



Check Point
SOFTWARE TECHNOLOGIES LTD.

We Secure the Internet.



White Paper

Winning Against Worms:

Combating Worms with Proactive Security



Intelligent Security

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

Contents

Introduction: The Changing Nature of Security	3
Increasing Security Demands on IT Departments	4
Limitations of Reactive Security Technologies	4
New Challenges of the Expanding Network Perimeter	5
A Better Approach: Proactive Internal and Endpoint Security	6
Port Vulnerabilities	7
Application Spoofing and Hijacking	7
Infected Email	8
Blended Threats	8
Propagation Within the Network	9
Attempts to Shut Down Security Applications	10
Integrity Enforces Security Policies on Endpoint PCs	10
Shifting from Crisis Management to Policy Management	11

Introduction: The Changing Nature of Security

Bagel, MyDoom, Netsky: A through Z. In 2004, IT administrators faced a relentless attack of worms and viruses, often with new variants popping up daily. This onslaught puts an end, once and for all, to the notion that you can protect your network simply by reacting to emerging threats. When software companies discovered vulnerabilities and issued patches months before hackers took advantage of the holes, attentive IT administrators could keep up with the threats and secure their networks. And when major viruses or worms emerged only every few weeks or months, frequently updating antivirus software and regularly running scans was a legitimate strategy.

But today, with exploit code sometimes following the discovery of software holes by a matter of days, waiting for threats to emerge is no longer a viable strategy. News reports in 2004 featured accounts of large commercial enterprises, airports, and even national defense agencies losing network availability for up to a week due to rapidly spreading worms. Businesses incurred major financial costs due to downtime, while the inability of government agencies to provide essential services clearly compromised their missions. This damage occurred despite the presence of antivirus software on virtually every PC (or network “endpoint”) in these enterprises.

While reactive technologies like antivirus are still an important component of your security arsenal, you also need proactive security that protects all systems on the network by anticipating and blocking attacks before they happen. A proactive strategy is necessary not only because virus and worm attacks are occurring more frequently, but also because the motivations of their creators have changed. Traditionally, a virus-writer’s desire was to win “geek cred” by unleashing code that spread far and fast throughout the Internet. Few of these viruses carried a payload designed to steal data or harm PCs and servers, although they did do damage by clogging Internet traffic and causing network downtime.

In the past two years, however, viruses and worms have become criminal tools. Some, such as the Badtrans and Orpheus worms, include keystroke loggers to steal passwords and other critical company information. Others, such as MyDoom, opened backdoors that allowed hackers to turn PCs into “Zombies” for relaying spam email, launching distributed denial of service attacks, or even for hosting illegal pornographic material—thus covering the tracks of the true perpetrators.

In addition to dealing with the administrative headaches of patching systems and removing infections from PCs, IT administrators now have to protect against data theft and the legal liabilities of having PCs hijacked for criminal activities. Furthermore, by constantly responding to crises, IT professionals have little or no time for long-term planning: testing and validating software patches or changing network configurations and architectures to improve security. Stable or declining IT staffing only exacerbates the problem, and redoubling efforts to keep up with threats only goes so far. Even working late hours and weekends may not suffice.

Increasing Security Demands on IT Departments

To understand just how much harder the IT administrator's job has become, consider a few key developments:

- The second-most widespread worm in history, Sobig.F, was intercepted over 33 million times by email security provider MessageLabs from its initial discovery in August 2003 to June 2004. Though impressive, Sobig.F is only a distant second to the biggest worm of 2004 (and of all time), MyDoom.A, which MessageLabs first discovered at the end of January 2004 and had already intercepted over 54 million times by June 2004.
- From December 2003 to January 2004, the total number of viruses MessageLabs intercepted per month increased roughly five-fold, from less than 5 million to just under 25 million. In February, that volume roughly doubled again to nearly 50 million.
- From February 15 to March 31, 2004, a significant new worm variant appeared nearly everyday.
- In addition to arriving more often, worms also appear earlier. In the case of the Slammer worm, 101 days elapsed between reporting of the vulnerability and discovery of the worm. For the Sasser worm, that lag had dropped to 19 days.

Limitations of Reactive Security Technologies

Clearly, the rapid evolution of security threats has permanently outpaced the ability of traditional security tools—such as virus scanning, software patching, and intrusion detection systems—to respond.

