Network Security Analyzer™

Security Information and Event Management

Key Benefits

- ***Enterprise-wide security intelligence***
- ***Heterogeneous & agentless device support***
- ***Real-time monitoring and alerting***
- ***Forensics and investigative root cause analysis***
- ***Reporting and monitoring portals***
- ***Compliance audit life cycle management***

Architectual Benefits

- ***Distributed and highly scalable***
- ***Heterogeneous device and vendor support***
- ***Anytime, anywhere web-based management***
- ***All-in-one solution with log management, monitoring, reporting and forensics***
- ***Role-based access and Active Directory/LDAP single sign-on integration***
- ***Out-of-the-box reporting and monitoring portals***

Powered by eIQ networks™

corero
FIRST LINE OF DEFENSE

Corero's Network Security Analyzer is an award-winning, easy-to-use and costeffective security information and event management (SIEM) and compliance audit life cycle management solution. It provides essential real-time security intelligence to help decipher hacker/virus behavior, combat security threats and meet regulatory compliance requirements across the entire IT infrastructure.

Corero's Network Security Analyzer (NSA) provides security professionals with the essential real-time security intelligence to help identify and understand hacker, virus and spam/spyware behavior, security breaches and unauthorized access to sensitive information. Armed with this information, enterprises are easily able to combat security threats and meet compliance auditing requirements.

NSA helps minimize incident response time and maximize the ability to take proactive and preventative actions. Using NSA's monitoring and correlation analysis, security professionals can quickly and easily gain insight into hacker and virus activity to improve overall security.

Architectural Overview

In today's environment, one of the primary key features for a security management solution is the ability to scale to large networked environments. Network Security Analyzer provides a distributed architecture for small to medium enterprises that scales to thousands of network devices. The architecture supports both stand-alone deployment for smaller networks and distributed deployment for larger installations. The flexibility of the NSA architecture allows for the creation of a security information and event management solution that can adapt to any environment.

The architecture allows Corero's customers to take advantage of out-of-the-box reporting and monitoring portals to offer new value-added revenue-generating services or expand their remote monitoring services to include comprehensive on-demand reporting and compliance audit log management. The built-in XML-based API allows MSSPs and enterprise customers to integrate NSA's reporting, alerting and monitoring data with other third-party portals. NSA delivers all necessary tools, such as centralized log management, monitoring/alerting reporting and forensics analysis to help meet both compliance and security operations management requirements in a single solution.

