

NitroView

Enterprise Security Manager (ESM), Enterprise Log Manager (ELM), & Receivers



The World's Fastest and Most Scalable SIEM

Finally ... an enterprise-class security information and event management system that identifies, correlates, and remediates threats in minutes instead of hours

Security management needs continue to push the limits of security information management platforms, requiring massive scalability, broad and deep visibility into business and IT systems, and blazing analytical performance.

To accommodate these needs, next-generation security management must be built upon a foundation of performance and scalability, allowing security and compliance professionals to collect, store, analyze, and act upon risks and threats—quickly, easily and accurately.

NitroView ESM rises to the challenge, leveraging our patented, high-speed and purpose-built data management engine to provide:

- Unbeatable performance, producing actionable security intelligence in minutes instead of hours
- Massive data collection across a wide range of sources
- Content awareness for broad visibility & deep analytics
- Long-term data retention, for immediate access to years of event and flow data
- Powerful detection & management of risks and threats
- Policy-aware Compliance Management
- Integrated tools for improved security workflow
- High availability options for maximum reliability

Powerful Security Information and Event Management

Unbeatable Performance

NitroView's patented data management engine processes and analyzes security information and provides it back to you as actionable security intelligence. Unlike most SIEM reports, however, the results are produced in a fraction of the time. Even during periods of peak event collection, on systems storing billions of records, NitroView can produce security and compliance information in just a few minutes, rather than hours or even days.

Massive Data Collection

Whether using a single, entry-level appliance or a fully distributed implementation of our flagship ESM X5, you'll appreciate the industry's highest event and flow collection rates, from a wide range of data sources. A single NitroView Receiver can collect over 20,000 events per second. The ESM itself can support multiple distributed receivers, and is able to handle hundreds of thousands of events per second without compression or aggregation. With aggregation, a single appliance can support tens of millions of events per second—enough for almost any network.

Long-term Data Retention

NitroView is able to store billions of events and flows, keeping all information available for immediate analysis, investigation and reporting. That's important when investigating low-and-slow attacks, searching for indications of advanced persistent threats, or attempting to remediate a failed compliance audit—all of which require looking at years of data, and having full access to the complete details of specific events.

Dynamic, Real-Time Baselines

Whether its network traffic, user activity, or trends in application use, any variation from normal activity could indicate that a threat is imminent. Normal event activity can also be a clue to a larger threat or incident. NitroView calculates real-time baseline activity for all collected information and alerts you of potential threats before they occur, while at the same time analyzing that data for patterns that could indicate a larger threat.

Content Awareness

NitroView's scalability and performance enables more events to be collected, from more sources. All information is heavily indexed, normalized, and correlated together to detect a wider range of risks and threats. When contextual information is available from vulnerability scanners, identity & authentication management systems, or privacy solutions, each event is enriched with that context for a better understanding of how events correlate to real business processes and policies.

Policy-aware Compliance Management

Compliance management requires more than simple event logging. It requires an understanding of network devices and their vulnerabilities, users and their roles, allowed applications and their use, and the business and operational policies that tie it all together. NitroView makes compliance management easy, and provides hundreds of pre-built dashboards and reports for PCI-DSS, HIPAA, NERC-CIP, FISMA, GLBA, SOX, and others.

Integrated Tools for Improved Security Workflow

NitroView ESM gets to the heart of security operations with integrated tools for configuration and change management, case management, and centralized policy management needed to improve workflow and facilitate daily information security operations.



NitroView ESM's dynamic baselines provide at-a-glance indication of network and event anomaly behavior

Turn Billions of Events & Flows into Security Intelligence in Minutes

Developed specifically for large-scale collection and real-time analysis of data, NitroView provides the performance needed to support the requirements of a content-aware, operational SIEM.

NitroSecurity has decades of experience in database technology, which provides a dramatic performance advantage over other SIEM systems. NitroView's highly optimized data management architecture uses patented techniques to provide simultaneous event collection, analysis and reporting—at extremely high speeds.

