

Securing Browsers to Protect Endpoints and Enterprises from Web-based Attacks



Contents

Introduction	3
Problem Statement: Web Usage Brings Huge Risks	3
Hackers Now Seek Profits, Not Glory	4
Why Traditional Controls Do Not Prevent Web-based Attacks	5
Signature Solutions	5
Firewalls	5
Web “Transactions” Need Different Security Controls	6
Signature-Free Technologies	6
Check Point WebCheck	6
Precision Emulation.....	7
How Check Point WebCheck Works.....	7
Protecting PCs from Internet Threats	7
Active Safety Features	7
Essential Security Layer.....	9
Benefits of WebCheck.....	9
Multiple Browser Support	9
Central Management and Logging	9
Signature Independent	9
Protects At All Times	9
Non-intruding	10
Conclusion	10
Appendix I: Technical Details of “Precision Emulation”	10
Without WebCheck	11
With WebCheck	11

Introduction

Enterprises must be more resourceful than ever to thwart new kinds of web-based attacks. The dominant threat to endpoint security now combines characteristics of historically effective attacks with new, more elusive methods of delivery and infection. The result: attacks are extremely difficult to stop and more serious in consequence than previous exploits.

This paper describes the emergence and characteristics of modern web-based attacks and why they are so common. The key idea is that traditional endpoint security controls are important, but are unable to fully cope with such attacks because they focus on the wrong things.

New controls for strong web security must extend to users' behaviors as well as PC software and configurations. Overreliance on signatures won't stop new attacks. And underpinning a security strategy simply by removal of malicious software will not block new attacks. The paper concludes with Check Point's enterprise solution to these web-based attacks: WebCheck™ for Check Point Endpoint Security.

Problem Statement: Web Usage Brings Huge Risks

Hackers are waging war against enterprises by exploiting web browsing habits of employees and contractors, stealing data, and making money. Exposure occurs if a business PC is used for business or personal use on the web. With each move a user makes online, hackers are close behind and doing everything they can to exploit the slightest misstep.

Organizations often have a false sense of security because traditional controls for securing enterprise endpoints do not provide dedicated protection against web-based threats. The following is a small sample of recent incidents in which criminal hackers have used the Internet as a platform to distribute their wares:

- In June 2009, more than 40,000 web sites were hit by a mass-compromise attack dubbed Nine Ball that injected malware into pages and redirected victims to a site that attempted to download further malware.¹
- May 2009, a series of rapidly spreading web site compromises known as Gumbler garnered media headlines. Gumbler-infected sites delivered keyloggers and other malware to visitors.²
- In February 2009, my.barackobama.com, the Obama campaign blogging site, was used to deliver malware infecting content to visitors.³
- The travel web site of the US government, govtrip.com, was hacked in February 2009 and used to distribute malware to government agencies.⁴
- In September 2008, malware was planted on the Business Week web site through an SQL injection attack. According to statistics from Google, 10% of the pages available on the Business Week web site were serving malware to visitors.⁵

¹ <http://www.networkworld.com/news/2009/061609-nineball-websense-attack.html?hpg1=bn>

² http://news.cnet.com/8301-1009_3-10244529-83.html

³ http://www.xiom.com/whid/2009/14/My.BarackObama.com_Infects_Visitors_With_Trojan

⁴ http://www.xiom.com/whid/2009/22/federal_travel_booking_site_spreads_malware

⁵ <http://www.xiom.com/whid-2008-35>

NEW ATTACKS, MORE RISKS

- Often web, not PC-based
- Financially motivated
- Silent
- Socially engineered
- Viral
- Morph rapidly

Hackers Now Seek Profits, Not Glory

Hacking has evolved from the attention-grabbing viruses of nearly a decade ago to the more covert and dangerous affair it is today. The result is that enterprises face more daunting online threats today than ever before and they are often less equipped to handle those threats.