Corero Network Security Analyzer

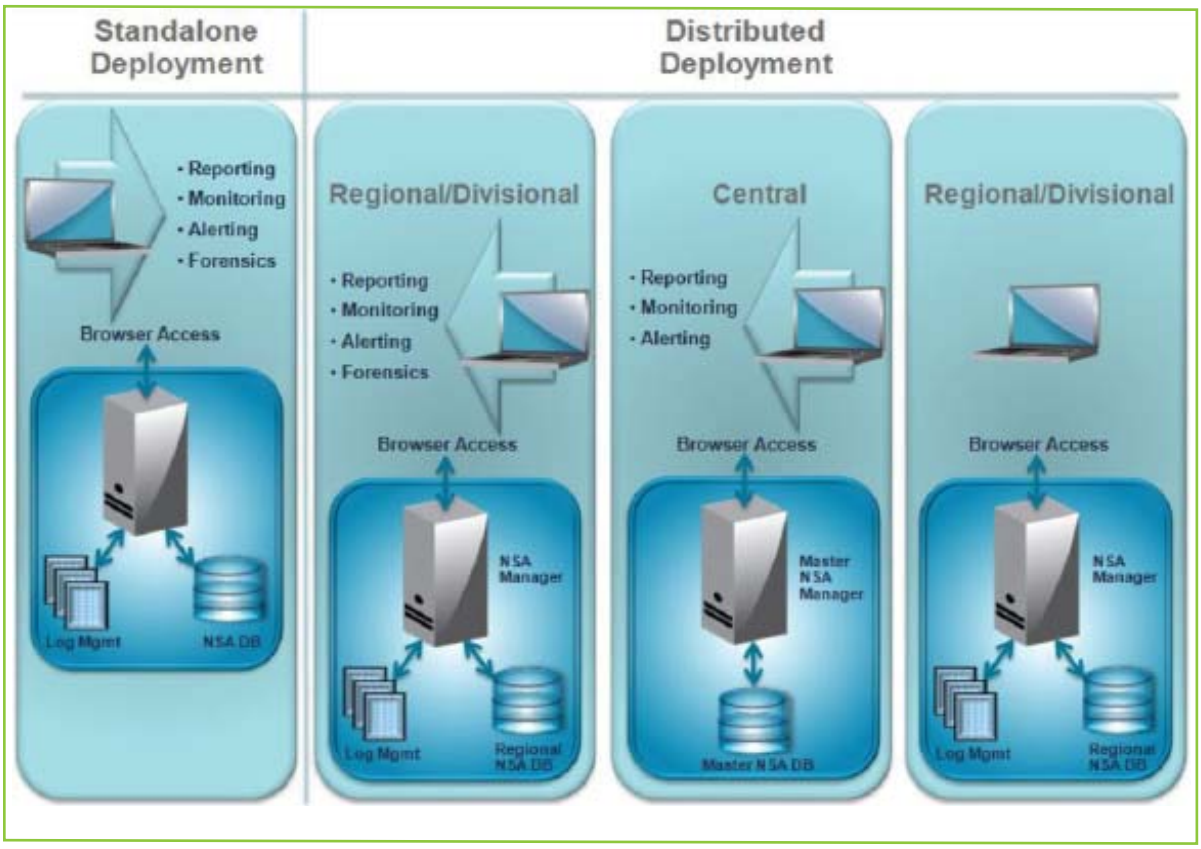

Figure 1. NSA Architecture — Network Security Analyzer provides a distributed architecture that scales to thousands of network devices. The architecture supports both a stand-alone deployment (left) for smaller networks and a distributed deployment (right) for enterprise installations.

Real-time Monitoring and Alerting Features and Benefits

Heterogeneous Real-time Monitoring: Monitors security event data across the entire network of security devices in real-time.

Real-time Alerting: Template-driven Alert Manager allows creation and definition of any number of alerts to reduce false positives and identify blended attacks.

Real-time Event Manager: View security event data from thousands of heterogeneous and multi-vendor network devices and prioritize the actions based on business impact of each event, allowing for corrective actions before an incident occurs.

Event Drilldown: Advanced on-the-fly event correlation and analysis of significant security events.

Monitoring Dashboard: Provides a quick, consolidated view of the environment. Create and view any number of user-specific monitoring views.

