



**Check Point**  
SOFTWARE TECHNOLOGIES LTD.

We Secure the Internet.



White Paper

# Achieving Immediate Value in Security Data Management with Check Point Eventia Suite

SIM and SEM technologies working together to make networks more secure



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

- Executive summary ..... 3
- Security data management challenges ..... 4
- Requirements of an SIEM solution..... 4
- Common vendor SIEM solution shortcomings ..... 5
- Benefits of Check Point SIEM solutions ..... 5
  - Eventia Suite architecture ..... 5
  - Aggregation and analysis of heterogeneous logs ..... 7
  - Centralized event correlation and detection ..... 7
  - Real-time threat protection and remediation ..... 8
  - Centralized reporting for forensic investigation and trend analysis ... 9
  - Regulatory compliance support and report generation ..... 10
- Key considerations for business and usability ..... 10
  - Rapid deployment ..... 10
  - Dynamic updates for ease of maintenance ..... 10
  - Scalable, distributed architecture ..... 11
- Conclusion ..... 11

## Executive summary

Companies face a daunting challenge in discerning and responding to threat information buried within large volumes of messages from disparate security and network devices. The problem stems from the complexity of multilayered security architectures, increased security vulnerabilities from online business and extended corporate networks, and increasingly complex threats. In addition, industry and government regulations such as the Sarbanes-Oxley Act of 2002 are forcing companies to close gaps in security administration and to implement effective controls.

In responding to these challenges, companies face difficult decisions regarding allocation of limited IT and security resources. New tools that fall under the category of security information and event management (SIEM) tools, if appropriately developed, can provide tremendous value in overcoming these problems. Security information management (SIM) tools focus on reporting and analyzing log data over time, while security event management (SEM) functionality focuses on real-time event correlation. Both technologies are critical to the secure operation of an enterprise.

Although most organizations will define an initial project focus on either security data analysis/reporting or event management, most customer requirement sets specify both SIM and SEM functions. Together, Eventia Analyzer and Eventia Reporter answer this call.

These two products from Check Point Software Technologies work together to offer a powerful and easy-to-use solution that provides immediate value out of the box. The tools are optimized for integration into the Check Point environment and support full, heterogeneous devices. They also gain immediate value in terms of prioritized, correlated security events, threat blocking, prevention, and reporting—making all the networks that use them safer than ever before.

## Security data management challenges

Companies face a major challenge in managing complex security environments. Today's complex, multilayered security architecture consists of many devices to ensure that applications, hosts, and servers running on the network are protected from harmful activity. These devices all generate voluminous logs that are difficult and time-consuming to interpret. In a typical enterprise, an intrusion detection system can produce more than a half million messages per day and firewalls can generate millions of log records a day.

The logged data may contain information that appears to reflect normal activity when viewed on its own, but reveal evidence of abnormal events, attacks, viruses, or worms when raw data is correlated and analyzed. With this in mind, enterprises need control over and practical value from the deluge of data generated by network and security devices. SIEM tools offer this centralized perspective. Without it, your IT staff is forced to pore over device logs individually, having only an outside chance of forming a mental picture of your organization's network security posture.

Also, companies face a challenge in security event reporting and in the increasing burden of regulatory compliance. More than ever, companies must demonstrate compliance with government and industry regulations, but they are left without appropriate mechanisms to easily and efficiently demonstrate, implement, or report on such controls. The reports from SIEM tools can be valuable inputs to management decision making, IT administration, and threat-pattern analysis and investigation.

## Requirements of an SIEM solution

The goal of any strong SIEM solution is to meet security management needs in a way that is practical, delivers essential value, and above all else, does not break the bank. An SIEM solution that meets these specifications also should deliver a core set of capabilities and be easy to understand and use, deploy quickly, integrate with anything, and accommodate any company's particular network and security environment. What's more, an SIEM solution should include the ability to:

- Collect logs from heterogeneous devices—read, parse, normalize, and gather information in near real time from heterogeneous devices in a corporate environment
- Centralize event detection—not only to detect events but also to reduce the level of background noise in order to distinguish between events that matter and those that do not
- Prevent and remediate threats—generate alerts, automate responses, and record and track event data for post-threat investigation
- Generate reports and support compliance efforts—generate reports for management, security trending and analysis, and demonstration of regulatory compliance and auditing

The very best SIEM solutions also must be scalable so companies can grow with them as corporate needs change over time.