Thus, even with efficient update mechanisms, antivirus software on some systems will always be outdated due to the time lag in issuing new virus-detection files. This delay was documented in a recent study of reaction times done by the German firm AV-Test GmbH (www.av-test.org) and presented at the Virus Bulletin 2004 Conference.

Twenty-four global companies, including the top five market leaders, participated in the study, which recorded the times required to issue virus definitions for 45 outbreaks in 2004, including members of the infamous Bagle, MyDoom, Netsky, and Sasser families. The fastest response time for the first generation of a virus was under 1.5 hours for Bagle.A. But the slowest time for a major antivirus vendor for that same virus was over 20 hours. Furthermore, no single company consistently posted the fastest response times. Companies that were relatively fast for one threat were stragglers for others.

The response time weakness is compounded by another timing problem. Regardless of the speed with which vendors issue new virus definitions, a delay in updating some endpoints can result in a costly enterprise network infection. For example, a laptop taken home over the weekend can easily pick up a new worm during personal Internet surfing. The user's antivirus provider may issue a signature update over the weekend as well, but as soon as the laptop connects to the LAN on Monday morning the worm immediately propagates to all vulnerable hosts. The antivirus product's auto-update mechanism doesn't have a chance to install a new definitions file before the damage is done.

The AV-Test study also measured the ability of antivirus applications to identify infectors heuristically, before specific definition files were available, and the results were disappointing. Only one product was able to detect one first-generation virus using heuristics, and in the vast majority of cases, products needed specific signature updates even to catch the latest variants (the .b or .c versions) of known worms.

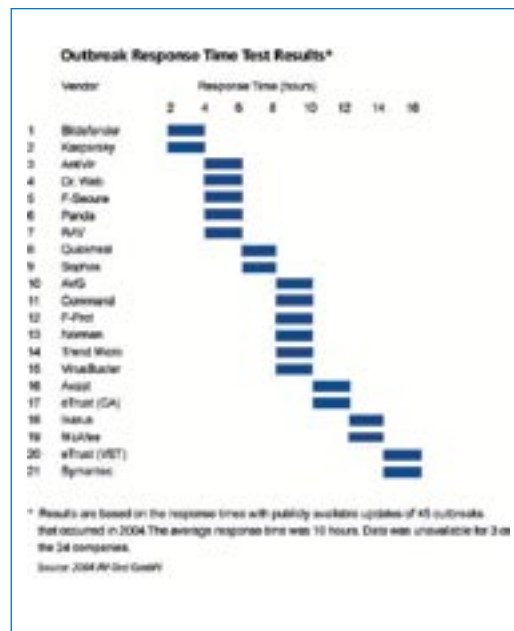
Similar response delays apply to operating system and application patches. In some cases, Microsoft has taken as long as nine months to provide a patch from the time that a vulnerability was reported to them.

And there is a further delay even after patches are issued, because IT administrators need to verify that the fix for one vulnerability doesn't introduce its own bugs. Due to the demand for a quick response, vendors write and issue patches rapidly, making them probably the least-tested pieces of software. While Microsoft may spend months or years doing quality assurance on a new version of Windows, it may write and release patches for the operating system in a matter of days. So to be safe, enterprises must conduct their own testing. This, plus the regular deployment process, can add several weeks to the response time for many enterprises.

Lastly, the inherent reactive nature of signature-based Intrusion Detection System (IDS) technology renders it powerless to prevent the damage caused by today's lightning fast attacks. And, many enterprises lack the IT staff needed to analyze the overwhelming volume of network IDS alerts and "false positive" alarms. Adding IDS logs from hundreds or thousands of network computers or "endpoints" only amplifies the problem.

New Challenges of the Expanding Network Perimeter

All these delays extend the time that your network is vulnerable to infection. Perimeter firewalls help by blocking ports used by known network worms. However, system administrators can't plug every hole, and newer communications programs create even more openings. The Web, for instance, is both an indispensable productivity tool and an open door to invaders (via port 80). Web sites can offer not only important information but also downloads that contain worms, backdoors, and Trojan horse applications. Employees can also allow worms onto the LAN via peer-to-peer networks and instant messaging applications.



