

Zone Labs Integrity



Product Sheet

Proactive Security for the Enterprise

Every PC accessing your enterprise network is a target for rapidly proliferating worms, penetration attacks, Trojan horses, spyware, and other exploits. Reactive, signature-dependent technologies such as anti-virus and intrusion detection can no longer be trusted to stop the newest variations of these threats.

Zone Labs® Integrity™ safeguards enterprise networks from penetration by malicious code or targeted attacks with its combination of proactive protection for every network endpoint along with central policy management and enforcement. Pre-defined policy templates, an intuitive Web-based management interface, and the most trusted PC firewall and application privilege controls let administrators quickly and easily develop, manage, and enforce unparalleled endpoint security. In essence, Integrity restores the confidentiality, integrity, and availability of enterprise data and critical systems without compromising IT or end user productivity.

Even the best PC security will leave a control gap if it fails to protect every form of network access. That's why the Integrity product line delivers Total Access Protection for the enterprise – an industry first from Zone Labs. With Total Access Protection, all enterprise network endpoints – employee and guest, remote and local, wired and wireless – can be protected by Zone Labs' market-leading security solutions.

Product Highlights

Most secure	Allows communication only by trusted applications, proactively stops worm propagation, and prevents hackers from discovering assets and exploiting open ports.
Easy management	Through its intuitive management interface, reusable policy elements, and predefined policy templates, Integrity streamlines and simplifies endpoint security management.
Assured Enforcement	Enforces compliance with policy requirements - such as up-to-date antivirus, patches, and applications – before granting network access.
Greatest scalability	Supporting the largest enterprises at the lowest TCO, Integrity scales to accommodate up to 75,000 simultaneously connected users per server.
Broadest integration	Integrity integrates with all the leading user directories and anti-virus products, as well as hundreds of VPNs, switches, and wireless access points.
Most flexible	With three security clients that can be used in any combination or on their own, Integrity delivers the flexibility that today's enterprises demand.



A Check Point Company

Best of Breed Security

Integrity enforces security on multiple levels to provide proactive, “always-on,” tamper-proof protection that stops known and unknown threats through:

- ▶ A stateful PC firewall that blocks all unsolicited inbound traffic, with stealth technology that makes PCs completely invisible to hackers.
- ▶ Application privilege control that prevents malicious software from capturing and sending ID’s, passwords, and confidential data to hackers.
- ▶ Email protection that guards against harmful attachments and address book hijacking.
- ▶ Optional Integrity IM Security that secures employee use of public instant messaging (IM) services.

Proactive Security Model

After installing Integrity, administrators can define and deploy a baseline security policy to PCs within minutes. This initial policy requires little configuration yet provides immediate endpoint firewall protection for the organization. Integrity also provides extensive controls for fine-tuning policies to the unique needs of the enterprise over time. For ultimate protection, Integrity can treat all network traffic and applications as untrusted unless stated otherwise by the security policy. This approach stops any malicious application, known or new, from compromising data confidentiality or business continuity.

Integrity allows administrators to control how, when and with which resources PCs can communicate, based on three network “zones” with varying levels of trust. The Blocked Zone stops any and all communication to or from specified network addresses. 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, that are in neither the Trusted Zone nor the Blocked Zone. Using traditional firewall rules, administrators can also create custom zones within the enterprise network and apply different levels of security to each. Such network segmentation contains worm outbreaks and enables very granular application of “least privilege” access to network resources.

A single Integrity firewall rule can filter endpoint traffic based on both source and destination, port, protocol, and time of day. Administrators can apply a rule to all endpoint communications, or to an individual application or group of applications. This powerful option enhances administrators’ ability to control which users can access specific resources securely. Rules are also reusable across multiple policies, reducing the time spent applying updates and managing exceptions.

Application Privilege Control

Application privilege control prevents Trojan horses, spyware, backdoors, and other malicious code from compromising the confidentiality of enterprise data. Integrity lets administrators specify which PC applications are allowed network access, which are not, and how to handle unrecognized programs.