A decade ago, hacking was generally characterized by a drive for glory, not financial motivation. Though sophisticated Trojan and other attack technology was around, it was rarely deployed—especially not for the financial gain for which such technology is used today. E-mail viruses such as the “I Love You” and “Melissa” were the norm, and they were widely reported in the press. Yesterday’s attacks were noticeable and had widespread impact. Many organizations responded by using desktop and gateway security applications such as signature-based antivirus products and firewalls.

Profit is the new motivation for hacking. The potential for profit is now big because the Internet has reached a critical mass of users who make financial transactions online. Making anonymous money transfers is easy with services like PayPal and eGold. And it’s not just individuals using easy-to-implement hacking tools—global organized crime is also tapping the expertise of hackers to augment or even replace higher risk and higher cost traditional tactics. Sophisticated blended threats have joined the universe of viruses, Trojans, worms, and other exploits and expanded attack possibilities beyond older exploits like spyware, adware, key loggers and root kits. New web-based attacks have three key properties:

- **Threats are much less noticeable** because they are designed to be silent on the victim PC. Only a loss of PC performance or stability might be apparent.
- **Threats are targeted** and sent in small batches to avoid detection. It’s now rare to see major headlines accompanying a particular threat.
- **Consequences are serious** and may include personal data loss/identity theft, as well as the silent takeover of individual PCs to create botnets—thousands of computers that can be controlled at once to launch large-scale attacks.

Web-based attacks include “drive-by” downloads, PHP and AJAX exploits—all retaining the worst characteristics of the recent past. They remain financially motivated, extremely damaging, and relatively silent and unnoticeable. Like earlier threats, they are once again viral and widely distributed.

Many enterprises assume they already have sufficient Internet security to prevent these web-based attacks—but remain unprotected. Unfortunately, most providers of endpoint security software do not yet offer the appropriate controls to prevent exploits by today’s web-based threats.

Why Traditional Controls Do Not Prevent Web-based Attacks

PC-based security software remains critically important today but is no longer enough to combat these new web-based attacks. Each type of solution arguably falls short in at least one important way.

Signature Solutions

This category of solution includes PC-based forms of security such as antivirus, anti-spyware and signature-based intrusion protection systems.

Signature solutions had difficulty keeping up with attacks a decade ago, and this was before modern automated, morphing and small-batch custom attacks were available. In the face of modern attackware, it is no wonder that experts and analysts have written hundreds of articles concluding the decline and death of antivirus.¹

The problem is antivirus software reacted too late for the “Morris” worm in 1998, for “Melissa” in 1999, and for “I Love You” in 2000—all of which were mass-mailed, relatively low-tech (slowly morphing) viruses. How can antivirus (and its cousins anti-spyware, IDS and similar) keep up with today’s viruses and worms that are blended, and more advanced? Indeed, they cannot. Recently, threats have appeared in small batches (thousands, not millions) that constantly morph, change their signature on every PC they hit, and stay hidden instead of drawing attention to themselves.

While antivirus, anti-spyware and similar security solutions are useful for “cleanup duty” in the aftermath of an attack, they are ineffective as a defense for some 0-hour web-based attacks.

Firewalls

Desktop firewalls shine where signatures don’t because they are effective against zero-hour, morphing, and targeted network attacks. They follow a simple and elegant rule: do not allow any traffic onto the PC unless the user and/or administrator specifically allow it.

This “reject all unless known good” rule is in direct opposition to the signature rule of “allow all except known bad.” It is easy to see why firewalls are much more effective than signature solutions at preventing threats and protecting PCs.

However, there are a couple of downsides to desktop firewalls. First, they generally allow user-solicited traffic on TCP port 80, the standard port used for HTTP traffic. When the user initiates an HTTP connection, the firewall acts as a wide-open highway that brings traffic straight onto the PC. Most studies show that spyware and other malware exists on over 80% of PCs running firewalls.²

Also, firewalls are focused on protecting users’ computers, not users’ behavior. Similarly, they do little to prevent direct online contact with malware.