## Common vendor SIEM solution shortcomings

Common complaints about SIEM tools are that they take too long to deploy and are hard to use. Often, the solutions do not live up to their hyperbole. Companies find themselves taken aback by the time it takes to get vendor-supplied tools up and running, tuned, and producing usable results. Companies are also surprised by the ancillary costs. As described by Gartner Research, “In many cases, organizations find that even when they work with the vendors, the resources required to support their environments are far more intensive and costly than the vendor estimated.”

In theory, highly complex SIEM solutions sound great, but they are not easy to implement in practice. This is due to the need for substantial tuning and testing over time. It is also due to the need for significant customization. Agnostic SIEM solutions that are not optimized for a particular environment are subject to time-consuming upgrades to stay in lock step with changes to device logs and data definitions. Solutions not tied to broader security product lines lack the ability to efficiently detect network topologies and integrate with other management dashboards.

## Benefits of Check Point SIEM solutions

Two SIEM solutions that meet the requirements and transcend the shortcomings discussed previously are Eventia Analyzer and Eventia Reporter from Check Point. As parts of Eventia Suite, they work together to offer a powerful and easy-to-use solution that achieves immediate value out-of-the-box.

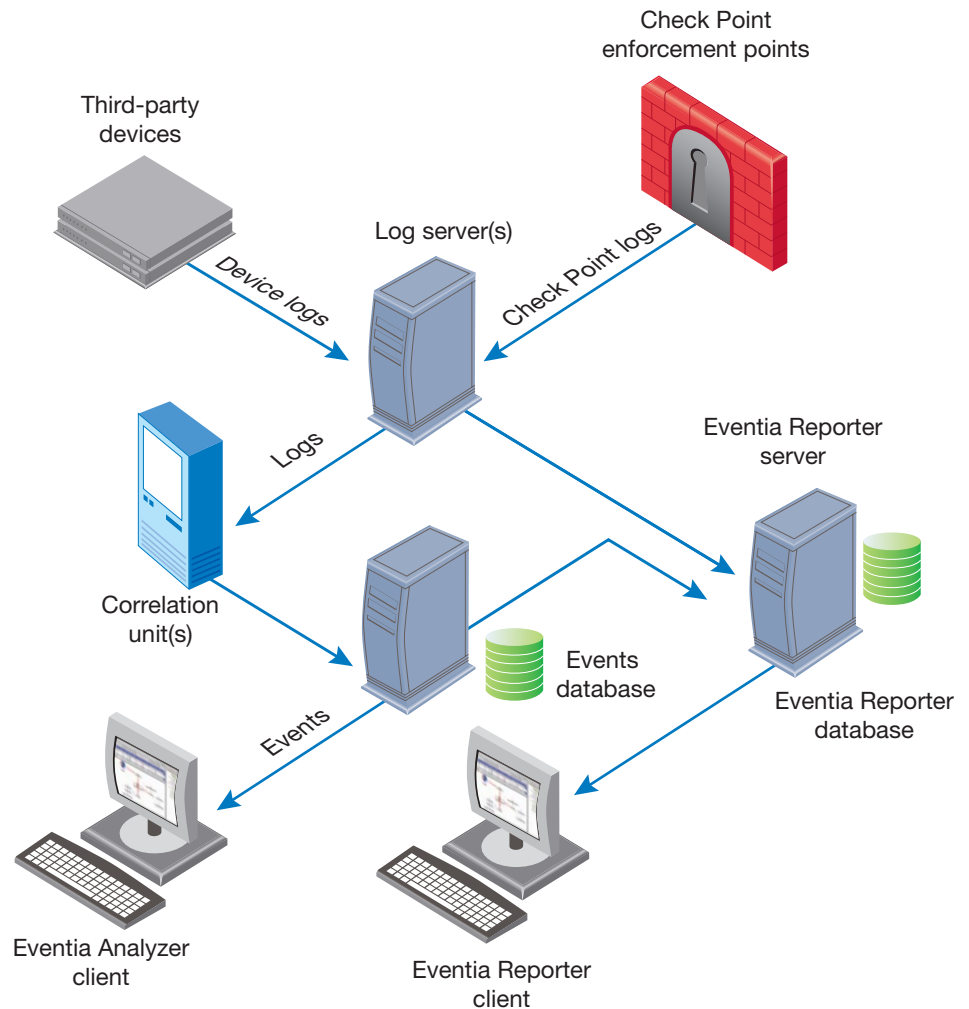
At the front end of the SIEM process, Eventia Analyzer correlates real-time security events on user networks. Moreover, the tool enables and simplifies the management and inspection of complex security environments. It filters out noise to identify events that matter, freeing up IT staff to focus on the most important threats and issues. Eventia Analyzer also reduces the burden of regulatory compliance by addressing key control requirements and enables management to gain a comprehensive, unified view of the organization’s security stance.