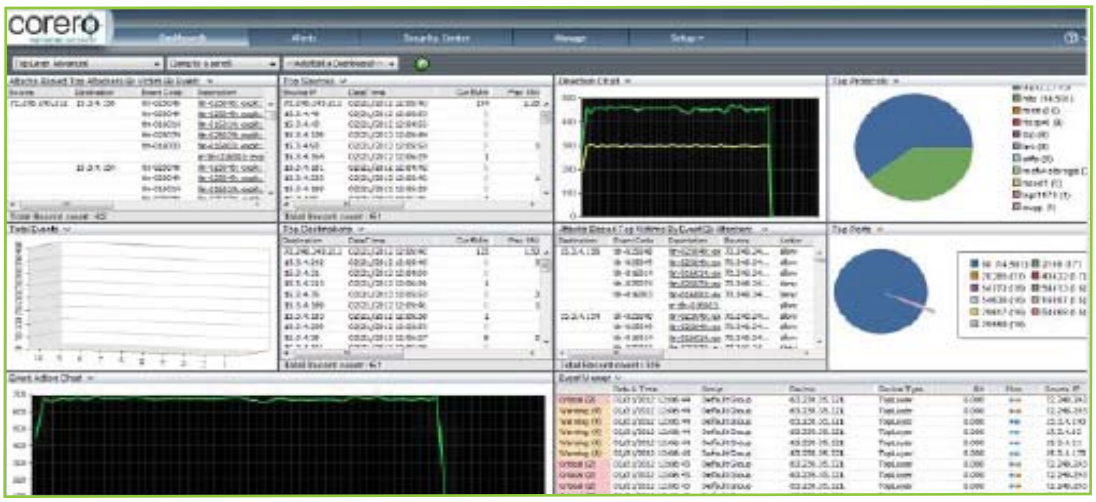

Figure 2. NSA Security Monitoring Dashboard

Security Reporting Features and Benefits

Reporting Portal with Powerful Drilldown: Reporting portal gives access to over 600 reports. Powerful drilldown feature displays second- and third-level details with a single click.

Intrusion and Rule-based Reporting: Through more than 50 attack and rule-based reports, NSA provides essential information to help security administrators get a comprehensive understanding of intrusions and rule violations.

Protocol and Web Usage Reporting: Get a firm handle on protocol and web usage patterns by user, department and/or device.

Spam and Spyware Reporting: Generates over 30 spam and spyware activity related reports.

Antivirus Reporting: Generates over 100 antivirus activity related reports that identify the presence of viruses across networks.

Vulnerability Reporting: Integrates and reports on vulnerability data derived from Nessus vulnerability scans.

Content Categorization Reporting: Generates content categorization related reports to help understand employee web usage patterns.

Automated Report Generation/ Distribution: Generates more than 600 reports. Email reports automatically to multiple recipients in HTML, MHTML, PDF, Word, Excel and text formats.