¹ <http://havemacwillblog.com/campaigns/the-avid-campaign/>

² Check Point ZoneAlarm statistics.

Desktop firewalls continue to be critical components of endpoint security because they provide network based protection in a way that nothing else can. When it comes to web-based attacks, however, they are not fully effective.

Web “Transactions” Need Different Security Controls

In the face of modern web attacks, new signature-based security solutions have emerged that try to protect users online. These new transaction security products use signatures of known bad web sites, including phishing sites and spyware distribution sites. Some also contain signatures of malicious web site behaviors. This information allows them to identify and prevent users from visiting web sites at a more general level, and keep a more secure environment.

These signature solutions are the first response to the new attack types, yet they are not the most effective. They are excellent as partial solutions but are no match for the threat environment described earlier wherein hackers design dynamic, morphing threats that get past signature systems. Just as today’s viruses can bypass antivirus systems, modern web attacks evade these signature-based web transaction security products.

Signature-Free Technologies

There are several technologies that have emerged to fight web-based attacks without the use of signatures. These can be classified in a few ways:

Manual virtualization systems: These systems virtualize all or a part of the host computer, and require that all changes from the Internet to the PC take place in the virtualized system. In this way, nothing harmful can transfer from the Internet to the PC. While this seems like an elegant solution, it requires the maintenance of both a virtual machine/file system and an actual one. It also requires making ongoing decisions about both systems—something an average enterprise user is unwilling or unable to do.

Method-blocking systems: This technology focuses on one or more known browser vulnerabilities that allow hackers to target users with malicious code. For example, cross-site scripting presents a vulnerability that enables a hacker to inject malicious code into other people’s web pages. A method-blocking system actually interferes with this feature, thus removing the method by which these attacks can be carried out. While these systems are important and necessary, their shortcoming is that they block only some methods of attack (usually just one), and therefore cannot stand on their own against the sheer breadth of tactics that web-based attacks employ.

Check Point WebCheck

Unlike previous security options, web “transaction” security or other technologies, Check Point WebCheck has been created exclusively to protect users against the full breadth of web-based attacks. Its main technology is a virtualization engine that surrounds users from all sides in a “bubble of security” as they browse the web. Its main goal is to make protection simple and seamless for the user.

Precision Emulation

With its precision emulation technology, Check Point WebCheck virtualizes only those parts of the operating system that the web browser is able to access. It also automatically maintains the virtual system it creates. This means that there is no large installation, much less system memory use and associated performance degradation, and no need for the user to keep track of multiple operating systems or file systems.

How Check Point WebCheck Works

Each time a user browses the web, a number of changes—most of them innocuous—are made to their computer system. For instance, when processing an online form to become a registered user of a web site, often the site’s server creates a cookie that is placed onto the user’s computer.

Hackers ensure that not all changes to a PC originating from a web browsing session are useful or benign. Check Point WebCheck software protects enterprises and their employees from such threats at the operating system and browser levels—without the need for signatures.

Protecting PCs from Internet Threats

The Check Point WebCheck virtualization engine follows a very simple, firewall-like rule. All user-solicited downloads from the Internet write to the computer just like normal. But unsolicited downloads such as drive-bys write to the emulation layer, never touching the computer.

The result is that users can browse to any web site and click on any link without worry because all unknown or unwanted changes (from browser exploits and drive-by downloads, spyware, and viruses) are made to a virtualized file system. Only the items the user purposely downloads are placed on the endpoint.

Visually, a user knows the virtualization engine is protecting them in two ways. The first indicator is a message in the title bar of the browser stating that Check Point WebCheck is enabled. The second is a thin halo that surrounds all browser windows.

The user is able to reset the virtualization layer at any time. Doing so resets the browser back to its initial state.

Active Safety Features

At the same time the virtualization layer is working to protect users, the active safety features are offering redundant or altogether new layers of protection.

