

Zone Labs Integrity Desktop

Product Sheet



In today's security-conscious enterprise, protecting the network at its most vulnerable entry point – endpoint PCs – is an absolute must. But at the same time, overburdened IT departments need a solution that keeps management overhead as low as possible. With Zone Labs Integrity™ Desktop your IT organization can secure all local, remote and mobile PCs, dramatically reducing the risk of today's most vexing vulnerabilities – rapidly mutating and proliferating worms, hacker attacks, Trojan horses, spyware and other malware – while maintaining business continuity. And you can do so with minimal IT resources, because Integrity Desktop gives end users the flexibility to adjust their end point security to suit their environment.

Market Leading Endpoint Security for Enterprise PCs

Leveraging the award-winning ZoneAlarm® Pro security technology is used by 25 million PC users, Integrity Desktop offers a wide range of capabilities for end users and administrators alike. For organizations that choose to allow end-users to configure the application, Integrity Desktop includes a configuration wizard, an easy-to-understand tutorial, and advanced context-sensitive help to speed users' familiarity and productivity.

Alternatively, administrators can deploy an initial configuration that individual users can update in order to respond to their changing risk profile. IT can also configure Integrity Desktop to download policy updates automatically at scheduled intervals.

Finally, if the administrator wishes, Integrity Desktop can be “locked down” after it's deployed. This provides fast, consistent baseline security that cannot be altered or disabled, even by end users with administrative privileges on the endpoint.

Proactive Protection with Best-of-Breed Capabilities

Integrity Desktop is a multi-layered endpoint security solution that provides a highly secure, proven and proactive defense against malicious activity including hacker attacks on enterprises. Its “always-on” tamper-proof protection stops known and unknown threats through:

- ▶ A stateful firewall with stealth technology that makes PCs completely invisible to hackers, and block unsolicited inbound traffic. To provide the utmost in protection, Integrity regards all unsolicited inbound traffic as “untrusted”.
- ▶ Trusted and Internet Zones that allow administrators to reduce risk by controlling how, when and with which resource endpoints can communicate, based on “zones.” The Trusted Zone contains traffic destinations that are known and trusted, such as the public IP address of a VPN concentrator, or the private subnets and IP ranges of the corporate LAN and DNS servers. The Internet Zone covers all traffic sources, outside or inside the perimeter firewall, which are in not in the Trusted Zone.



A Check Point Company

- ▶ Application privilege control that prevents unauthorized and malicious applications from capturing and sending enterprise data to hackers. Application control prevents Trojan horses, spyware and other malicious code from trafficking enterprise data by restricting network access to only approved applications.
- ▶ Instant Messaging protection that guards endpoint PCs by blocking dangerous IM transmissions. Whether your users access public IM services such as AOL, Yahoo, MSN or ICQ using native or third-party clients, Integrity Desktop's optional IM Secure Pro companion application encrypts instant messages, filters content, controls usage and blocks unsolicited communication, as well as reporting usage and events.

Integrity Desktop also provides numerous security advantages that no other endpoint security offering can match. These include:

- ▶ Expert firewall rules that allow qualified end users to define perimeter firewall type port, protocol, source, destination and time of day rules. An expert rule can govern all communications, or communication to and from an individual application. This gives security-savvy end users and security administrators precise control over their endpoint security.
- ▶ Personal email protection that guards against potentially harmful attachments and SMTP mailers used by many worms. Integrity's MailSafe capability finds and quarantines more than 45 potentially harmful types of attachments. MailSafe stops email-borne viruses even before anti-virus updates are available, and prevents viruses from hijacking email address books and propagating themselves.
- ▶ User spoofing protection that prevents simulated keyboard or mouse input designed to disable endpoint security or grant network access to malicious applications. Other endpoint firewall products are susceptible to user spoofing; Integrity Desktop stops it immediately.

Security Policy Enforcement through VPN Integration

Through Cooperative Enforcement™ technology, Integrity Desktop provides policy enforcement in conjunction with virtual private network (VPN) gateways from Check Point Software Technologies, Cisco Systems, Nortel Networks, Aventail,

Neoteris and other leading providers. Cooperative Enforcement integrates Integrity Desktop with VPN gateway products to ensure that endpoint security is in effect before a user is granted remote access to an enterprise's internal network. It also verifies that the endpoint is protected by Integrity Desktop throughout the remote access session.

Easy Management for Both IT and End Users

Integrity Desktop's endpoint security is optimized for end user manageability, but can also be easily configured and updated by IT administrators. To streamline software installation, Integrity Desktop employs the MSI standard to minimize the time and effort to deploy Integrity to end users. It can also be deployed using network management systems such as Tivoli, SMS and HP OpenView.

Basic central management capabilities are available in command-line mode and include functionality such as configuring software, periodic security policy updated and centralized event log collection.

From an end user's perspective, Integrity Desktop offers award-winning usability with features that include:

- ▶ A user-friendly tabbed panel for each group of protection settings – firewall, application privilege control, email protection, and alerts and logs. Integrity Desktop provides intuitive, at-a-glance access to any policy element the employee needs to set or modify.
- ▶ Educational alerts with configurable sensitivity and explanations that maintain employees' productivity and reduce help desk calls.
- ▶ Automatic detection of wired and wireless networks and their MAC addresses, to help mobile employees set the right rules for the different types of networks they connect to.
- ▶ Automatic VPN detection and configuration that applies appropriate settings the first time a user attempts a remote access connection, enabling trouble-free remote access and eliminating the need for end users to make VPN configuration decisions.
- ▶ Privacy and productivity features, such as blocking ads, cleaning caches, and controlling cookies, to further help end users derive the maximum protection from Integrity Desktop.

Integrity Desktop software can be easily upgraded to Zone Labs' centrally managed client applications, Integrity Agent and Integrity Flex – without changing client software. Integrity Agent offers maximum, centralized control and can be completely transparent to the end user and, while Integrity Flex offers the same features and functionality of Integrity Agent it also allows end users to manage security when they're disconnected from the enterprise network. As your organizational needs change, Integrity Desktop adapts to your new requirements.

Only Zone Labs Delivers Total Access Protection

Together, Integrity's client-based and clientless options deliver Total Access Protection for the enterprise – an industry first from Zone Labs. With Total Access Protection, all enterprise network endpoints – employee and guest PCs, remote and local PCs, wired and wireless PCs – can be protected by Zone Labs' market-leading security solutions.

Proven Leadership: Zone Labs

Zone Labs, a Check Point Company, is the recognized leader in enterprise endpoint security. Today, Zone Labs Integrity, proven in more than 1100 enterprises worldwide, provides the most secure defense for endpoint PCs and enterprise data in today's highly vulnerable networked environments. For more information, please visit www.zonelabs.com.

System Requirements

- Compatible with Microsoft® Windows® 95, Microsoft® Windows® 98/NT4.0/2000, OSR2, 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

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

© 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. v06.18.04



A Check Point Company



We Secure the Internet.