Along with new inroads, today's network is more vulnerable because it extends beyond the traditional perimeter of the wired corporate LAN. Road warriors and telecommuters work outside the perimeter firewall (and gateway email scanners) and are vulnerable to infections that can make their way into the network when they bring in their laptops or log in remotely. Companies that offer wireless access to visiting clients and customers are susceptible to additional sources of infection.

A Better Approach: Proactive Internal and Endpoint Security

The reactive approach is doomed to fail. At best, it is a game of Russian roulette—hoping that the bullet of a virus or worm attack will miss your company and hit another, allowing you time to update every endpoint's antivirus definitions and install software patches before the infection comes around to you. At worst, it is an exercise in damage control—hoping you can spot the signs of an infection early on and limit its spread across your network.

It is far more effective to take a proactive approach. While it's impossible to know precisely what the next worm will look like and what it will do, it is possible to identify the types of vulnerabilities that worms may exploit and to guard against them.

For example, without knowing the details of the next email-borne worm, you can block it by controlling the kind of attachments that are allowed into your network and onto PCs. Without knowing exactly what port a worm may try to slither through, you can block it by only opening ports for use by known, trusted applications. And by automatically screening inbound PC traffic for malicious executable code, you can stop the buffer overflow and other attacks targeting the applications and operating systems of your network endpoints. Implementing and enforcing these policies not only on remote laptops but also on each PC that accesses your internal network allows you to extend your proactive strategy beyond the limitations of the perimeter to prevent users from bringing infections inside. And should an infection make its way into your network, the right internal security gateways and PC-based protection will limit its spread.

Check Point Integrity™ offers the essential elements of enterprise-wide, proactive protection against worms and other PC-directed attacks. It combines Check Point's award-winning stateful PC firewall with powerful central-management capabilities. Using Integrity, administrators can define and enforce security policies for each PC and ensure that only PCs in compliance with corporate policy are able to join the network.

For complete and seamless internal security, Integrity integrates with Check Point InterSpect™, the industry's first internal security gateway. InterSpect segments the internal network into organizational security zones. Combined with Integrity, InterSpect ensures that the latest worms cannot cross network segments, and infected PCs are quarantined until the threat is removed. They also ensure that every PC that attempts to connect to the LAN complies with enterprise security policy before its granted access.

To understand how proactive internal and endpoint security works, consider some real life examples of how it defeats key avenues of attack used by worms and viruses: port vulnerabilities, application spoofing and hijacking, email viruses, blended threats, attempts to shut down security applications, and propagation within the network.

Port Vulnerabilities

The first significant worm to infect the Internet, the Morris worm of 1988, spread by sending malformed commands to a vulnerable application listening on an open port, and that tried-and-true method of infection still works today. The Blaster worm of August 2003, for example, slipped through port 135 and exploited a flaw in Windows' remote procedure call (RPC) in order to execute code on the infected system. Unlike email-attached worms, it required no assistance from end users. Microsoft had issued an advisory and a patch for the RPC vulnerability less than a month before Blaster appeared, and at least half of all users had not yet applied it. As Cnet News.com wrote shortly after the outbreak began:

“The ability of the MSBlast worm to spread has underscored the view that today's methods of patching security flaws, while necessary to lock down specific computers, is too time-consuming to react to critical vulnerabilities... The University of Florida, for instance, has had hundreds of systems infected due to a compromised PC connected to its network via a dial-up line.”

If that dial-up PC had Check Point Integrity installed, however, it would have been automatically protected even without the operating system patch or virus definition. By default, Integrity blocks all inbound connection attempts from untrusted networks, and any ports that are subsequently opened are only allowed for specific, approved applications. It can also be configured to block outbound connections by any executable code it doesn't recognize. This provides a level of protection beyond traditional network-level firewalls, which can open or close ports but cannot always control what applications use them. And it is critical for situations in which legitimate applications must use the same ports that are also targets for network worms. Likewise, Integrity automatically blocks access to non-essential services on PCs that Windows turns on by default and that worms exploit.

Furthermore, by incorporating an understanding of how LAN and Windows-based applications are used on the network, InterSpect ensures that network traffic conforms to protocol standards and expected usage. InterSpect also ensures secure use of Microsoft applications in situations where other solutions force a trade-off between connectivity and security. For example, the Blaster Worm exploited the MS-RPC protocol; InterSpect can block malicious RPC connections while allowing non-dangerous RPC connections to proceed. Because the InterSpect gateway watches traffic as it flows through the network, it can also catch fast moving worms that other technologies are unable to detect or contain.