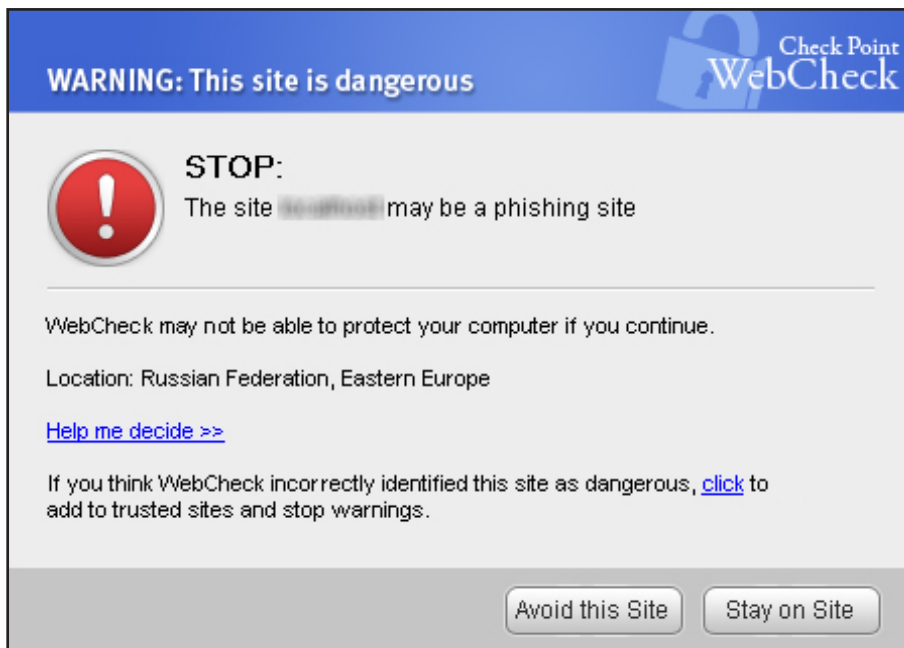
To prevent users from visiting fraudulent versions of real web sites, WebCheck uses a dual-mode anti-phishing engine comprised of a phishing signature database and advanced heuristic detection. When a user visits a known phishing site, the signature-based detection engine shows a warning such as the following.

PRECISION EMULATION: UNDER THE HOOD

Check Point Securing Browsing’s “precision emulation” technology intercepts Microsoft Windows interfaces to work directly with files and registry keys. See Appendix I for details and a diagram.



Not all phishing sites can be detected with signatures and block lists. In response, Check Point has developed a heuristic phishing detection engine that can spot fake and fraudulent copies of more than 50 financial, social networking, and shopping web sites. When the heuristic engine has detected a fraudulent site, a warning like the one below is shown in the browser.



Check Point WebCheck also rates each site visited to warn users if a site has weak or suspicious credentials. Numerous attributes are examined to determine if the site is dangerous. Attributes include age of the domain, whether the IP is listed in public spam blocking lists, if the site is hosted in certain foreign countries, and other factors. An alert like the one below warns the user to exercise caution when a suspicious site is encountered.

HEURISTIC COVERAGE

WebCheck provides preemptive heuristic phishing protection for more than 50 major web sites. Examples include:

