

### Key Benefits

- Enterprise-wide security intelligence
- Heterogeneous & agentless device support
- Real-time monitoring and correlated alerting
- Forensics and investigative root cause analysis
- Reporting and monitoring portals
- MSSP support with advanced user access controls
- Compliance audit lifecycle management

### Architectural Benefits

- Distributed and highly scalable
- Heterogeneous device and vendor support
- Anytime, anywhere Web based management
- All-in-one solution with log management, monitoring, correlation, reporting, and forensics
- Role-based access and Active Directory/ LDAP single sign-on integration
- Out-of-the-box reporting and monitoring portals
- XML based API for easy integration by MSSPs and Enterprise customers

## Security Information and Event Management

The Top Layer Network Security Analyzer is an award winning, easy-to-use and cost effective Security Information/Event Management (SIEM) and Compliance Audit Lifecycle Management (CALM) 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.

Top Layer's Network Security Analyzer<sup>™</sup> ("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 provides essential real-time security intelligence across thousands of network devices that have an impact on a company's security framework. NSA automatically collects and correlates event data from variety of heterogeneous multi-vendor network devices — routers, switches, firewalls, VPNs, IDS/IPS systems, proxy servers, spyware, antivirus, SPAM and content filtering web security appliances. This information will help eliminate false positives, identify security breaches and corporate violations, improve security operations, and deliver the necessary tools to meet Sarbanes-Oxley, PCI, GLBA, HIPAA, and FISMA compliance.

NSA helps minimize incident response time and maximize the ability to take proactive and preventative actions. Using their all-time monitoring and correlation analysis, security professionals can quickly and easily gain insight into hacker and virus activity to improve the 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 a stand-alone deployment for smaller networks and a distributed deployment for medium enterprise installations. The flexibility of the NSA architecture allows for the creation of a security information and event management solution that can adapt to any

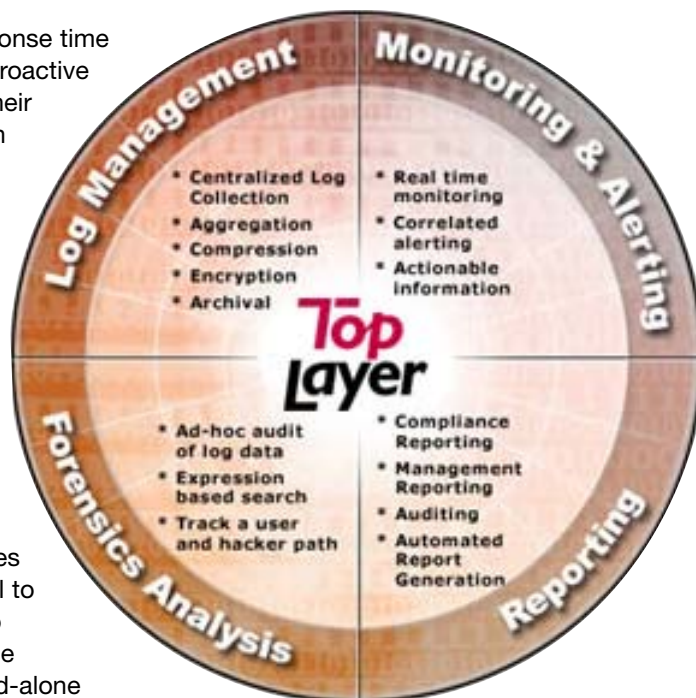


Figure 1: Comprehensive SIEM and Compliance Audit Management solution required to meet government regulations including HIPAA, GLBA, Sarbanes-Oxley, and FISMA

## NETWORK SECURITY ANALYZER

environment. The architecture allows MSSPs to take advantage of out-of-the-box reporting and monitoring portals to offer new value-added revenue generating services or expand their current 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 3rd 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, all in a single solution.

