

Eventia Analyzer

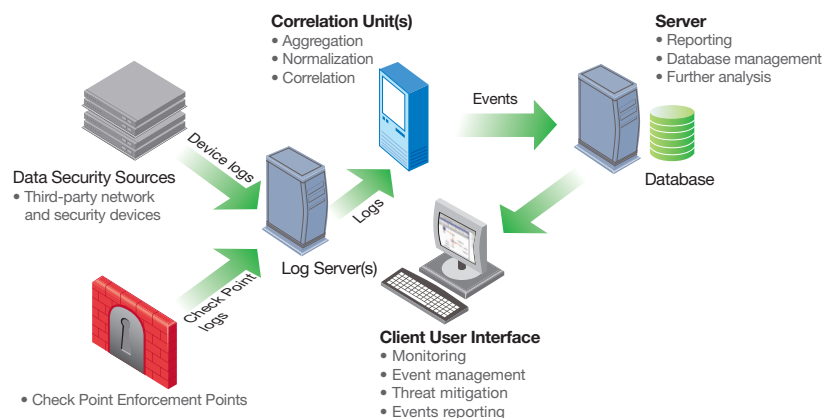
Security event management made simple

YOUR CHALLENGE

Today's complex, multilayered security architecture consists of many devices to ensure that servers, hosts, and applications 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 500,000 messages per day and firewalls can generate millions of log records a day. In addition, 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. Enterprises need control over and practical value from the deluge of data generated by network and security devices.

OUR SOLUTION

The Eventia Suite is a security information and event management (SIEM) solution designed to help IT security departments reduce the cost and complexity of security log analysis and reporting. The Eventia Suite includes Eventia Analyzer™ for real-time, security event correlation and Eventia Reporter™ for centralized reporting and historical trend analysis. Eventia Analyzer correlates log data from Check Point perimeter, internal, Web, and endpoint security devices—as well as third-party security devices—automatically prioritizing security events for decisive, intelligent action. By automating the aggregation and correlation of raw log data, Eventia Analyzer not only minimizes the amount of data that needs to be reviewed but also isolates and prioritizes real security threats. These threats may not have been otherwise detected when viewed in isolation per device, but pattern anomalies appear when data is correlated over time. With Eventia Analyzer, security teams no longer need to comb through the massive amount of data generated by the devices in their environment. Instead, they can focus on deploying resources on the threats that pose the greatest risk to their businesses.



Eventia Analyzer provides a large number of predefined events and a wizard for quick event customization.

PRODUCT DESCRIPTION

Eventia Analyzer is a comprehensive security event management solution that automatically prioritizes events for decisive, intelligent action.

PRODUCT FEATURES

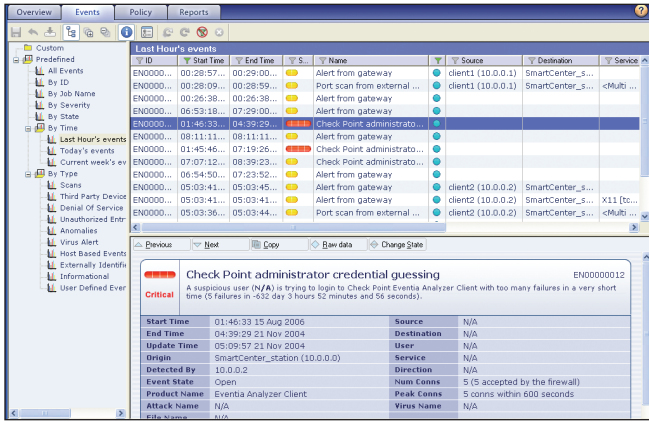
- Centralized event correlation for Check Point gateways and third-party devices
- Intelligent learning mode to baseline normal activity
- Predefined and custom security events
- Real-time alerts and automated blocking of harmful activity
- Integrated with Check Point SmartCenter™ and Provider-1®

PRODUCT BENEFITS

- Filters out noise to identify security events that matter
- Reduces business risk by responding in real-time
- Prioritizes resources to address the most critical threats
- Provides ease of deployment and use for low TCO
- Addresses regulatory compliance requirements



The NGX platform delivers a unified security architecture for Check Point.