Banking

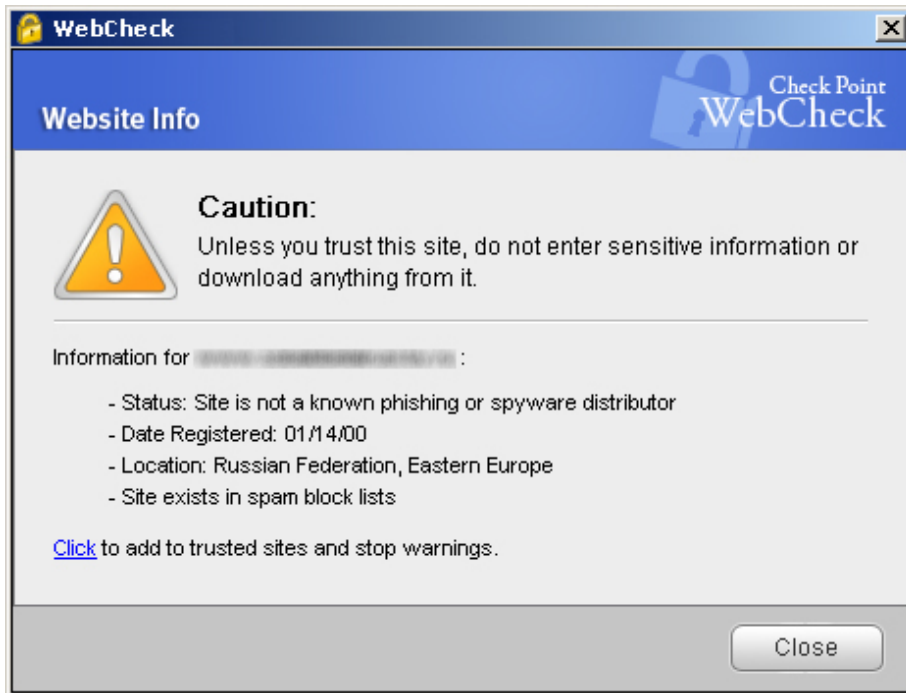
- Bank of America
- Citibank
- Wells Fargo

Commerce

- eBay
- PayPal
- Amazon

Social Networking & Web Mail

- MySpace
- Yahoo Mail
- MSN Hotmail



Essential Security Layer

By adding a new security layer, Check Point WebCheck provides the strongest protection yet from phishing sites, malicious drive-by downloads, unauthorized registry changes, adware, spy cookies, clutter, and more. The solution works with Microsoft® Internet Explorer and Mozilla Firefox browsers.

Benefits of WebCheck

Multiple Browser Support

Check Point WebCheck provides browser security parity across Microsoft Corporation's Internet Explorer 6, 7, and 8, plus Mozilla Firefox 2 and 3. Administrators can protect earlier, potentially unsafe browser versions.

Central Management and Logging

Using a simple Check Point Endpoint Security policy, consistent security is maintained across multiple browser types and versions. Central logging also allows administrators to gain quick, central insight into browser security events across the enterprise.

Signature Independent

While advanced signatures have their place, they must be coupled with a zero-hour system that, like WebCheck, employs the simple firewall-like rule: Reject all changes to the user's PC unless the user specifically solicits them.

Protects at All Times

Because web-based attacks can occur the moment the user encounters a web site, Check Point WebCheck does not passively wait for malware to transfer from the Internet to the PC. Its virtualization layer and active security layers proactively protect the user at all times.

Non-intruding

No special setup or maintenance on the part of the enterprise administrator is required. All virtualization activity is invisible to the user and requires zero maintenance. Only when data loss is imminent will WebCheck interrupt the user.

WebCheck Feature	Description
Browser virtualization	Zero day protection for browser plugin vulnerabilities and drive-by downloads
Central security policy management	Supports central security management of IE 6, 7,8 and Firefox 2, 3
Central logging & reporting	Log browser security events and generate reports
Anti-phishing (signature)	Alerts users when they visit a known phishing web site
Anti-phishing (heuristic)	Examines traits of a web site to determine if it may be a fraudulent copy of a legitimate site
Site status check	Alerts users when they visit a suspicious site

Conclusion

The emergence of web-based attacks using the most effective malicious strategies and characteristics of prior attacks has changed web-based interaction and transaction forever. Traditional security, while effective against aspects of today's threats, cannot effectively protect an enterprise PC or a user's private information from web-based attacks.

Today's web-based attacks require a third generation solution; one that goes beyond the best of other new technologies, such as the newest signature-based security, updates to virus and spyware eradication mechanisms, and new generation firewalls.

Successful protection from web-based attacks requires a dual approach. Organizations need to combine the old benefits of traditional security controls with web-focused controls that thwart attacks from today's dominant vector for security exploits. To ensure that PCs are not breached, virtualization technology will prevent unauthorized browser-driven writes to the endpoint operating and file systems.

