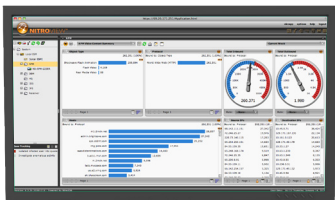


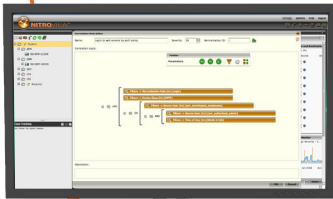
NitroView

Unified Security and Compliance

Unmatched Speed and Scale



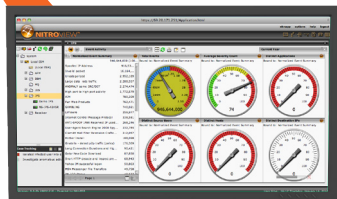
Application
Data Monitoring



Database
Monitoring



Log
Management



IPS

Content Aware
SIEM™





Today's security challenges demand a new approach to security management.

Sensitive information is at a greater risk, from more directions, using more sophisticated attacks. Compliance drivers are also evolving - mandating greater security, and imposing more severe penalties to compensate for these challenges.

How can you meet these challenges, and stay ahead of growing threats and increasing compliance requirements? NitroView rises to the occasion by integrating key information security functions into a single cohesive solution, using a patented high-speed data management and analysis engine to improve the breadth of analysis while reducing the Mean Time to Remediate (MTTR) from hours to just seconds.

The result is greater visibility into all of the relevant aspects of your information infrastructure. This means better threat detection capabilities to prevent data loss, as well as more accurate and complete compliance reports to prevent failed audits and fines.

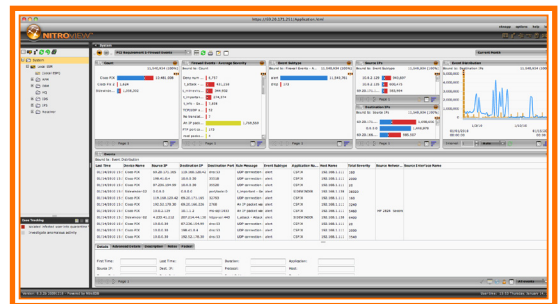
Instead of deploying several different solutions for log management, event management, data loss prevention and compliance, these and other functions are consolidated into a single, tightly integrated security and compliance management solution.

Industry's Fastest Database

It wasn't easy. Combining security functions such as Log Management, Compliance Reporting, Event Management, Threat

Management, Policy Management, and even Configuration Management into a "single pane of glass" required massive information collection. It required a database architecture capable of capturing and processing hundreds of thousands of security events per second from a multitude of devices. It required moving beyond logs into direct monitoring of networks, databases, and even application payload information. It required innovations in data storage and retrieval, in order to provide real-time reporting while at the same time scaling to a new order of magnitude of billions of security data records. But we did it.

Hundreds of man-years of R&D have turned into the fastest, most integrated security and compliance management solution available- NitroView from NitroSecurity.



NitroView Enterprise Security Manager & Enterprise Log Manager

NitroView Enterprise Security Manager (ESM) is the first and only Content Aware Security Information and Event Management system (SIEM).

Built on top of the world's fastest data collection, management and analytics engine, NitroView ESM is able to look deeper into network and application activity - all the way to the actual information stored within an application's payload. By analyzing this data for anomalies and trends, and correlating it against information collected from over 200 third party log and event sources, NitroView ESM is able to detect a broader range of threats, with fewer false positives.

In addition, NitroView ESM uses context provided from network flows, vulnerability scanners, identity management and authentication management systems to make sense of all that information, helping security analysts be more effective.

Deepest Log Management Integration

NitroView ESM is also the first SIEM to fully integrate Log Management functionality with the NitroView Enterprise Log Manager (ELM). With one log collection facility, central management of log storage and retention, and a single interface for all event management and log management features, this isn't a "bolt-on" integration, but true "single pane of glass" security management. Jump directly from any event to the relevant record in the source log file with a single click, perform text searches, or adjust log filter, storage and retention parameters - all from within the NitroView ESM console.