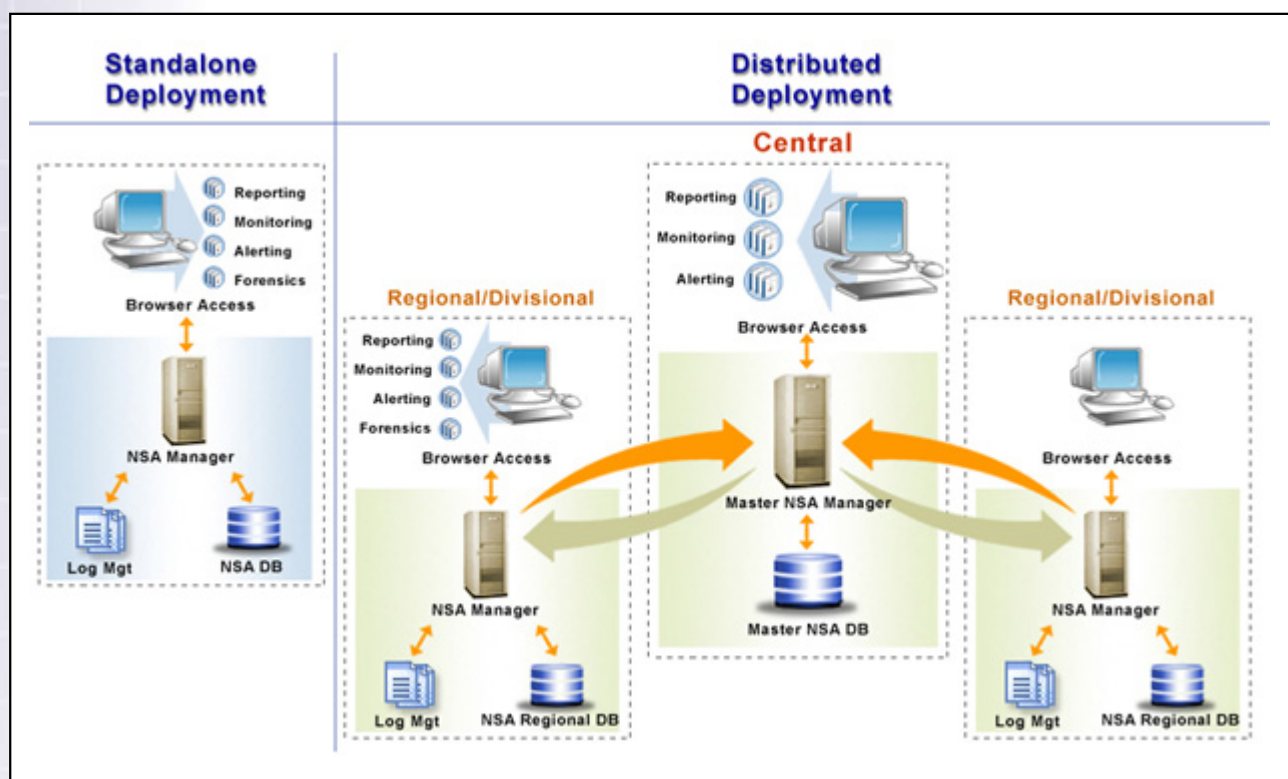


Figure 2: NSA Architecture

### 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 Correlated 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** – Monitoring dashboard provides a quick, consolidated view of the environment. Create and view any number of user specific monitoring views and toggle between the different views.

# NETWORK SECURITY ANALYZER

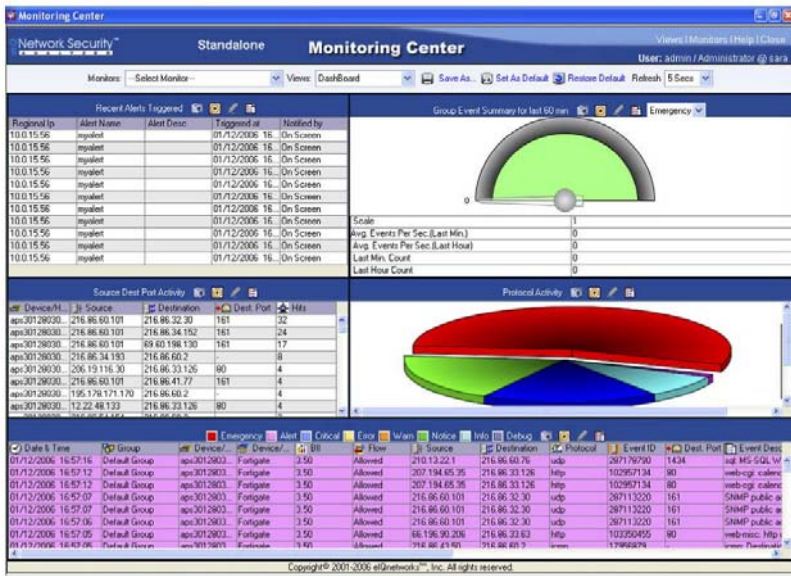


Figure 3: NSA Security Monitoring Dashboard

## Security Reporting Features and Benefits

**Reporting Portal with Powerful Drilldown** – Reporting portal gives access to over 600 reports. Powerful drilldown feature displays 2nd and 3rd level details with a single click.