For the back end of SIEM, Eventia Reporter delivers a user-friendly solution for tracking and auditing network traffic. This centralized reporting system enables security managers to quickly sift through vast amounts of data collected from Check Point perimeter, internal, Web, and endpoint security gateways. With Eventia Reporter, administrators can access security or network metrics more often and at a higher level to support important decisions related to resource allocation, security optimization, and regulatory compliance.

## Eventia Suite architecture

Eventia Suite delivers a flexible, scalable platform capable of managing millions of logs per day. By virtue of its distributed architecture, which supports both Eventia Analyzer and Eventia Reporter, Eventia Suite can be installed on a single machine but retains the flexibility to spread its processing load across multiple correlation units and reporting servers, distributing data analysis across the enterprise and reducing network load. Looking closer, you will see that Eventia Suite consists of the following components:

- A correlation unit that analyzes each log entry as it enters a log server, looking for patterns according to the predefined events policy within Eventia Analyzer. When a threat pattern is identified, the correlation unit forwards what is known as an event to the Eventia Analyzer server
- The Eventia Analyzer server that receives events from a correlation unit, assigning severity levels to events, invoking any defined automatic reactions, and adding events to the events database, which resides on the server
- The Eventia Analyzer client that displays the summary of events detected and is the interface for managing and fine-tuning events policy
- The Eventia Reporter server on which a log consolidator reads logs from multiple log servers and stores the relevant logs in the reports database. Eventia Reporter generates reports from data in this database as well as from data in the Eventia Analyzer database
- The Eventia Reporter client that allows users to edit, filter, schedule, and generate reports for automatic distribution



*The Eventia Suite architecture can scale to handle millions of logs per day, per correlation unit.*

## Aggregation and analysis of heterogeneous logs

Eventia Analyzer collects logs from a full range of devices that comprises a company's network and security infrastructure. Collection includes parsing log information for the most important elements as well as normalizing it—reformulating it into a common framework so that appropriate comparisons, correlations, and counts can be made. Eventia Analyzer collects and aggregates information from antivirus applications, email servers, firewalls, intrusion detection systems, operating systems, routers, switches, and Web servers. Raw log data is collected via secure connections from Check Point and third-party devices by Eventia Analyzer correlation units, where it is centrally aggregated, normalized, and analyzed.

The Eventia Analyzer log server collects standard system logs and interprets nonstandard logs coming from a vast array of devices. It does not need an agent to collect nonstandard logs and is equipped to easily collect and process millions of logs per day.

## Centralized event correlation and detection

The correlation unit of Eventia Analyzer is the key component in aggregating and analyzing log entries and identifying events. Correlation units receive and process millions of logs that can be generated across a company's network of devices. Data reduction and correlation functions are performed at various layers, so only significant events are reported up the hierarchy for more analysis. Log data that exceed the parameters set in predefined event policies trigger security events.

These events can be denial of service attacks, network anomalies, unauthorized logins, unauthorized scans targeting vulnerable hosts, or other host-based activity.