Integration

- Fully integrated Enterprise Log Management for log retention and compliance
- Fully integrated Database Activity Monitoring for the detection and protection of sensitive information
- Fully integrated Application and Protocol content analysis for data leakage and fraud detection
- Fully integrated Intrusion Prevention for active protection against network attacks, exploits and vulnerabilities

Compliance

- Customizable dashboards to support real-time compliance management
- Monitor and log data access by identity, roles and privileges
- Detect sensitive data within application content
- Over 300 pre-built real-time dashboards and reports for key compliance requirements, including PCI-DSS, HIPAA, NERC-CIP, FISMA, GLBA and SOX.
- Fully integrated log management with flexible storage and retention by log type or source to support specific compliance audit trail requirements

Threat Management

- Customizable dashboards to support real-time incident response and forensics
- Real-time drill-down into events, network activity, assets, and vulnerabilities collected from over 200 third party sources
- Visualized context using auto baselines, network topology overlays, and even geo-location services
- Over 200 pre-built correlation rules for the detection of larger incidents and threats
- Network topology, user identity, and geo-location context for easy location of threats both inside and outside of your company

Log Management

- Collect, hash, and store any log file, in any format, in tamper-proof storage system for chain of custody
- Filter log contents upon collection, and/or fully parse logs for deeper analysis
- Flexible storage allows on appliance storage and/or network attached storage, with a Fiber Channel SAN option for maximum storage, scale, and performance
- Integrated IT search capability



Flexible Deployment Options

Scalable from “all in one” installations with full ESM and ELM functionality in a single appliance, to highly distributed, hierarchical deployments of specialized collection and management appliances.

NitroView ESM

- ESM/ELM “all in one” appliances for smaller non-distributed networks
- ESM 4000 models for small to mid-size networks
- ESM 5000 models for mid to large networks
- ESM X5 models for extremely large networks
- NitroView Receiver models for distributed collection of logs, events, and network flows

NitroView ELM

- ESM/ELM “all in one” appliances for smaller non-distributed networks
- ELM 4000 models for small to mid-size networks
- ELM 5000 models for mid to large networks

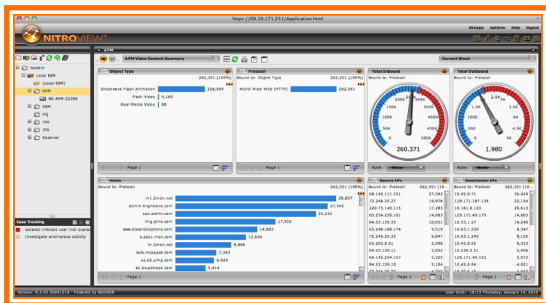


NitroView Monitoring and Deep Packet Inspection

When you have the fastest, most scalable SIEM, you have the capacity to easily collect all relevant security information from your network infrastructure.

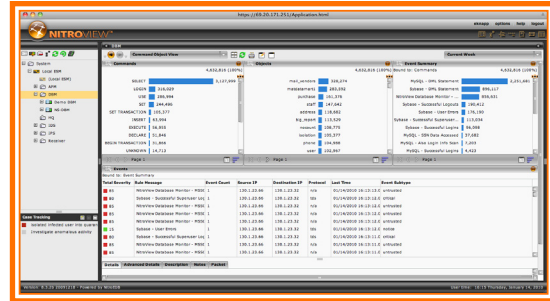
That's why NitroSecurity offers a variety of purpose-built appliances, which perform deep packet inspection to provide maximum visibility into what's happening in your network. Each NitroView monitoring appliance can be used on its own, or as a fully integrated component of NitroView Enterprise Security Manager, supplementing the hundreds of third party log and event sources already supported by NitroView ESM.

NitroView Application Data Monitor



- Fully decode and inspect the contents of application traffic, documents, and protocols
- Monitor application content and trigger alerts based on application content to detect policy violations, data leakage, and fraud
- Capture and log session detail around all triggered events
- Supports over 400 applications and protocols

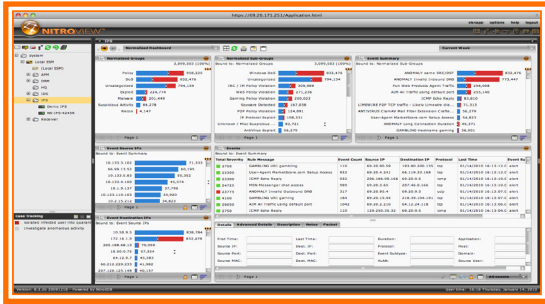
NitroView Database Monitor



- Monitor and log all database activity and session detail
- Discover databases, and whether sensitive data is stored on them
- Detect all access to sensitive data: from users, applications, malware, utilities, “back-doors,” queries, LAMP scripting, and ODBC.
- Trigger alerts based on database activities and commands, and on pattern-matching within queries and results
- Rebuild full session details from any event, from login to logoff
- Supports DB2, Oracle, MS SQL, MySQL, Informix, and SyBase databases



NitroGuard IPS



- In-line network monitoring to detect and prevent intrusion attempts, exploits, and other attacks
- Open source syntax, but with a highly optimized engine
- Centralized policy management for easy protection of larger networks
- Adaptive protection leveraging the full analytical power of NitroView
- Integrated network flow collection for added context around threat activity

Certifications

- FIPS 140-2, Level 2 Validated
- Common Criteria EAL 3 augmented with Flaw Remediation Certified



Flexible Deployment Options

Purpose-built appliances for network, data base and application monitoring

NitroView DBM

- DBM 2000 models for networks with light to moderate database activity
- DBM 4000 models for networks with heavy database activity
- DBM Agents for direct database server monitoring (optional)

NitroView ADM

- ADM 1000 models for lower bandwidth network content monitoring
- ADM 2000 models for higher bandwidth network content monitoring

NitroGuard IPS

- IPS 1000 models for 100 - 500Mbps intrusion prevention
- IPS 2000 models for 500Mbps - 1Gbps intrusion prevention
- IPS 4000 models for multi-Gigabit intrusion prevention
- IPS 5000 models for 10Gbps intrusion prevention

You Won't Believe Your Eyes

Blazing speed. Massive scale.
Unmatched integration.

