

“Eventia Analyzer looks at patterns in the chaos of data. This SIEM application will show us what is really going on—from a security standpoint.”

*Systems Specialist and Network Engineer
International Pharmaceutical Company*



CUSTOMER NAME

International Pharmaceutical Company

INDUSTRY

Pharmaceuticals

CHECK POINT PRODUCTS

- Eventia® Analyzer
- Eventia® Reporter
- SmartCenter™
- UTM-1 Edge™

CUSTOMER NEEDS MET

- Correlated logs from Check Point and third-party security devices
- Prioritized security events for decisive, intelligent action
- Minimized amount of data to be reviewed

Global Biopharmaceutical Company Stays Secure with Security Information and Event Management System

ABOUT THE PHARMACEUTICAL COMPANY

A Fortune 1000 global biopharmaceutical company headquartered in the United States focuses on therapies for sleep disorders, neurological diseases, cancer, pain management, and addiction.

THE CHALLENGE

As a leading pharmaceutical company, the organization is challenged with continuing security audits of its network and data security systems by its partner companies and the Federal Drug Administration (FDA). It must also comply with security-related legislation such as the Sarbanes-Oxley Act and the Healthcare Information Portability and Accountability Act. To pass partner and FDA audits and show compliance with regulatory requirements, the company must document its security procedures and supply the supporting data to back it up. Unfortunately, with more than 25 firewalls and other security devices spread around the globe at different sites, aggregating millions of data logs from all these sources into actionable information can be an insurmountable task.

“From an FDA and auditing standpoint for partners and government agencies, we need to show we’re in control and that we can decipher network intelligence out of millions of firewall, router, switch, and other systems logs,” says the company’s systems specialist and network engineer. “We have to be able to look deeply at events that we might be interested in and make sense of them.”

Moreover, with only two people to manage the logs, there was not enough manpower to analyze them one by one, hoping to catch something by chance, according to the company’s systems and network engineer. The company needed a security information and event management (SIEM) system that takes massive volumes of data logs from all of the company’s security devices and gathers them into a central repository.



THE CHECK POINT SOLUTION

As a long-time Check Point customer, the pharmaceutical company has a substantial standing investment in VPN-1® technology. With Eventia® Analyzer, the company is able to correlate log data from Check Point security devices—as well as third-party security devices—automatically prioritizing security events for decisive, intelligent action. And because Eventia Analyzer is tightly integrated with Check Point VPN-1 gateways and centralized management system, the company will spend less time in the configuration and deployment phases.

By automating the aggregation and correlation of raw logs, the company utilizes Eventia Analyzer to minimize the amount of data to be reviewed and also to isolate and prioritize critical security threats. According to the company's IT team, these threats may not have been detected if they were just viewed on a per-device basis, because event patterns appear when data is correlated over time.

With Eventia Analyzer, the team of site administrators no longer needs to comb through data generated by the devices on the company's network. Instead, they can focus on meeting the documentation, auditing and compliance requirements that come with doing business in the heavily regulated pharmaceutical industry.

“When it comes to documenting our security procedures and back up for auditors, the FDA and other agencies, it's a matter of showing them that we're monitoring the situation on a periodic basis,” he says, “and if anything should come up, we have policies to track any type of incident.”

Deploying Eventia Analyzer

When it came time to deploy Eventia Analyzer, the engineer at this pharmaceutical company found the process to be very clean and straightforward. Working with Check Point security engineers, he was able to implement the SIEM application as part of the overall company infrastructure at several sites in the United States and in Europe. Even though each of the company's remote sites manages its own SmartCenter™, Eventia Analyzer still needs to be able to grab data from each of them. In such a distributed environment, the company is able to get aggregated network information from Eventia Analyzer, according to the company's systems and network engineer.

THE BENEFITS OF CHECK POINT SECURITY

For the pharmaceutical company, the number-one advantage of using a suite of Eventia products—Eventia Analyzer in conjunction with Eventia® Reporter—is the ability to take virtually innumerable logs from Check Point firewalls and other security devices and combine that data with logs from third-party devices. The company can then generate extensive information on the health of its firewalls and network by running up to 30 predefined reports or customizing reports to reveal “interesting and strange” traffic, as their network engineer puts it.

“Our internal quality groups really like the Eventia reports,” he says. “But auditors want to see that we are using tools like Eventia Analyzer and that we are reviewing the reports periodically for anything that looks like an issue.”

Network events

When it comes to actual network events that Eventia Analyzer has detected, only one attempt came up, but there was no cause for alarm, the pharmaceutical firm's network engineer says. “Only one time did we actually have to block a range of IP addresses. In cases such as those, Eventia Analyzer is our early warning system and first line of defense, alerting us to potential problems so that we can use other tools to take a closer look at them.”

Eventia Analyzer can also help the company detect “testing the locks” intrusion attempts and configuration issues on DMZ servers as well as revealing other configuration issues. For example, the company's European sites use UTM-1 Edge™ network perimeter security devices. On those devices, port 80 had been left open, allowing external HTTP traffic into the network. “Eventia Analyzer showed us fairly quickly that the Internet was knocking on our backdoor, trying to get in.”

THE FUTURE

Currently, the organization is evaluating IPS-1™ from Check Point, an intelligent intrusion prevention system. The company believes it will be an advantage to stay with Check Point for secure remote access, and, potentially, intrusion prevention as security data for all these devices can be accessed and managed centrally.

CONTACT CHECK POINT

Worldwide Headquarters

5 Ha'Soleim 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 | www.checkpoint.com

©2003–2008 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, 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, 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, SMP, SMP On-Demand, SofaWare, SSL Network Extender, Stateful Clustering, 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, 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.