The screenshot displays the 'Check Point Eventia Analyzer Client' window. The main pane shows a table of 'Last Hour's events' with columns for ID, Start Time, End Time, Severity, Name, Source, Destination, and Service. A detailed view of a specific event is shown below the table:

Check Point administrator credential guessing		EN00000012
<b>Start Time</b>	01:46:33 15 Aug 2006	<b>Source</b> N/A
<b>End Time</b>	04:39:29 21 Nov 2004	<b>Destination</b> N/A
<b>Update Time</b>	05:09:57 21 Nov 2004	<b>User</b> N/A
<b>Origin</b>	SmartCenter_station (10.0.0.0)	<b>Service</b> N/A
<b>Detected By</b>	10.0.0.2	<b>Direction</b> N/A
<b>Event State</b>	Open	<b>Num Conns</b> 5 (5 accepted by the firewall)
<b>Product Name</b>	Eventia Analyzer Client	<b>Peak Conns</b> 5 conns within 600 seconds
<b>Attack Name</b>	N/A	<b>Virus Name</b> N/A

The capability of Eventia Analyzer to drill down on a specific event allows it to detect threats that other solutions might not discover.

Out-of-the-box, Eventia Analyzer comes equipped with an extensive set of predefined events. In addition, a custom event wizard enables customers to easily create their own events to suit their particular environments. Administrators may perform event search queries, sorts, and filters, as well as manage event status. With new information, an open event may easily be closed or changed to a false alarm. Administrators can manage and modify future event policy.

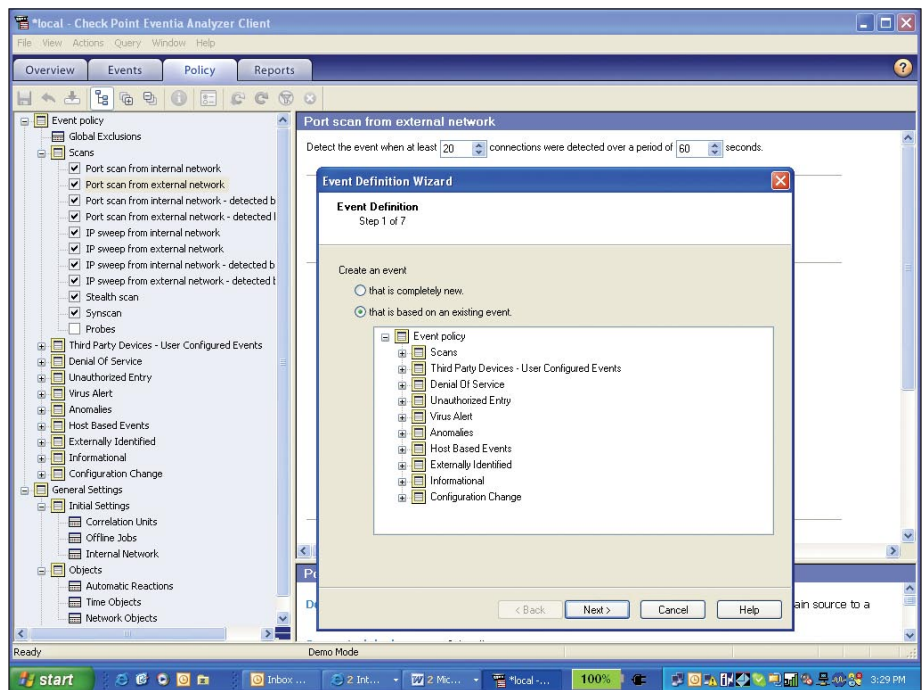
Once installed on a network, Eventia Analyzer can be implemented in an intelligent, learning mode where it automatically learns the normal security activity pattern for a given site and suggests policy changes to reduce false-alarm events. By weeding out irrelevant data and by correlating data among multiple devices and over time, Eventia Analyzer is able to zero in on threats that pose the greatest risks to the enterprise.

Through the Eventia Analyzer client user interface, administrators gain a comprehensive, unified view of the company's security status. Users can monitor and query overall events as well as drill down to manage events, mitigate threats, set policy, and schedule reports.

### Real-time threat protection and remediation

Eventia Analyzer performs real-time event correlation based on pattern anomalies and previous data, as well as correlation based on predefined security events.

With Eventia Analyzer, security administrators can develop policies for automated alerting and can schedule automated actions to respond to threats, such as blocking malicious IP sources.