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

SCALABLE, DISTRIBUTED ARCHITECTURE

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 has the flexibility to spread its processing load across multiple correlation units.

CENTRALIZED EVENT CORRELATION

Eventia Analyzer provides centralized event correlation and management for all Check Point products—as well as third-party devices such as firewalls, routers, switches, operating systems, mail servers, Web servers, intrusion detection systems and antivirus applications. 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, correlated, and analyzed. Data reduction and correlation functions are performed at various layers, so only significant events are reported up the hierarchy for further analysis. Log data that exceeds the parameters set in predefined event policies triggers security events. Eventia Analyzer provides a large number of predefined, but easily customizable, security events for quick deployment. These events can be unauthorized scans targeting vulnerable hosts, unauthorized logins, denial of service attacks, network anomalies, and other host-based activity. Customers can also easily create their own events using a wizard or predefined event to fine-tune the system to their particular needs.

Events are then further analyzed and severity levels assigned. Based on the severity level, an automatic action may be triggered at this point to stop the harmful activity immediately at the gateway. As new information flows in, severity levels can be adjusted to adapt to changing conditions.

EASY DEPLOYMENT

Eventia Analyzer interfaces with existing SmartCenter and Provider-1 log servers, eliminating the need to configure each device log server separately for log collection and analysis. All objects defined in SmartCenter™ or Provider-1® are automatically accessed and used by the Eventia Analyzer server for event policy definition and enforcement. In addition, this tight integration enables Eventia Analyzer to automatically learn the network's topology and detect correlated events that are sensitive to topological parameters.

EASY MAINTENANCE

Once installed on the network, Eventia Analyzer has a learning mode to baseline the normal activity pattern for a given site and suggest policy changes for fine-tuning the system. Easy-to-use event wizards provide users greater flexibility in customizing events to suit their particular environments. The ease of installation and maintenance enables customers to leverage existing IT/security staff.

TECHNICAL SPECIFICATIONS

Platforms	Linux, SecurePlatform™, Solaris, Windows
Device/OS support	3COM firewall, Apache Web server, Cisco PIX and IDS, Cisco Router, Connectra, FreeBSD OS, FireWall-1 GX, Integrity, Intrushield, ISS RealSecure, Kaspersky Antivirus, Linux OS, NetContinuum, NetScreen, Sendmail, Snort IDS, Solaris OS, Symantec Antivirus, Tipping Point SMS, Trend Micro Antivirus, UTM-1, VPN-1 Power, VPN-1 SecureClient, VPN-1 UTM, Windows OS
Check Point version support	NG and NGX versions

©2003–2007 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, Confidence Indexing, ConnectControl, Connectra, Connectra Accelerator Card, Cooperative Enforcement, Cooperative Security Alliance, CoSa, DefenseNet, Dynamic Shielding Architecture, Eventia, Eventia Analyzer, Eventia Reporter, Eventia Suite, FireWall-1, FireWall-1 GX, FireWall-1 SecureServer, FloodGate-1, 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, Policy Lifecycle Management, Provider-1, Safe@Home, Safe@Office, SecureClient, SecureClient Mobile, SecureKnowledge, SecurePlatform, SecurePlatform Pro, SecuRemote, SecureServer, SecureUpdate, SecureXL, SecureXL Turbocard, Sentivist, 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 SecureServer, VPN-1 UTM, VPN-1 UTM Edge, VPN-1 VSX, Web Intelligence, ZoneAlarm, 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, 6,496,935, 6,873,988, and 6,850,943 and may be protected by other U.S. Patents, foreign patents, or pending applications.

March 5, 2007 P/N 502429

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.