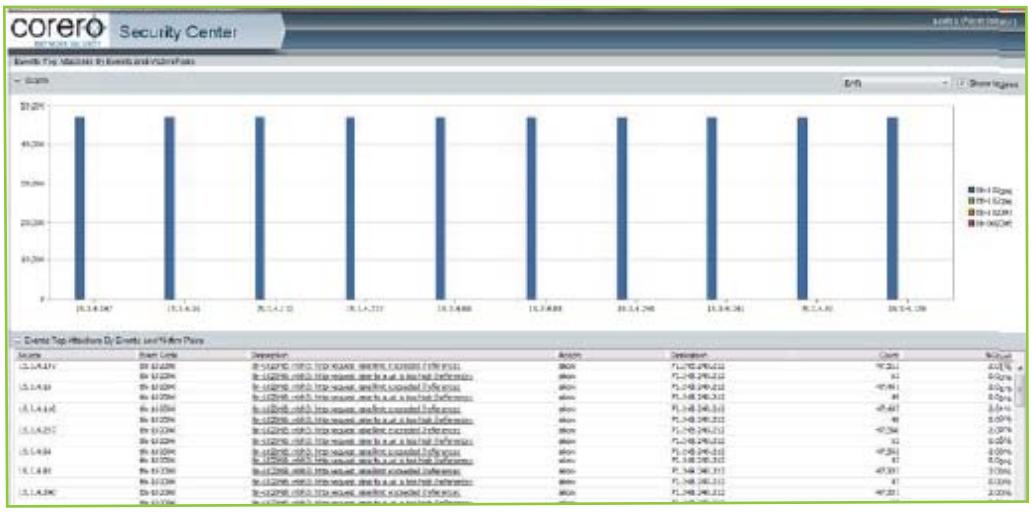

Figure 3. Detailed Event Reports for Improved Security Intelligence

Corero Network Security Analyzer

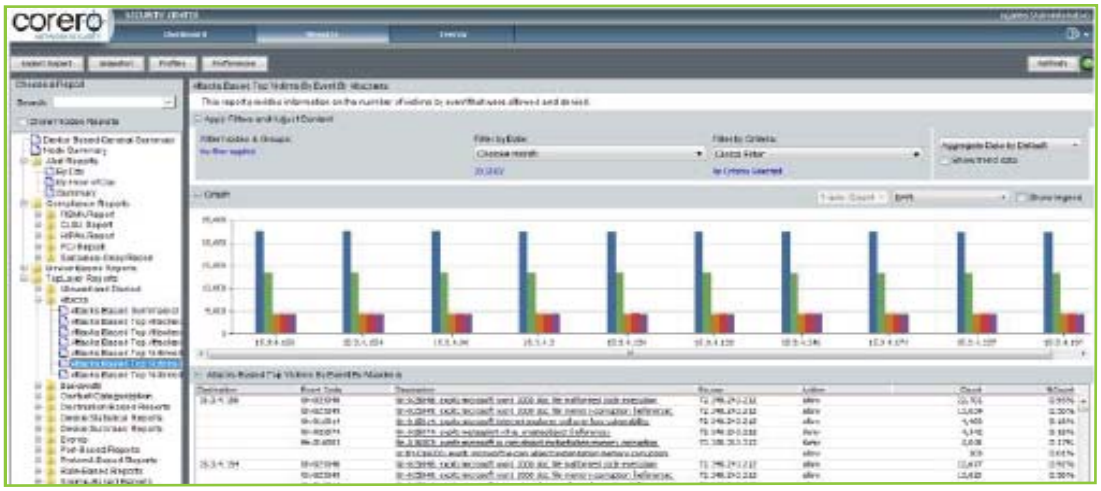

Figure 4. Regulatory Compliance Audit Cycle Management for SOX, HIPAA, GLBA and FISMA

Minimum System Requirements

- ***Processor: Single Intel P4 3.2 GHz or higher***
- ***Storage: 100 GB or higher***
- ***Memory: 2 GB or higher***
- ***Operating system: Microsoft Windows Server 2003***

Compliance Audit Life Cycle Management Features and Benefits

Automated Log Archiving for Compliance: Automatically compresses, encrypts and archives logs for investigative analysis and regulatory compliance.

Compliance Monitoring: Centralized monitoring and alert correlation for real-time investigation of security incidents with regulatory compliance implications.

Compliance Reports: Detailed reports to Sarbanes-Oxley (SOX), Health Insurance Portability and Accountability Act (HIPAA), Gramm-Leach-Bliley Act (GLBA) and the Federal Information Security Management Act (FISMA).

Scalable Search: An easy-to-use mechanism to search hundreds of GB of log data across multiple devices based on user search criteria to aid in investigative/forensics analysis.

Activity Investigation: Identify anomalies and employee corporate policy violations.

Recommended System Requirements

- ***Processor: Dual Xeon Quad Core 2.0 GHz or higher***
- ***Storage: 500 GB or higher on 15K RPM SCSI drives***
- ***Memory: 8 GB or higher***
- ***Operating system: Microsoft Windows Server 2003 or Windows Server 2008 R2***

About Corero Network Security

Corero Network Security, an organization's First Line of Defense, is an international network security company and the leading provider of Distributed Denial of Service (DDoS) defense solutions. As the First Line of Defense, Corero's products and services stop DDoS attacks, protect IT infrastructure and eliminate downtime. Customers include enterprises, service providers and government organizations worldwide. Corero's appliance-based solutions are dynamic and automatically respond to evolving cyber attacks, known and unknown, allowing existing IT infrastructure — such as firewalls — to perform their intended purposes. Corero's products are transparent, highly scalable and feature the lowest latency and highest reliability in the industry. Corero is headquartered in Hudson, Massachusetts with offices around the world. www.corero.com.

Corporate Headquarters
1 Cabot Road
Hudson, MA 01749
Phone: +1.978.212.1500
www.corero.com

EMEA Headquarters
68 King William Street
London, England
EC4N 7DZ
Phone: +44 (0) 207.959.2496