The screenshot shows the Integrity Policy Studio interface. At the top, it displays the administrator's name (Super Administrator), login time (2003-12-04 11:34:33), and duration (0:04:58). The main area is titled "POLICY STUDIO: Classic Firewall Rules" and shows a table of rules for the "fw_vpn" policy. The table has columns for Rank, Name, Source, Destination, Protocol, Time, Action, and Track. Below the table are buttons for ADD, EDIT, REMOVE, ENABLE, and DISABLE. At the bottom, there are buttons for CANCEL, DELETE, and a text input for "New Policy Name", along with COPY and DEPLOY POLICY buttons. The footer includes the version (4.5.000.0), powered by TrueVector, and copyright information (© 2000-2003 Zone Labs, Inc.).

Rank	Name	Source	Destination	Protocol	Time	Action	Track
1	All traffic	Any	Any	IP_EVERY	Any	Allow	None
2	Allow Web	Any	Any	IP_TCP	Any	Allow	None
3	Allow Mail	Any	Any	IP_TCP	Any	Allow	None
4	Allow DSN	Any	Any	IP_TCP IP_TCP_UDP	Any	Allow	None
5	Allow DHCP	Any	Any	IP_UDP	Any	Allow	None
6	Allow DB	Any	Any	IP_TCP	Any	Allow	None
7	Block_all	Any	Any	IP_EVERY	Any	Block	Alert & Log

Integrity gives administrators the flexibility to fine tune security policies using classic firewall rules.

Integrity's Zones

Zone	Description
Trusted Zone	Sources and destinations you trust
Blocked Zone	Sources and destinations you don't want endpoints communicating with.
Internet Zone	Sources and destinations you have not placed in either the Trusted Zone or Blocked Zone.

Integrity's Program Observation feature automatically creates an inventory of all PC applications that attempt network access, enabling fast, efficient identification and securing of potential network vulnerabilities.

Integrity application control can be implemented using firewall rules or application privilege rules. As with Integrity's firewall rules, administrators can apply different application privilege rules in the Trusted and Internet zones. For example, an application may be allowed to accept inbound connections from the Trusted Zone but not the Internet.

Integrity prevents even sophisticated attempts to subvert its application protections. Application component control ensures that all DLLs, OCXs, and other components used by a trusted application are authenticated based on their MD5 checksums. Application spoofing protection provides an additional layer of security, validating application identity with "known good" MD5 checksums. Integrity also prevents malware from using a trusted application such as Internet Explorer – or even a chain of trusted processes – to send confidential data out to the Internet.

Email and Instant Messaging Protection

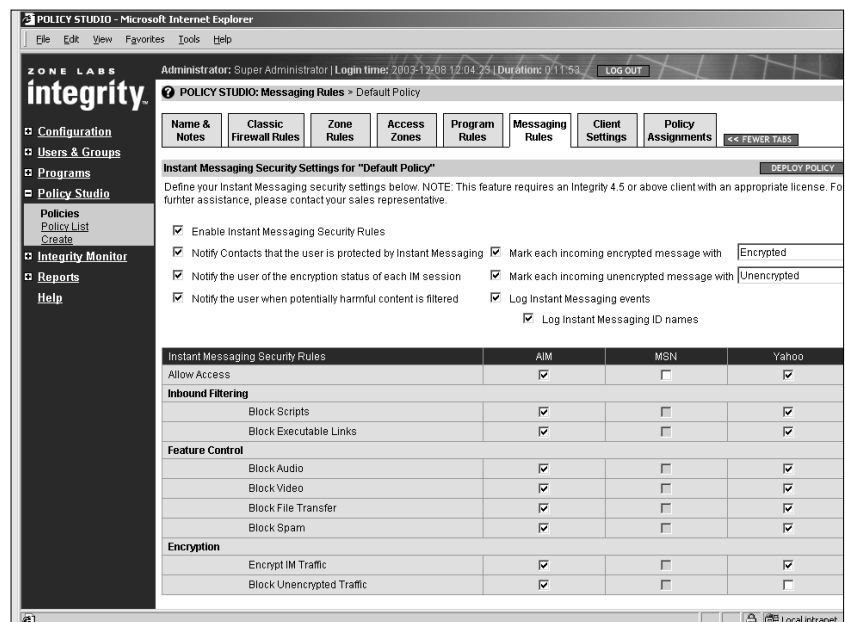
Email and Instant Messaging are an integral

and valuable part of enterprise communications. In fact, IM is now the most rapidly growing method of Internet communications. The challenge is that email and IM are extremely vulnerable to exploitation by hackers or malware.