Application Spoofing and Hijacking

Integrity's application controls allow it to block Internet access by dangerous programs that employees either deliberately install (such as file-swapping programs) or applications they unwittingly install, such as Trojan horse or spyware programs. Integrity verifies the identity of trusted applications not merely by their executable names but by fingerprinting them using a “known good” MD5 hash of the application. This prevents worms or Trojans from spoofing trusted applications. And it enables administrators to control what versions of applications are permitted to run—allowing them to block either older versions with known vulnerabilities or new versions that have not yet been tested and approved.

“The ability of the MSBlast worm to spread has underscored the view that today's methods of patching security flaws, while necessary to lock down specific computers, is too time-consuming to react to critical vulnerabilities... The University of Florida, for instance, has had hundreds of systems infected due to a compromised PC connected to its network via a dial-up line.”

Integrity even protects against a class of clever worms that slips past other firewalls by “injecting” themselves into the processes of allowed applications. The Bagel worm, for example, takes advantage of the Open Process API in Windows that allows one application to control another: in this case, Bagel rides piggyback on Windows Explorer. Other firewalls would only see that Explorer.exe was attempting to open a port. But Check Point Integrity monitors the open process feature to prevent such application hijackings in the first place.

Infected Email

The most common method of spreading viruses—attaching them to email messages—remains the most effective. Despite admonishments against opening messages from unknown senders and clicking on attachments, many employees still fall prey to infected email. One reason is the increasing sophistication of social engineering tactics, such as spoofing the sender address—a tactic used by the Bagel, MyDoom, and Netsky worms. Virus writers are also replacing the poor grammar and nonsensical message text of older emails with very convincing forgeries of official notices. MyDoom.A and Netsky.P, for example, masquerade as email error messages and instruct users to open the attached files to get more information. Netsky.A spoofs an address and message from an Internet auction site, once again asking the user to click on an attachment for details.

Fortunately, Integrity’s application controls prevent executable viruses in email attachments from spreading into or across the corporate LAN. Integrity also closes a hole in enterprise email security—namely, the use of personal email software to download attachments from POP and IMAP servers—by quarantining over 45 dangerous attachment file types. As with all other aspects of Integrity, inbound mail rules can be customized to individual users or groups of users.

Integrity also blocks mass-mailing worms from spreading in two ways. Its outbound MailSafe feature prevents a PC’s mail client from sending messages to more than a set number of recipients at once or from sending a single message repeatedly. And Integrity’s application control blocks massmailing worms that carry their own SMTP email engines (a common practice of modern worms).

Blended Threats

Security threats are not only growing faster, they are growing smarter. Instead of exploiting a single vulnerability, so-called blended threats incorporate multiple attack strategies. The trend began with the infamous Nimda worm of late 2001, which spread by infecting files and Web pages, mass-mailing copies of itself, and propagating via open file shares on local networks. It has continued with worms like Netsky, which spreads via mass emails, via open file shares, and by spoofing desirable downloads on PC-based file-trading servers.

Blended threats are also more challenging for antivirus software to fully eradicate. Though the applications can usually (after some time) identify and delete the main worm or virus causing the infection, they do not always eliminate all paths of the ever-more complex payloads, such as a keystroke logging program or DLLs or registry changes that open up backdoor ports. These lingering vulnerabilities pave the way for future infections. The Doomjuice worm, for example, used a backdoor created by the MyDoom worm in order to gain access to systems.

Antivirus software has even more difficulty with a new, varied class of threats lumped under the term “spyware.” Some forms of spyware consist of Trojan horse applications or DLL files bundled with Internet downloads. These spyware programs harvest information from PCs for various commercial purposes and send it out to the programs’ authors. In the process, they often clog enterprise networks and generate help desk calls when PC response times suffer. While antivirus products can sometimes mitigate this problem to a degree, newer spyware is increasingly effective at embedding itself in the operating system so it’s extremely difficult to remove.