NitroView is the fastest, most
integrated security and compliance
management solution available.

But don't just take our word on it-
because seeing is believing.

Contact us today to learn more and
schedule a convenient web demo.

Contact Information

1-888-LOG-SIEM

www.nitrosecurity.com



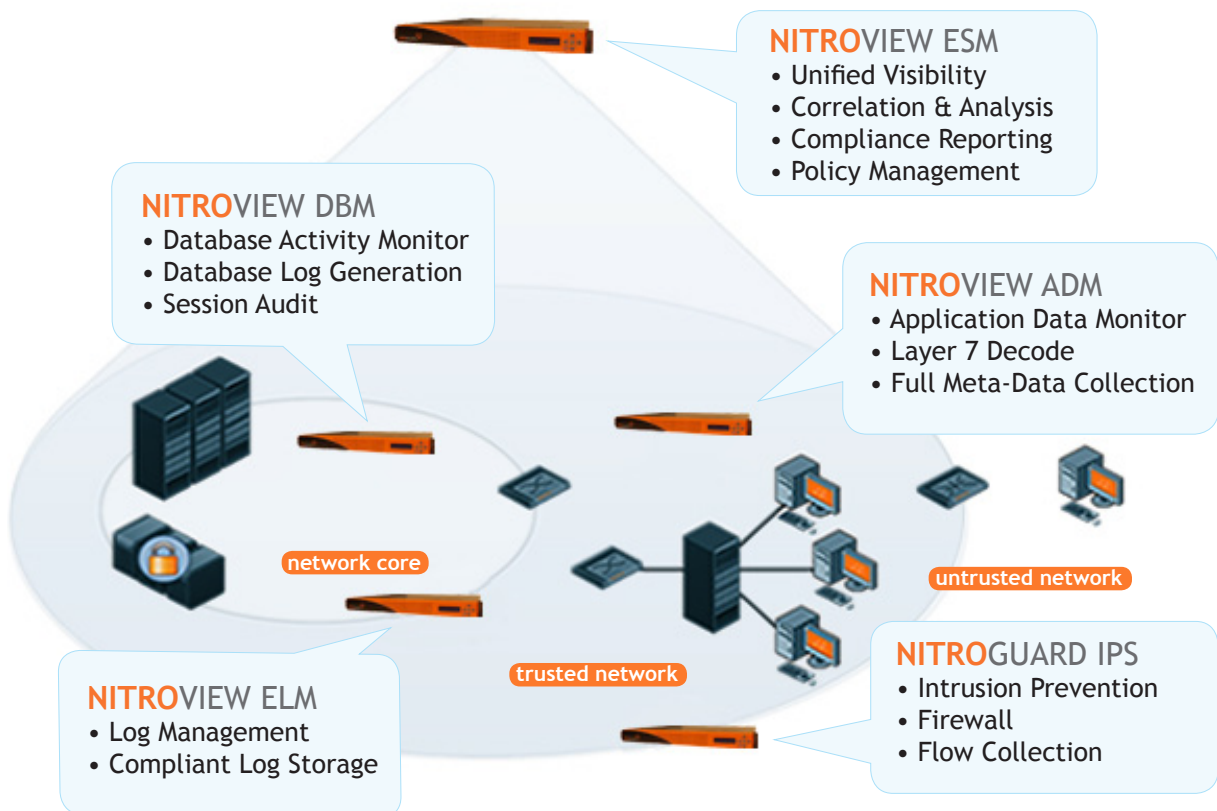
[twitter/nitrosecurity](https://twitter.com/nitrosecurity)



[linkedin.com/companies/nitrosecurity](https://www.linkedin.com/companies/nitrosecurity)



[youtube.com/user/NitroSecurity](https://www.youtube.com/user/NitroSecurity)



Corporate Headquarters
230 Commerce Way, Suite 325
Portsmouth, NH 03801, USA
Main Phone: 603.766.8160
Main Fax: 603.766.8169
www.nitrosecurity.com

Virginia Field Sales Office
12030 Sunrise Valley Drive, Suite 180
Reston, VA 20191, USA
Main Phone: 603.766.8160
Main Fax: 703.860.7404