Integrity provides automatic protection for both technologies. Integrity's MailSafe capability monitors personal email messages retrieved from POP or IMAP servers, and finds and quarantines more than 45 potentially harmful types of attachments that could bypass enterprise antivirus mechanisms.

In fact, MailSafe stops email-borne viruses even before anti-virus updates are available, and prevents viruses from hijacking email address books and propagating themselves.

Through its optional IM Security module, Integrity also lets enterprises enjoy the productivity benefits of public IM while mitigating the security risks. When employees access IM services such as AOL, Yahoo, MSN or ICQ using native or third-party clients, Integrity IM Security enables central management of message encryption, content filtering, usage controls, and unsolicited communication blocking, as well as usage and event reporting.



The optional Integrity IM Security module enables IT managers to centrally manage security policies that protect the network while enabling productive instant messaging.

Easy to Manage

Integrity features an extensible client/server architecture that's fully compatible with existing network IT infrastructures and integrates with industry-standard hardware, software, and networks. The web-based management console provides intuitive management tools for policy creation, management, and deployment.

Rapid Client Configuration and Deployment

Integrity lets administrators create downloadable, pre-configured software packages to quickly and easily install new and upgraded Integrity client software, with little or no end-user involvement. Integrity employs the MSI standard to minimize the time and effort to deploy Integrity to end users. Upon installation, Integrity clients connect to the management server and receive a baseline policy. Administrators can quickly and easily configure this initial security policy using predefined "best practice" policy templates.

Once deployed, Integrity's agents can operate in the background, leaving employees free to concentrate on their work. The Integrity Flex client option provides additional flexibility, ensuring that users adhere to corporate policy while on the corporate network, while allowing them to control their security settings when disconnected from it. All Integrity clients offer Total Client Lockdown, which ensures that PC security and policy enforcement cannot be altered or disabled even by end users with local administrative privileges.

Simplified Policy Management

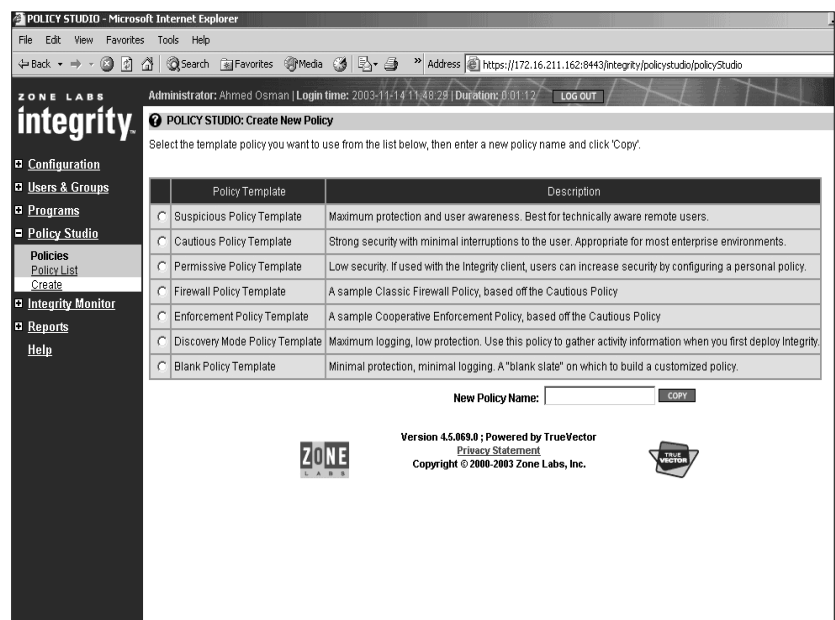
Integrity was specifically designed to minimize the time needed to manage security policies. For example, administrators need only create a reusable policy element once and assign it to multiple policies. When the policy element is changed, Integrity automatically updates all associated policies and pushes them to all affected clients within seconds. Integrity also

simplifies application control management by letting administrators apply a set of rules to groups of related programs.