Integrity’s stateful firewall and application controls defeat blended threats and the various forms of spyware the same way they stop worms in general. By allowing only approved communication into and out of the endpoint—and blocking all other attempts at network communication—Integrity prevents keystroke loggers, Trojan horses, and other forms of spyware from sending valuable or sensitive information out to the Internet. They also block attempts to make inbound connections to the backdoors that blended threats increasingly leave on enterprise PCs. Similarly on the network side, InterSpect™ examines all application layers, and brings cumulative data from the network configuration, security rules, and communication and application states to evaluate connection attempts.

Propagation Within the Network

One of the reasons the Blaster and Sasser worms caused so much damage is that they propagate across enterprise networks through PC ports that need to be open for local file and printer sharing. Even if an enterprise has not yet deployed Check Point’s internal security application controls to stop the newest Blaster-type worm, it still benefits from the ability of Integrity and InterSpect to contain traffic within subnets or zones. For instance, Integrity may enable file and printer sharing in a narrowly defined “Trusted” zone while blocking access to the rest of the LAN through file and printer sharing ports. The network zone approach effectively quarantines any exploit that penetrates the perimeter, preventing the major disruptions that can occur when a worm has unrestricted access to most network nodes.

In the case where a network contains thousands of individual systems, InterSpect can be deployed at various points in the infrastructure to segment the network into multiple security zones and to control access and communications between these zones. InterSpect allows all necessary traffic to flow throughout the network, yet prevents unauthorized use between segments. It allows configuration of physical or virtual zone segments, and allows organizations to enforce zone-based security policy, thus enabling true organizational or departmental security zones.

Integrity’s and InterSpect’s zones are analogous to watertight chambers in a ship that prevents a single leak from sinking the entire vessel. Zones may correspond to existing subnets in the network, or they may be customized to the security and productivity needs of the enterprise. The designation of zones is based on what individual users do and on what resources they need to access, not on where they are located. And the administrator can easily change zone designations, as needed.

Another important feature of InterSpect is its ability to quarantine infected systems to contain attacks. The quarantine capabilities can be configured to automatically isolate compromised computers, preventing the spread of infection to other systems. Network administrators can also use the quarantine capability to isolate servers and mitigate risks before and during remediation efforts.

Attempts to Shut Down Security Applications

A number of worms, such as LovGate.V, specifically target security applications by attempting to shut them down. Without hardening, an application is very easy to terminate; simply invoking the Windows Task Manager can kill some security programs.

Integrity, however, is hardened against shutdown attempts—be it by rogue code or a rebellious end user. Even with administrator privileges, a user or worm, cannot shut down the application. Integrity's strength comes, in part, from its segmentation into driver, service, and client levels. Some other software firewalls combine the service and the client components. So attacks that shut down the client—a fairly easy operation for any application—also terminate the service. But the Integrity service can run independently from the client, and its driver can run independent of the service.

In addition to protecting itself, Integrity guarantees that other security applications are functioning properly. In particular, it can check that an antivirus application from any specified vendor is running with up-to-date virus definitions. The presence of a current antivirus application is one of several conditions that must be met before Integrity will allow the PC to access the company network.

Integrity Enforces Security Policies on Endpoint PCs

A chain is only as strong as its weakest link. Likewise, even the best enterprise security shields can fail due to vulnerabilities on individual PCs. Integrity strengthens these weak links by integrating with other security measures and enforcing policies down to the PC level. In addition to being a first line of defense, Integrity is also a tool to deploy and enforce security policies throughout the network. Administrators can set Integrity to check the security posture of every PC that's connected to the network and enforce compliance with a broad range of security policy elements including:

1. A current version of the Integrity client is running with an up-to-date policy.
2. An approved antivirus application with up-to-date signature files is running.
3. Administrator-required patches and service packs are installed.
4. Administrator-specified registry settings are present.
5. Administrator-required processes and applications (including versions) are running, and forbidden processes and applications are neither running nor installed.

Check Point provides Total Access Protection for the enterprise by ensuring policy compliance on all PCs that access the network – employee and guest, remote and internal, wired and wireless. Cooperative Enforcement™ technology enables Integrity to integrate with hundreds of network gateway products — from VPNs to switches and wireless access points — in order to ensure that non-compliant PCs are quarantined and brought back into compliance before they're allowed access to network resources.