Rich, Flexible Analytics

Patented technology also enables real-time statistical calculations—including baselines and deviations—on all collected information. This enables NitroView to detect anomalies across all monitored activity, from networks, users, applications, or any other information source. It also enables visual indicators of trend activity across all dashboards, for at-a-glance trend analysis.

High Acquisition Rate

Unlike most databases, NitroView's data management engine is able to collect, parse and insert new information at extremely high rates—up to thousands of times faster than commercial SQL database management systems. This also allows NitroView to maintain these high collection rates without impacting the performance of other SIEM functions, such as analysis and reporting.

Rapid Response

NitroView's patented data management engine eliminates the need to perform time-intensive database table scans, producing detailed reports and queries in just

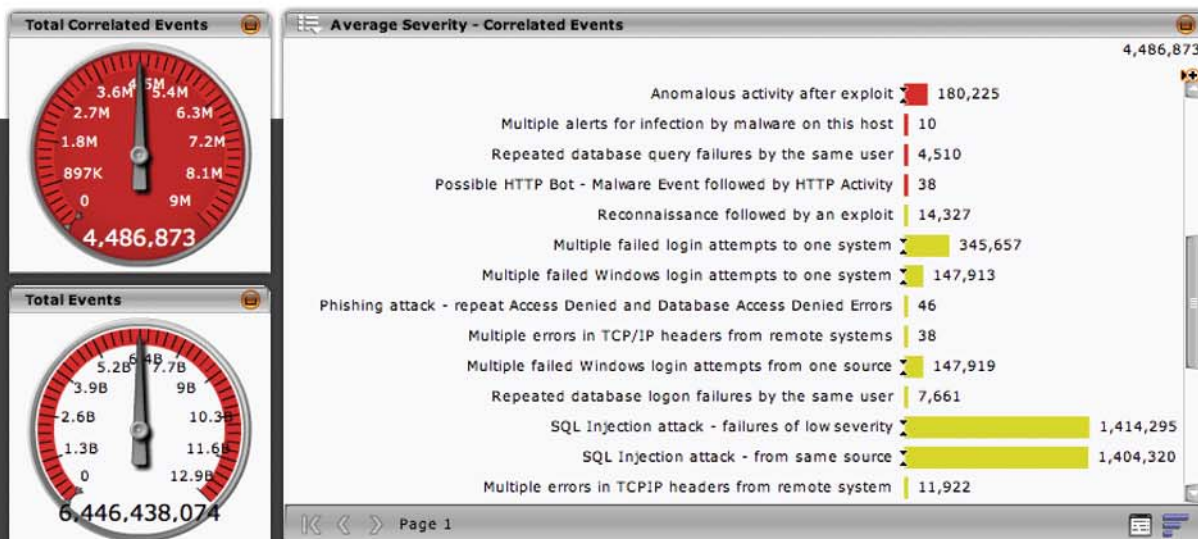
minutes instead of hours. NitroView won't slow down during periods of peak event activity—making NitroView the perfect real-time analytical tool for your Security Operations Center.