While Integrity provides optimum usability, it also offers an array of powerful policy management tools. Administrators can choose to define distinct policies that are automatically applied to endpoints as they move between networks, locations, and users. Integrity can dynamically assign a policy based upon a user's IP connection address, user group or role, type of gateway (such as a VPN, switch, or wireless access point), or even a combinations of these criteria. To guarantee protection for every endpoint, Integrity assigns a basic default policy for unrecognized users.

Integrity offers several administration tiers, including a read-only role that gives selected Integrity Server users the ability to view any screen but not edit or deploy policies, or make other changes. This lets support staff troubleshoot endpoint issues without being allowed to make unauthorized policy decisions. Integrity also assures high availability with server failover support that automatically shifts security monitoring and enforcement to a back-up server if needed.

Actionable Monitoring and Reporting



Predefined policy templates allow immediate endpoint protection across the enterprise with just a few clicks.

The Integrity Monitor presents the real-time, graphical status of all connected Integrity clients. Integrity's reporting capabilities provide both broad and detailed analytic insight into endpoint events. In conjunction with Crystal Reports, Zone Labs allows administrators to view an extensive suite of filterable activity reports that provide graphs and granular detail on application usage, users with the most security alerts, policy compliance violations, and more.

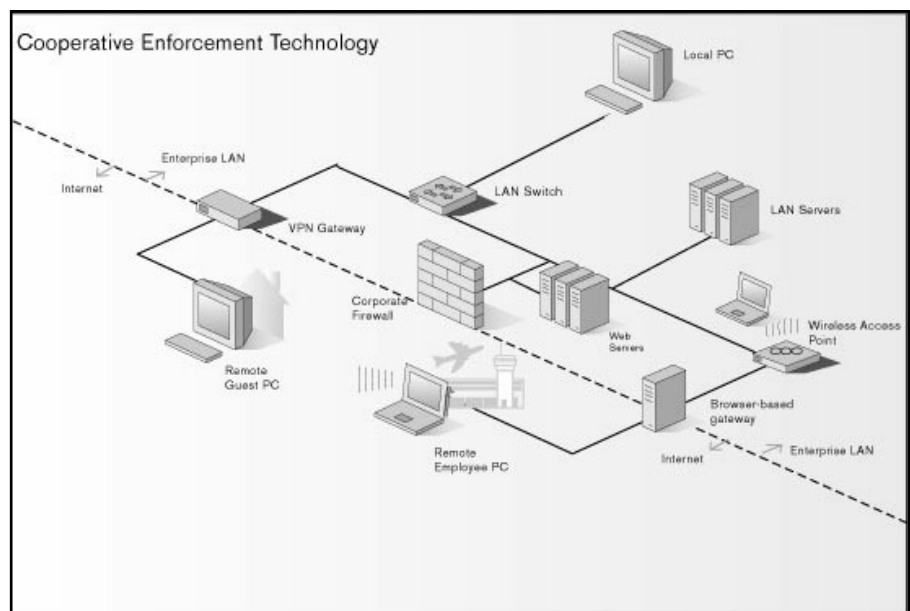
Assured Policy Compliance

Integrity lets an enterprise define and enforce a secure state on every PC that connects to its network. By enforcing a comprehensive security policy as a condition of network access, Integrity delivers highly effective protection against the newest worm and virus infections, spyware, Trojan horses, and other exploits that compromise security and business continuity.

Integrity can ensure that a PC is running updated antivirus, has critical patches and service packs installed, has the latest versions of applications such as browsers and VPN clients, is not running any prohibited programs, has specified registry keys present, and meets other trust criteria before it gains authorized access to the network. If an endpoint violates any of these rules, Integrity restricts network access to customizable remediation resources providing end user guidance and downloadable updates. As a result, both end user and IT productivity are maintained while the network is secured.