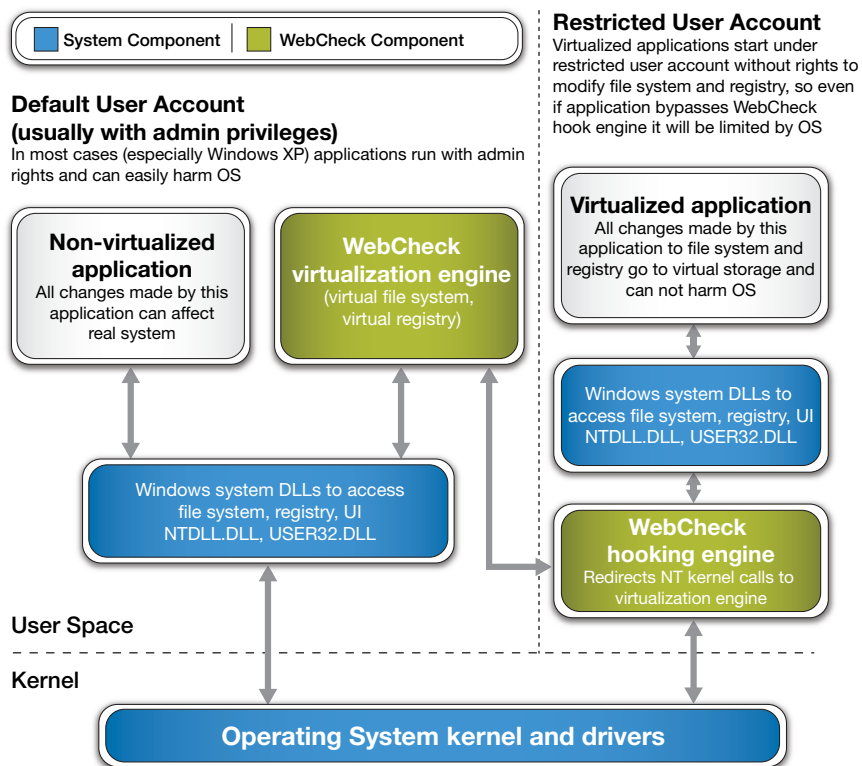
Check Point WebCheck is the only enterprise solution to provide this exciting and effective new integrated technology.

Appendix I: Technical Details of "Precision Emulation"

Check Point WebCheck's precision emulation intercepts Microsoft Windows interfaces to work directly with files and registry keys. As shown in the diagram below, Check Point WebCheck creates two major components:

- A virtualization engine, which implements a duplicate Windows file and registry system
- A hooking engine, which selectively redirects NT kernel calls to the virtualization engine.

WebCheck and Its Components and High-level Operation



Without WebCheck

Often times, user accounts run with administrative privileges, giving applications the freedom to read and write to the operating system and kernel. This allows malicious code to harm the operating system.

With WebCheck

The WebCheck hooking engine intercepts indiscriminate NT kernel calls. At this point, it decides if a kernel call was solicited by the user or was automatic, as in a drive-by download. It determines this based upon whether or not expected UI calls were made (user initiated) or not (automated, drive-by). User-solicited calls are made to the native system component as always, so as not to interrupt the user's normal workflow. Unsolicited calls, however, get applied to the virtualization engine and virtual file and registry system, therefore never reaching the actual computer. At the end of each browsing session, the virtual layer can be reset to a clean state.



About Check Point Software Technologies Ltd.