*Your security staff can respond to threats and prevent future occurrences with Eventia Analyzer.*

When fully integrated with a SmartCenter™ server, Eventia Analyzer can access all Check Point gateways on your network and enforce automatic actions on them against critical threats for real-time, dynamic threat mitigation. Administrators can track and manage open events; perform event search queries, sorts, and filters; and close events due to false alarms. It also allows your security team to track events and save audit logs that can be used for post-incident investigation, trending and analysis, and demonstration of regulatory compliance.

## Centralized reporting for forensic investigation and trend analysis

Once your enterprise has correlated information on real-time security events, it is time to analyze the trend data over time. That's where Eventia Reporter comes in. Eventia Reporter handles the security information management components of SIEM, and the tool makes quick work of log data. It is a critical part of a seamless security information and event management solution.

First, Eventia Reporter provides a large number of predefined reports that save administrative time and cost by eliminating the need to create custom reports. These reports are organized into easy-to-use categories like cross-product security and network activity, firewall security and network activity, endpoint security, and antivirus as well as product-specific reports. Each report is further subdivided into sections that provide detailed information about a particular type of traffic or activity on the network. Also, reports can be tailored to suit the information requirements of different users. If there is a specific need not addressed by a predefined report, a security administrator can easily customize a report by adjusting the report filters to capture only the relevant data.

Eventia Reporter also enables administrators to schedule regular reports without constant manual intervention. Multiple reporting schedules can be maintained, making it flexible enough to meet the most demanding reporting needs. These reports can be automatically distributed to specific users via email or uploaded to FTP or Web sites. Easy report definition and distribution makes Eventia Reporter a powerful decision support system. More than 40 predefined reports—each with multiple report sections—deliver a wealth of information ranging from endpoint to firewall to user to VPN-tunnel activity. Each of these reports includes detailed—as well as graphical—executive summaries, providing consistent presentation of data across the enterprise, enabling more effective data collection and analysis.

### **Regulatory compliance support**

Eventia Suite users have the ability to view and manage comprehensive security information for their companies' entire networks. Its capabilities directly address several key Sarbanes-Oxley control requirements, in particular in the areas of monitoring, management reporting, and internal controls and assessment (detecting network behavior anomalies, managing problems and incidents, ensuring overall systems security, and managing performance and capacity). This security information and event management solution also supports compliance with other government and industry regulations and rules including Basel II, Federal Information Security Management Act, Gramm-Leach-Bliley Act, Health Insurance Portability and Accountability Act, and the Payment Card Industry Data Security Standard.

With Eventia Reporter, administrators can generate reports to aid management decision making and oversight, internal trending, and analysis and investigation. Security administrators can trace back from reports to see detailed information about the triggering events. These reports also help management gain an overall view of its infrastructure and security status.

### **Key considerations for business and usability**

In providing powerful SIEM capabilities, Eventia Suite also meets key business and usability considerations. These considerations are for rapid deployment; dynamic updates for ease of maintenance; and scalable, distributed architecture.

#### **Rapid deployment**

Eventia Suite's tight integration with the Check Point unified security architecture enables rapid deployment and ease of management. Eventia Analyzer can be integrated with existing Check Point solutions, including SmartCenter for synchronization of network objects and for efficiently executing the corrective responses to threats. Eventia Analyzer also responds immediately to incorporate any changes to individual Check Point device log definitions. With Eventia Reporter, customers can leverage existing SmartCenter storage capabilities, thereby minimizing their capital investment.

#### **Dynamic updates for ease of maintenance**

With Eventia Suite's dynamic update capabilities, customers will be able to download the latest security event rules, device support configurations, and new reports on an ongoing basis, between software revisions, as they become available. Administrators will have flexibility to upgrade their software based on internal company time schedules, ensuring minimal disruption to service.

## Scalable, distributed architecture

As an out-of-the-box SIEM solution, Eventia Analyzer delivers a flexible, scalable platform capable of managing millions of logs per day, per correlation unit, in large enterprise networks. Through its distributed architecture, Eventia Analyzer can be installed on a single server but retains the flexibility to spread its processing load across multiple units, distributing correlation across the enterprise, and reducing network load. Eventia Reporter offers a variety of installation configurations that address the different needs of organizations. Where cost and simplicity are the primary considerations, Eventia Reporter can be installed on the same machine as an Eventia Analyzer server. In environments where performance and deployment flexibility are key requirements, an Eventia Reporter server installed on a dedicated machine is recommended.