**Correlated Reporting** – Get a holistic view and understanding of hacker and virus activity by correlating data across all network devices instead of looking at each device data separately.

**Intrusion and Rule based Reporting** – Through over 50 attack and rule based reports, NSA provides essential information to help security administrators get a comprehensive understanding of the 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 small and medium enterprise 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 and Distribution** – Generates over 600 easy-to-understand reports. Provides a mechanism to e-mail reports automatically to multiple recipients in HTML, MHTML, PDF, Word, Excel, and Text formats.

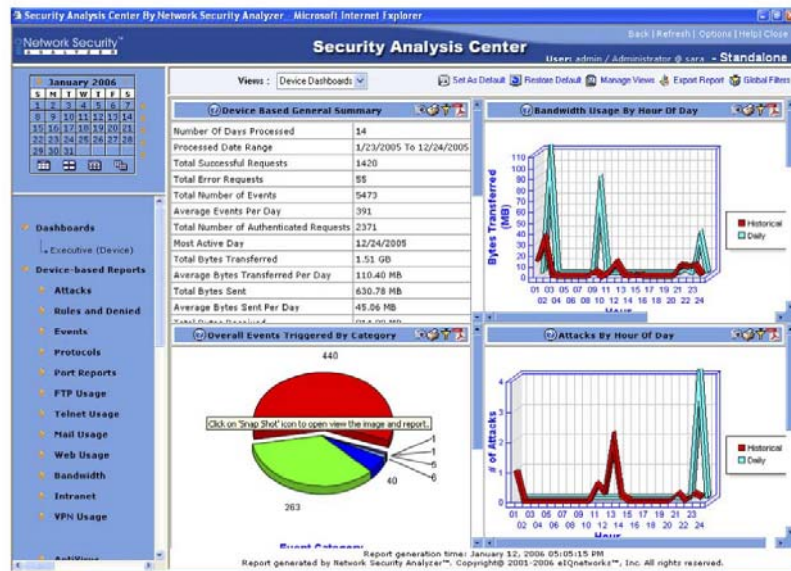


Figure 4: Detailed Reports for Improved Security Intelligence

## System Requirements

- Processor - Pentium 4 – 2.8 GHz or higher
- Disk Space – 20 GB or higher
- RAM - 2 GB or higher
- Operating System - Windows Server 2000 / 2003
- Fast I/O
- Internet Explorer 6.0 with Java

## Compliance Audit Lifecycle Management (CALM) Features and Benefits

**Automated Log Archiving for Compliance** – Automatically compresses, encrypts and archives log files 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 specific 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 configurable search criteria to aid in investigative/forensics analysis.

**Activity Investigation** – Identify anomalies and employee corporate policy violations.

## Monitoring and Correlated Alerts Compliance Reporting

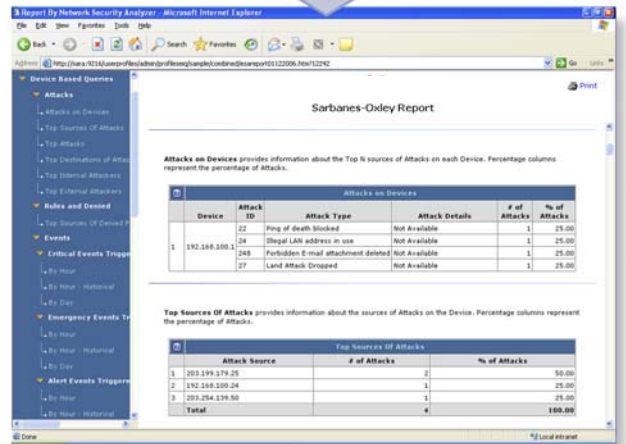


Figure 5: Regulatory Compliance Audit Management for SOX, HIPAA, GLBA, and FISMA Government Regulations

## Awards



## About Top Layer

Top Layer is dedicated to its role as the leading global provider of Network Intrusion Prevention Systems (IPS), developing and bringing to market network security infrastructure solutions that help commercial and government organizations protect their critical on-line assets from the losses and risks associated with cyber threats. Our family of IPS appliances is designed with "Three Dimensional Protection" that provides the most advanced protection capabilities against known and unknown attacks at the highest tested performance rates. Top Layer Networks is headquartered in Massachusetts USA with sales and support presence in Canada, France, Germany, Japan, Korea, The Netherlands and the United Kingdom.

**Top Layer™**

perfecting the art of network security

Top Layer Networks, Inc. 2400 Computer Drive • Westboro, MA 01581 USA • +1.508.870.1300 • Fax +1.508.870.9797

[www.TopLayer.com](http://www.TopLayer.com)