To control network access, Zone Labs' unique Cooperative Enforcement™ technology integrates Integrity with the broadest range of VPNs, switches, routers, and wireless

access points from Check Point, Cisco, Nortel, Avenail, Neoteris, Enterasys, Foundry, and many other networking leaders. In fact, Integrity integrates with more than 200 network access devices that support the industry standard 802.1x Extensible Authentication Protocol. By supporting the non-proprietary, IEEE definition of the EAP standard, Integrity enables uniform policy enforcement enterprise-wide with whatever networking equipment a customer chooses. Consequently, Integrity customers are not locked into one vendor's proprietary implementation.



Integrity checks each endpoint for compliance with all policy requirements including anti-virus updates, patches, and registry keys. Out of compliance endpoints are quarantined until users remediate violations.

For enterprises that have not yet upgraded to 802.1x-compliant LAN equipment, Integrity can also enforce network access policies without requiring gateway integration. Because Total Client Lockdown ensures that Integrity clients cannot be tampered with or disabled, the standalone approach to policy enforcement is a viable option for Integrity administrators.

Policy Enforcement Without Client Software

Until recently, enterprises had limited ability to mitigate the risks posed by guess PC access to their networks. Administrators lacked the authorization or resources to install security software on those endpoints even though they have the same vulnerabilities as IT-controlled PCs. Integrity Clientless Security addresses this exposure by enforcing baseline security requirements and disabling spyware on both guest and employee endpoints that seek access to an enterprise's Web-based gateways and applications. The same network access rules enforced by Integrity client-based solutions can now be enforced without the need for IT to install client software.

Together, Integrity's client-based and clientless options deliver the Total Access Protection that ensures all enterprise network endpoints – employee and guest, remote and local, wired and wireless – comply with all network access requirements.

Low Total Cost of Ownership

The ability of Integrity to integrate with the broadest range of network hardware and software allows enterprises to increase the rate of return on their prior technology investments. In addition to extensive gateway integration, Integrity automatically synchronizes with and supports group structures imported from directories and authentication systems based on NT Domain, Microsoft Active Directory, RADIUS, LDAP, and RSA SecurID, minimizing the time that staff spends maintaining Integrity groups. It also integrates with the most common database management systems, including Microsoft SQL Server 2000 and Oracle 9i.

Integrity synchronizes with leading anti-virus products to ensure that policy enforcement rules are always up-to-date. From a reference PC it can automatically gather signature file updates for Symantec, McAfee, Trend Micro, Computer Associates or Sophos anti-virus products and immediately deploy new policies requiring end users to install the updates. This unique Integrity benefit virtually eliminates administrative time to manually gather and update policy data.

Each Integrity Server supports up to 75,000 concurrently connected users. For smaller implementations, Integrity Server Workgroup Edition provides the simplest, fastest, and lowest TCO deployment, supporting up to 1,000 users with a

Feature	Integrity Agent	Integrity Flex	Integrity Desktop
Proactive endpoint security, including a stealthing, stateful firewall, advanced application control, and optional instant messaging security	X	X	X
Remote access denied if Integrity client is not running	X	X	X
LAN and remote policy enforcement of up-to-date anti-virus, patch, and other policy requirements	X	X	
Central GUI management and monitoring of enterprise policies	X	X	
Highly scalable, highly available management server	X	X	
Command line configuration tools			X
End user GUI help resources		X	X
On-network and off-network security policies		X	

built-in database that eliminates third party database and integration costs.

Centralized & Decentralized Management Options

Integrity clients offer a comprehensive and flexible range of endpoint security management options for the enterprise. The three unique security clients – Integrity Agent, Integrity Flex, and Integrity Desktop – are compatible and can coexist within the same enterprise to meet different user needs.