Tight integration with Provider-1 also enables service providers and large enterprises with distributed networks to perform global as well as targeted log analysis of a specific customer or network segment. The distributed architecture of Eventia Suite enables multiple instances of correlation units and log servers that can be implemented to run in parallel, scaling to meet the analysis and reporting needs of large-scale environments.

## Conclusion

Security information and event management solutions tie a company's disparate security and network data together. On the one hand, security information management tools focus on reporting and analyzing log data over time. On the other hand, security event management functionality focuses on real-time event correlation. Both technologies are critical to the secure operation of an enterprise, enabling security administrators to respond to security threats, and then analyze and respond to information hidden in the deluge of individual device logs.

Two Check Point SIEM tools—Eventia Analyzer and Eventia Reporter—work together to make your network more secure, offering a powerful, easy-to-use solution that achieves immediate value out-of-the-box. They also are optimized for tight integration into Check Point environments and support full, heterogeneous devices. Finally, they return immediate value-add in terms of prioritized, correlated security events, threat blocking, prevention, and reporting—making all the networks that they are implemented on safer places for all users.

## About Check Point Software Technologies Ltd.

Check Point Software Technologies Ltd. ([www.checkpoint.com](http://www.checkpoint.com)) is a leader in securing the Internet. It is a market leader in the worldwide enterprise firewall, consumer Internet security and VPN markets. Through its NGX platform, the company delivers a unified security architecture for a broad range of perimeter, internal, Web, and endpoint security solutions that protect business communications and resources for corporate networks and applications, remote employees, branch offices and partner extranets. The company's ZoneAlarm Internet Security Suite and additional consumer security solutions are among the highest rated in the industry today, proactively protecting millions of people from hackers, spyware, viruses and identity 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 hundreds of leading companies. Check Point solutions are sold, integrated and serviced by a network of thousands of Check Point partners around the world and its customers include 100 percent of Fortune 100 companies and tens of thousands of businesses and organizations of all sizes.

## 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](mailto: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>

©2003–2006 Check Point Software Technologies Ltd. All rights reserved. Check Point, AlertAdvisor, Application Intelligence, Check Point Express, Check Point Express CI, the Check Point logo, ClusterXL, ConnectControl, Connectra, Connectra Accelerator Card, Cooperative Enforcement, Cooperative Security Alliance, CoSa, DefenseNet, Eventia, Eventia Analyzer, Eventia Reporter, Eventia Suite, FireWall-1, FireWall-1 GX, FireWall-1 SecureServer, FloodGate-1, Hacker ID, IMsecure, INSPECT, INSPECT XL, Integrity, Integrity Clientless Security, Integrity SecureClient, InterSpect, IQ Engine, MailSafe, NG, NGX, Open Security Extension, OPSEC, OSFirewall, Policy Lifecycle Management, Provider-1, Safe@Home, Safe@Office, SecureClient, SecureClient Mobile, SecureKnowledge, SecurePlatform, SecurePlatform Pro, SecuRemote, SecureServer, SecureUpdate, SecureXL, SecureXL Turbocard, SiteManager-1, SmartCenter, SmartCenter Express, SmartCenter Power, SmartCenter Pro, SmartCenter UTM, SmartConsole, SmartDashboard, SmartDefense, SmartDefense Advisor, Smarter Security, SmartLSM, SmartMap, SmartPortal, SmartUpdate, SmartView, SmartView Monitor, SmartView Reporter, SmartView Status, SmartViewTracker, SofaWare, SSL Network Extender, Stateful Clustering, TrueVector, Turbocard, UAM, UserAuthority, User-to-Address Mapping, VPN-1, VPN-1 Accelerator Card, VPN-1 Edge, VPN-1 Express, VPN-1 Express CI, VPN-1 Power, 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, Web Intelligence, ZoneAlarm, ZoneAlarm Anti-Spyware, ZoneAlarm Antivirus, 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. 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.

December 12, 2006 P/N 502315



**Check Point**<sup>®</sup>  
SOFTWARE TECHNOLOGIES LTD.

We Secure the Internet.