected. Zone Labs provides transparent enforcement to end users, allowing them to maintain productivity and continue using their preferred IM client.

A first for endpoint security, Integrity IM Security gives IT the flexibility to control IM-specific rules – such as allowing or disallowing usage; encrypting traffic using Triple DES (168-bit) encryption and blocking unencrypted traffic; filtering out potentially dangerous content such as URLs, and video and music files; and providing inbound threat protection.

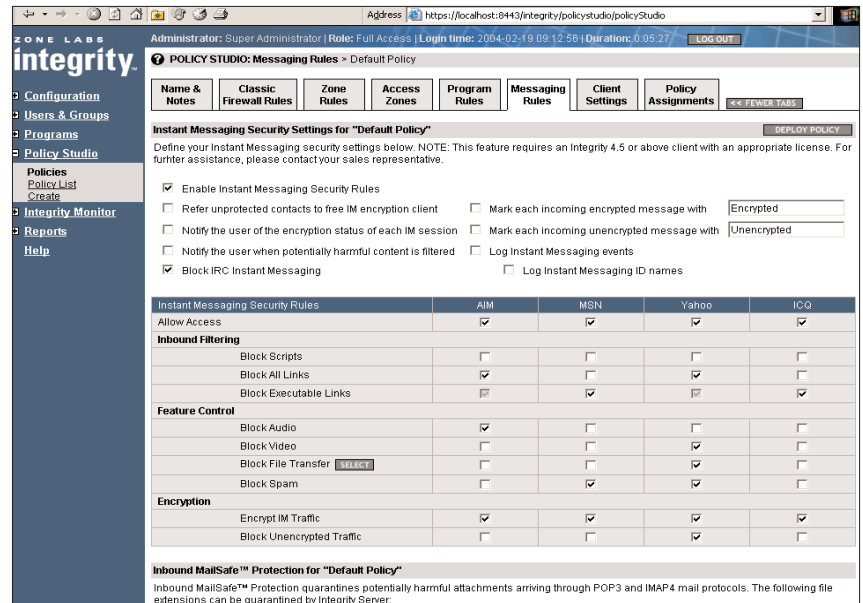
## Zone Labs Delivers Best-of-Breed IM Security

Integrity IM Security provides strong security for all IM functions including:

- Inbound threat protection: Zone Labs guards endpoint PCs by blocking dangerous IM transmissions such as invalid messages, buffer overflow attacks, unsafe scripts and either all URLs or only executable URLs. It defends endpoint PCs and files from hackers, thieves, vandals and

social engineers who attempt to access or gain control over PCs and corporate networks – for example, a social engineer who sends a URL link to an unsuspecting user, who is taken to a dangerous Web site and their PC compromised.

- Message encryption: Zone Labs encrypts IMs between any two protected clients that are connected to the same IM service, even if the IM clients are different, e.g., it can encrypt messages between Yahoo! Messenger and Trillian. This protects intellectual property and confidential information from being monitored or stolen. It also optionally extends encryption beyond the enterprise by directing external contacts to free IM encryption tools.
- Spam blocker: Zone Labs rejects IMs sent by anyone other than a known, approved contact, shielding users from social engineering, inappropriate content and wasted time.
- Access control: IT can permanently or temporarily shut down IM access per IM service and/or user in real-time, as emergency situations may dictate.
- Feature control: IT can either block or enable the audio and video features of IM, and file transfer per file type.



Zone Labs' point-and-click interface allows IT to easily enable and disable specific IM features.

### Detailed Reporting and Easy Management

To help IT best understand and manage enterprise IM traffic, Zone Labs' comprehensive reporting provides in-depth and configurable reporting per time period and user or groups of users, including:

- Who uses IM and who uses it most heavily
- Security events
- Features used
- Match corporate ID to IM IDs
- Services, clients and versions used

Zone Labs' reporting also gives actionable insight into IM use for security and HR policy enforcement and network planning. For example, administrators can disallow use of specific client versions upon discovery of vulnerabilities.

To ensure ongoing security, a security log records IM security events as they occur for review from a centralized, configurable location. This keeps IT informed about security events occurring on users' PCs and records IM activity for forensic purposes. Because Integrity IM Security is fully integrated into the Integrity Management Console, it offers the same level of easy, centralized management.

### The Proactive Protection Your Enterprise Needs, Now

As IM's popularity rises, so do the risks associated with enterprise usage. Integrity IM Security mitigates the security challenge posed by public IM services, offering essential, comprehensive endpoint security. With Zone Labs, IM can help productivity soar without exposing the enterprise to IM-borne threats, using a range of enforcement options. And because Zone Labs' IM Security solution seamlessly integrates with Integrity, IT can rest assured knowing that maximum IM security can be quickly implemented and easily managed – a win-win for both users and the IT department.

### Client System Requirements

Integrity IM Security is a product module of Zone Labs Integrity that integrates seamlessly and is priced separately. Client system requirements include:

- Compatible with Microsoft® Windows® 98/NT4.0/2000 and XP
- IBM PC or 100% compatible
- Pentium II processor 233 MHz (450 MHz or higher recommended)
- 32 MB RAM (128 MB or higher recommended)
- 10 MB Hard disk space

### Instant Messaging Client Support

- AOL Instant Messenger (as supported in AIM version 4.3 or later)
- Yahoo! Messenger (as supported in Yahoo! Messenger version 5.0 or later)
- MSN Messenger (as supported in MSN Messenger 5.0 or later or Windows Messenger 4.7 or later)
- ICQ (as supported in ICQ Pro 2003b and ICQ Lite, build 1302)
- IRC (as supported in mIRC 6.14)
- Third party clients such as Trillian that access the above services
- Integrity version 4.5 or later is required, client and server

### Availability and Pricing

IM Security for Integrity is available as an Integrity module. If you would like to add IM Security to your existing Integrity implementation, or would like to license both products, please contact your Zone Labs enterprise sales team at **1-877-876-4960 (option 1)**, or please complete our contact form at [www.zonelabs.com/imsecuritysales](http://www.zonelabs.com/imsecuritysales)

---

#### **US Headquarters**

Zone Labs, Inc.  
475 Brannan Street  
Suite 300  
San Francisco, CA 94107  
tel 415.633.4500  
fax 415.633.4501

#### **European Headquarters**

Zone Labs, GmbH  
Frankfurter Str. 181 a  
63263 Neu-Isenburg,  
Germany  
tel +49.6102.36689.0  
fax +49.6102.36689.99

[www.zonelabs.com](http://www.zonelabs.com)

© 2004 Zone Labs. All rights reserved. IMsecure, TrueVector, ZoneAlarm and Zone Labs are registered trademarks of Zone Labs. The Zone Labs logo, Zone Labs Integrity and Cooperative Enforcement are trademarks of Zone Labs L.L.C. Zone Labs Integrity protected under U.S. Patent No. 5,987,611. Reg. U.S. Pat. & TM Off. Check Point is a trademark of Check Point Software Technologies Ltd. All other trademarks are the property of their respective owners. v.06.18.04



A Check Point Company

