



Integrity Desktop

Preemptive endpoint security

YOUR CHALLENGE

Endpoint PCs—local, remote, and mobile—access your network to do work and keep your business running. At the same time, they open up your business to vexing vulnerabilities such as rapidly mutating and proliferating worms, hacker threats, Trojan horses, spyware, and other malware. You need a solution that protects your endpoints, while at the same time keeps IT management overhead as low as possible.

OUR SOLUTION

Based on ZoneAlarm®—the world's most trusted personal firewall—Check Point Integrity™ Desktop is a standalone desktop firewall solution for enterprise endpoint PCs. For organizations that choose to allow end-users to handle desktop security, Integrity Desktop includes a configuration wizard, an easy-to-understand tutorial, and advanced context-sensitive help to speed user familiarity and productivity.

Administrators can deploy an initial policy configuration that end-users can update to respond to their changing risk profile. Integrity Desktop can also be “locked down” after it is deployed. This provides fast, consistent, baseline security that cannot be altered or disabled, even by end-users with administrative privileges on the endpoint.

Most trusted endpoint protection

Integrity Desktop is a multilayered endpoint security solution that provides a highly secure, proven, and proactive defense against malicious activity including hacker attacks on enterprises. Its “always-on,” tamperproof protection stops known and unknown threats with the following:

Stateful inspection firewall with stealth technology—makes PCs completely invisible to hackers and blocks unsolicited, untrusted inbound traffic.

Integrated anti-spyware—as an add-on option, Integrity Anti-Spyware detects and removes spyware to protect endpoints from financial damage caused when spyware steals or exposes data and increases helpdesk expenses by harming PC performance. Based on real-time data from millions of PCs, it defeats thousands of spyware programs. Detailed logging enables monitoring of spyware trends.

Application privilege control—prevents unauthorized and malicious applications from capturing and sending enterprise data to hackers.

Trusted and Internet Zones—allows administrators to reduce risk by controlling how, when, and with which resources endpoints can communicate. The Trusted Zone contains traffic destinations such as the public IP address of a VPN concentrator or the private subnets and IP ranges of the corporate LAN and DNS

PRODUCT DESCRIPTION

Check Point Integrity™ Desktop delivers preemptive protection against the latest worms, viruses, spyware, and hacker attacks.

PRODUCT FEATURES

- Most trusted endpoint protection
- Integrated anti-spyware
- Remote access policy enforcement
- Simple end-user administration
- Privacy and productivity enhancing tools

PRODUCT BENEFITS

- Provides the most secure protection against hackers
- Detects, quarantines, and removes spyware
- Offers trouble-free remote access
- Minimizes administration overhead
- Increases end-user manageability and productivity



Intelligent Security

Check Point protects every part of your network—perimeter, internal, Web—to keep your information resources safe, accessible, and easy to manage.

servers. The Internet Zone covers all traffic sources outside or inside the perimeter firewall that are not in the Trusted Zone.

Instant messaging (IM) security—blocks dangerous IM transmissions, whether your users access public services or ICQ. As an add-on option, Integrity IM Security encrypts instant messages, filters content, controls usage, and blocks unsolicited communication.

Unique security advantages

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

Expert firewall rules—allow qualified end-users to define perimeter firewall port, protocol, source, destination, and time-of-day rules. An expert rule can govern overall communications or communications to and from specific applications. This gives security-savvy end-users and security administrators precise control over their endpoint security.

Personal email protection—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 antivirus updates are available and prevents viruses from hijacking email address books and propagating themselves.

User spoofing protection—prevents simulated keyboard or mouse input designed to disable endpoint security or grant network access to malicious applications.

Remote access policy enforcement

Through Cooperative Enforcement® technology, Integrity Desktop provides policy enforcement in conjunction with leading VPN gateways. Cooperative Enforcement ensures that endpoint security is in effect before a user is granted remote access to an enterprise's internal network. It also verifies that Integrity Desktop protects the endpoint throughout the remote access session.

Simple end-user administration

Integrity Desktop is optimized for end-user manageability and offers award-winning end-user usability features:

- User-friendly, tabbed panels for each group of protection settings—firewall, application privilege control, email protection, and alerts and logs
- Educational alerts with configurable sensitivity and explanations
- Automatic detection of wired and wireless networks and their MAC addresses
- Automatic VPN detection and configuration that applies appropriate settings the first time an end-user attempts a remote-access connection
- Privacy and productivity features, such as ad blocking, cache cleaning, and cookie control

Integrity Desktop can be easily upgraded to our centrally managed Integrity client. As your organizational needs change, Integrity Desktop adapts to your new requirements.

Total Access Protection

Integrity Desktop is an important pillar of Total Access Protection, under which the full spectrum of enterprise Windows PC users—employee and guest, remote and internal, wired and wireless—can be protected by Check Point's market-leading security solutions.

SYSTEM REQUIREMENTS

Minimum hardware specifications

<i>Processor</i>	Intel Pentium II 450 MHz
<i>RAM</i>	256 MB
<i>Disk space</i>	30 MB

Operating systems

- Windows XP Pro (SP2)
- Windows 2000 Pro (SP4)

©2005 Check Point Software Technologies Ltd. All rights reserved. Check Point, Application Intelligence, Check Point Express, the Check Point logo, AlertAdvisor, ClusterXL, Cooperative Enforcement, ConnectControl, Connectra, CoSa, Cooperative Security Alliance, Eventia, Eventia Analyzer, Eventia Reporter, FireWall-1, FireWall-1 GX, FireWall-1 SecureServer, FloodGate-1, Hacker ID, IMsecure, INSPECT, INSPECT XL, Integrity, InterSpect, IQ Engine, Open Security Extension, OPSEC, Policy Lifecycle Management, Provider-1, Safe@Home, Safe@Office, SecureClient, SecureKnowledge, SecurePlatform, SecuRemote, SecureXL Turbocard, SecureServer, SecureUpdate, SecureXL, SiteManager-1, SmartCenter, SmartCenter Pro, Smarter Security, SmartDashboard, SmartDefense, SmartLSM, SmartMap, SmartUpdate, SmartView, SmartView Monitor, SmartView Reporter, SmartView Status, SmartViewTracker, SofaWare, SSL Network Extender, Stateful Clustering, TrueVector, Turbocard, UAM, User-to-Address Mapping, UserAuthority, VPN-1, VPN-1 Accelerator Card, VPN-1 Edge, VPN-1 Pro, VPN-1 SecureClient, VPN-1 SecuRemote, VPN-1 SecureServer, VPN-1 VSX, VPN-1 XL, Web Intelligence, ZoneAlarm, ZoneAlarm Pro, Zone Labs, and the Zone Labs logo are trademarks or registered trademarks of Check Point Software Technologies Ltd. or its affiliates. All other product names mentioned herein are trademarks or registered trademarks of their respective owners. The products described in this document are protected by U.S. Patent No. 5,606,668, 5,835,726, 6,496,935, 6,873,988 and 6,850,943 and may be protected by other U.S. Patents, foreign patents, or pending applications.

November 2, 2005 P/N 501929

Worldwide Headquarters
3A Jabotinsky Street, 24th Floor
Ramat Gan 52520, Israel
Tel: 972-3-753-4555
Fax: 972-3-575-9256
Email: info@checkpoint.com

U.S. Headquarters
800 Bridge Parkway
Redwood City, CA 94065
Tel: 800-429-4391; 650-628-2000
Fax: 650-654-4233
www.checkpoint.com



Check Point®
SOFTWARE TECHNOLOGIES LTD.

We Secure the Internet.