Integrity Agent affords maximum, centralized IT control over endpoint security policies that can be completely transparent to end users. Ideal for organizations that want to apply consistent security policy across non-technical user populations, Integrity Agent is centrally managed through the Integrity Server management console. Administrators can choose to enforce their Integrity Agent policies only when the PC is connected to enterprise network, or at all times.

Integrity Flex provides all of the features and functionality of Integrity Agent, and adds the ability for end users to manage their own security policy when they're not connected to the enterprise network. It enforces administrator-defined policy

transparently when the user is connected to the enterprise, just like Integrity Agent. When mobile employees are disconnected from the enterprise and need to access other networks, such as customer LANs or home networks, Integrity Flex provides an intuitive GUI that allows them to easily make any adjustments needed to use other networks' resources while maintaining the security of their PC.

Integrity Desktop is a decentralized, standalone solution that lets end users control their PC security environment – perfect for technically savvy end users who have the ability to determine their security policies, and in situations where IT does not have the resources or charter to centrally manage the endpoint.

Leveraging the award-winning security technology that over 30 million ZoneAlarm users depend on, Integrity Desktop offers end users a simple and intuitive interface for adjusting security settings. Like the other clients, Integrity Desktop can be deployed via network management systems such as SMS, Tivoli, and HP OpenView or by using installation scripts. Basic Integrity Desktop management capabilities are available in command-line mode and include the ability to pre-configure the software, periodically update end user policies, and centrally collect end user event logs.

For companies that don't want users to adjust IT security policy, administrators can lock down Integrity Desktop and its policy, providing fast, consistent baseline security that cannot be altered by end users.

Integrity Server

Hardware Specifications

- Intel Pentium III (600MHz) or greater
- Installer requires at least 256 color video

We strongly recommend running Integrity Server and the associated database server on separate host computers.

Physical Memory and Disk Space

Concurrent Connections	RAM	Disk Space
up to 500	512 MB	80 MB
up to 2000	1 GB	80 MB
up to 5000	2 GB	80 MB
up to 20,000	2 GB	80 MB
over 20,000	contact sales rep	contact sales rep

Operating Systems

- Windows 2000 server (SP4) and Advanced Server (SP4)
- Windows Server 2003

Browsers

- Internet Explorer 6 and above
- Netscape Navigator 7 and above

Database Management Systems

- Oracle 9iR2 with Oracle thin JDBC driver version 1.2
- Microsoft SQL Sever 2000 (SP3) with Microsoft SQL Server 2000 Driver for JDBC SP1

JDBC drivers must be downloaded from the vendor Website prior to installing Integrity Server.

We strongly recommend running Integrity Server and the associated database server on separate host computers.

Database Server Hardware

Concurrent Connections	RAM	Disk Space
up to 500	512 MB	1 GB
up to 2000	1 GB	2 GB
up to 5000	1 GB	6 GB
up to 20,000	1 GB contact sales rep	8 GB contact sales rep
over 20,000		

This table lists required memory and disk space for a database running as a stand-alone server.

Integrity Agent and Integrity Flex

Workstation Hardware Specifications

	Optimal	Minimal
Processor	Pentium II 450 MHz	Pentium II 233 MHz
RAM	128 MB	32 MB
Disk Space	10 MB	10 MB

We strongly recommend running Integrity Server and the associated database server on separate host computers.

Operating Systems

- Server 2003, XP Pro, 2000 Pro SP4
- NT 4.0 Workstation SP6a, 98 SE, 95 OSR2*
- XP Professional
- Windows 2000

* requires Internet Explorer 5 or above

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, Inc. All rights reserved. Zone Labs, TrueVector, ZoneAlarm, and Cooperative Enforcement are registered trademarks of Zone Labs, Inc. The Zone Labs logo, Zone Labs Integrity and IMsecure are trademarks of Zone Labs, Inc. Zone Labs Integrity protected under U.S. Patent No. 5,987,611. Reg. U.S. Pat. & TM Off. Cooperative Enforcement is a service mark of Zone Labs, Inc. All other trademarks are the property of their respective owners. v.04.21.04



A Check Point Company



We Secure the Internet.