Using the 802.1x Extensible Authentication Protocol, Integrity integrates with over 200 network devices, including switches, routers, and wireless access points from vendors such as Cisco, Nortel, Avenail, Enterasys, and Foundry. Policy enforcement even extends to PCs that do not have the Integrity client software installed. Employees or guests accessing the company network via a Web interface, for example, can first download Integrity Clientless Security—an ActiveX applet that runs the same basic configuration checks as Integrity—to disable malware such as spyware and keystroke loggers before letting the user see a network log-in screen.

Despite its strict policy enforcement capabilities, the main goal of Integrity is not to keep people off the network, but rather to make it as easy as possible for users to comply with security standards and gain access. Improved security should not come at the price of lost productivity.

User assistance is a critical component of Integrity. End users whose PCs are out of compliance with any aspect of the required policy are denied access and automatically redirected to servers that provide self-service remediation resources. Once end users take the simple steps needed to comply with security policy, Integrity and the network gateway automatically restore the users' authorized access privileges.

Shifting from Crisis Management to Policy Management

While virus and worm activity has its ebbs and flows, the overall trend is toward increasing threat levels for the foreseeable future. With IT departments stretched to the breaking point already, they can hardly afford to address future demands with the same reactive technologies they have used up until now.

Traditional protection measures such as antivirus scanning and patch application certainly have a continued role to play, but they can no longer be relied on for complete protection. Nor can traditional, network-level firewalls secure the ever-expanding perimeter resulting from remote and wireless access or manage threats that come from within.

The proactive technology at the core of Check Point InterSpect and Integrity meet both of these challenges. The combined solution stops the latest worms at both the network and endpoint levels, and it ensures that only endpoints compliant with security policy are allowed access to the LAN. This dual layer approach to worm defense offers the highest assurance of network integrity and business continuity no matter what new techniques worm writers develop. By closing system vulnerabilities, you can pre-emptively stop or contain all classes of attacks, rather than waiting for the next one to emerge. And by securing all nodes of the network, you secure all entry points.

About Check Point Software Technologies

Check Point Software Technologies (www.checkpoint.com) is the worldwide leader in securing the Internet. It is the market leader of both the worldwide VPN and firewall markets. Through its Next Generation product line, the company delivers a broad range of intelligent Perimeter, Internal and Web security solutions that protect business communications and resources for corporate networks and applications, remote employees, branch offices and partner extranets. The company's ZoneAlarm product line is one of the most trusted brands in Internet security, creating award-winning endpoint security solutions that protect millions of PCs from hackers, spyware and data theft. Extending the power of the Check Point solution is its Open Platform for Security (OPSEC), the industry's framework and alliance for integration and interoperability with "best-of-breed" solutions from over 350 leading companies. Check Point solutions are sold, integrated and serviced by a network of more than 2,200 Check Point partners in 88 countries.

CHECK POINT OFFICES

Worldwide Headquarters

3A Jabotinsky Street, 24th Floor
Ramat Gan 52520, Israel
Tel: 972-3-753 4555
Fax: 972-3-575 9256
e-mail: info@Checkpoint.com

U.S. Headquarters

800 Bridge Parkway
Redwood City, CA 94065
Tel: 800-429-4391 ; 650-628-2000
Fax: 650-654-4233
URL: <http://www.checkpoint.com>

©2004-2005 Check Point Software Technologies Ltd. All rights reserved. Check Point, AlertAdvisor, Application Intelligence, Check Point Express, the Check Point logo, ClusterXL, Cooperative Enforcement, ConnectControl, Connectra, CoSa, CooperativeSecurityAlliance, FireWall-1, FireWall-1 GX, FireWall-1 SecureServer, FloodGate-1, HackerID, 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, SecureServer, SecureUpdate, SecureXL, SiteManager-1, SmartCenter, SmartCenter Pro, Smarter Security, SmartDashboard, SmartDefense, SmartL.SM, SmartMap, SmartUpdate, SmartView, SmartView Monitor, SmartView Reporter, SmartView Status, SmartViewTracker, SofaWare, SSL Network Extender, TrueVector, 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 trade-marks 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 and 6,496,935 and may be protected by other U.S. Patents, foreign patents, or pending applications.

February 2, 2005 P/N: 501692



Check Point
SOFTWARE TECHNOLOGIES LTD.

We Secure the Internet.