Check Point Software Technologies Ltd. (www.checkpoint.com), worldwide leader in securing the Internet, is the only vendor to deliver Total Security for networks, data and endpoints, unified under a single management framework. Check Point provides customers uncompromised protection against all types of threats, reduces security complexity and lowers total cost of ownership. Check Point first pioneered the industry with FireWall-1 and its patented Stateful Inspection technology. Today, Check Point continues to innovate with the development of the software blade architecture. The dynamic software blade architecture delivers secure, flexible and simple solutions that can be fully customized to meet the exact security needs of any organization or environment. Check Point customers include tens of thousands of businesses and organizations of all sizes including all Fortune 100 companies. Check Point award-winning ZoneAlarm solutions protect millions of consumers from hackers, spyware and identity theft.

CHECK POINT OFFICES

Worldwide Headquarters

5 Ha'Solelim Street
Tel Aviv 67897, Israel
Tel: 972-3-753 4555
Fax: 972-3-624-1100
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
URL: <http://www.checkpoint.com>

©2009 Check Point Software Technologies Ltd. All rights reserved. Check Point, AlertAdvisor, Application Intelligence, Check Point Endpoint Security, Check Point Endpoint Security On Demand, Check Point Express, Check Point Express CI, the Check Point logo, ClusterXL, Confidence Indexing, ConnectControl, Connectra, Connectra Accelerator Card, Cooperative Enforcement, Cooperative Security Alliance, CoreXL, CoSa, DefenseNet, Dynamic Shielding Architecture, Eventia, Eventia Analyzer, Eventia Reporter, Eventia Suite, FireWall-1, FireWall-1 GX, FireWall-1 SecureServer, FloodGate-1, Full Disk Encryption, Hacker ID, Hybrid Detection Engine, IMsecure, INSPECT, INSPECT XL, Integrity, Integrity Clientless Security, Integrity SecureClient, InterSpect, IPS-1, IQ Engine, MailSafe, NG, NGX, Open Security Extension, OPSEC, OSFirewall, Pointsec, Pointsec Mobile, Pointsec PC, Pointsec Protector, Policy Lifecycle Management, Power-1, Provider-1, PureAdvantage, PURE Security, the puresecurity logo, Safe@Home, Safe@Office, SecureClient, SecureClient Mobile, SecureKnowledge, SecurePlatform, SecurePlatform Pro, SecuRemote, SecureServer, SecureUpdate, SecureXL, SecureXL Turbocard, Security Management Portal, Sentivist, SiteManager-1, Smart-1, SmartCenter, SmartCenter Express, SmartCenter Power, SmartCenter Pro, SmartCenter UTM, SmartConsole, SmartDashboard, SmartDefense, SmartDefense Advisor, Smarter Security, SmartLSM, SmartMap, SmartPortal, SmartProvisioning, SmartUpdate, SmartView, SmartView Monitor, SmartView Reporter, SmartView Status, SmartView Tracker, SMP, SMP On-Demand, SofaWare, SSL Network Extender, Stateful Clustering, Total Security, the totalsecurity logo, TrueVector, Turbocard, UAM, UserAuthority, User-to-Address Mapping, UTM-1, UTM-1 Edge, UTM-1 Edge Industrial, UTM-1 Total Security, VPN-1, VPN-1 Accelerator Card, VPN-1 Edge, VPN-1 Express, VPN-1 Express CI, VPN-1 Power, VPN-1 Power Multi-core, VPN-1 Power VSX, VPN-1 Pro, VPN-1 SecureClient, VPN-1 SecuRemote, VPN-1 SecureServer, VPN-1 UTM, VPN-1 UTM Edge, VPN-1 VSX, VSX-1, Web Intelligence, ZoneAlarm, ZoneAlarm Anti-Spyware, ZoneAlarm Antivirus, ZoneAlarm ForceField, ZoneAlarm Internet Security Suite, ZoneAlarm Pro, ZoneAlarm Secure Wireless Router, Zone Labs, and the Zone Labs logo are trademarks or registered trademarks of Check Point Software Technologies Ltd. or its affiliates. ZoneAlarm is a Check Point Software Technologies, Inc. Company. 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, 5,987,611, 6,496,935, 6,873,988, 6,850,943, and 7,165,076 and may be protected by other U.S. Patents, foreign patents, or pending applications.