totalsecurity™

Check Point®
SOFTWARE TECHNOLOGIES LTD.

"Eventia Analyzer and Eventia Reporter were easy to deploy. The Eventia Suite gives me a clear, uncluttered picture of important security events on our network."

Shannon Gage
Principal Technical Support Manager
Denbighshire Country Council

CUSTOMER NAME
Denbighshire County Council

INDUSTRY
Local Government

CHECK POINT PRODUCTS
- Eventia® Analyzer
- Eventia® Reporter
- VPN-1® Power NGX R65
- SmartCenter™

CUSTOMER NEEDS MET
- Reduces cost and complexity of security management
- Prioritizes network and security events for decisive, intelligent action
- Saves administration time, minimizes amount of data to be reviewed

CYNGOR Sir Ddinbych Denbighshire COUNTY COUNCIL

Denbighshire County Council Selects Eventia Suite to Simplify Security Management

ABOUT DENBIGHSHIRE COUNTY COUNCIL

Denbighshire County Council in North Wales, United Kingdom serves a local population of 93,000. A key part of the council's IT remit is providing and supporting leased-line Internet access for 66 primary and secondary schools across the county, as well as Internet services within the County's local libraries. This is in addition to maintaining the Council's own internal network.

THE DENBIGHSHIRE COUNTY COUNCIL CHALLENGE

Managing Web access for such a diverse range of users means that close control over IT security is vital, to protect against threats and attacks from these multiple endpoints. The challenge for the council's IT team was sorting through the huge volumes of log data produced by its security and network devices every day.

"Our firewalls and other security devices produce around 1GB of log data every day," says Shannon Gage, Principal Technical Support Manager, for Denbighshire Country Council. "This was making it difficult for me to do regular security health-checks and pro-actively identify any emerging issues or threats."

Turning millions of data logs from multiple sources into usable, actionable information can be an insurmountable task—especially for smaller IT teams. This makes it difficult to perform security checks, or to spot emerging attacks or vulnerabilities in any kind of systematic way. It also diverts the IT team's resources away from other important network management tasks.

The council's IT team needed a security information and event management (SIEM) system that takes the massive volumes of data logs from all of the company's security devices and gathers them into a central repository. This data can then be correlated and analyzed, and critical security events prioritized—reducing the complexity of security management, and saving time for the IT team.

THE CHECK POINT SOLUTION

As a long-time Check Point customer, the council has a substantial standing investment in VPN-1® technology, with two Nokia IP security platforms each running VPN-1 Power NGX R65. These provide comprehensive security and remote connectivity, and defend against denial-of-service (DoS) attacks on the council's main 100MB Internet link, its corporate network and the leased-line connections serving each school and library, preventing hacking and intrusion attempts and securing network traffic.

With Eventia® Analyzer, the company is able to correlate log data from the Check Point VPN-1 Power solutions, and from third-party security devices, automatically prioritizing security events for decisive, intelligent action. Because Eventia Analyzer is tightly integrated with Check Point's gateways and centralized management system, time spent in the configuration and deployment phases was minimized.

By automating the aggregation and correlation of raw logs, the company utilizes Eventia Analyzer to minimize the amount of data for review and also to isolate and prioritize critical security threats. This in turn frees up time for the council's IT team.

According to the council's IT team, Eventia Analyzer helps them make detailed inspections of network traffic patterns and device logs easily, and gives the ability to identify issues or threats that may not have been otherwise detected, because of the ability to filter out extraneous 'chatter' from devices.

DEPLOYING EVENTIA SUITE

According to Gage, deploying Eventia Analyzer and Eventia Reporter was easy and straightforward. Working with Check Point security engineers, she was able to integrate the SIEM application into the overall network infrastructure and get up and running quickly.

THE BENEFITS OF CHECK POINT SECURITY

For Denbighshire County Council, the key benefit of using the Eventia suite of products is the time saved in network and security administration, by automating collection of raw log data, correlating it and prioritizing alerts.

"I wanted to be able to work more efficiently and improve my network's overall security. Eventia Analyzer and Eventia Reporter were easy to deploy. The Eventia Suite gives me a clear, uncluttered picture of important security events on our network." says Gage. "The analysis and reporting functions are cutting my administration time by an average of two days per month, letting us focus on more strategic tasks."

According to Gage, Eventia's range of predefined reports was very useful for quick, initial analysis of security data. She adds that since deployment, she has already found a handful of security issues that required attention, and is confident that her team is able to respond with greater precision to new threats by using Eventia Analyzer.

Currently, reports from Eventia Reporter are used only by the IT team for network management. However, Gage feels it is valuable that the reports are also available for forensic analysis following any future security issues.

THE FUTURE OF DENBIGHSHIRE COUNTY COUNCIL

The Council is planning to upgrade its VPN-1 Power firewalls to extend remote connectivity and security features, and believes that the combination of VPN-1 and Eventia Suite gives it the basis for a future-proofed, centrally managed security infrastructure that can quickly adapt and respond to its changing needs.

CONTACT CHECK POINT

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 | www.checkpoint.com

CHNTHNNT P/N 503075