Diverse Device Support

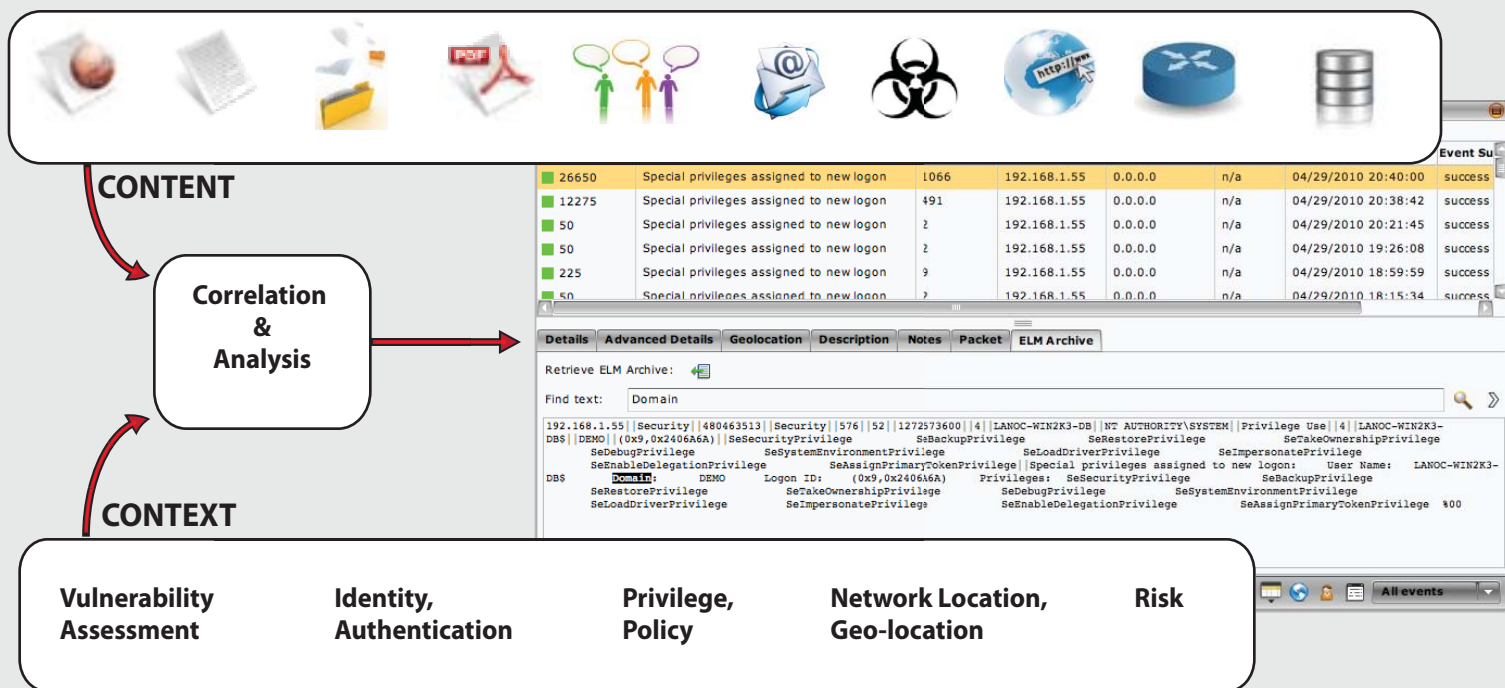
NitroView can support a wide range of devices because the underlying architecture supports diverse indexes. This means that NitroView can collect more than just log and event data, collecting and analyzing identity information, database activity, policy, privacy and other information from third party systems and applications.

Efficient Storage Utilization

NitroView's patented data indexing also allows more information to be stored using less physical storage, while maintaining full granularity of all collected information. This allows billions of events and flows to be stored locally on the NitroView appliance—fully accessible for analysis and reporting.



Fast, Reliable and Powerful Event and Flow Collection



NitroView Receiver collects third party events and logs — and performs native network flow collection — faster and more reliably than any other solution.

NitroView Receiver appliances are responsible for the collection of log and event information from hundreds of third party devices including firewalls, IDS/IPS devices, UTMs, switches, routers, applications, servers and workstations, identity and authentication systems, vulnerability assessment scanners, and more,¹ using a variety of collection methods including passive log collection, authenticated log collection, CEF, OPSEC, SDEE, XML, ODBC, and others — including encrypted collection validated to FIPS 140-2 Level 2.

Flexible Collection Architecture

NitroView supports fully centralized “all in one” event collection and management, or fully distributed event collection using dedicated NitroView Receiver appliances, rated for a few thousand to tens of thousands of events per second. Virtual appliances are also available, making highly distributed deployment easier and more cost effective.

High Reliability

NitroView Receivers can be deployed redundantly for maximum reliability without any risk of data loss. In addition, every NitroView Receiver caches all collected data locally to preserve data in the event of a network communication error or outage.

Robust Collection, Powerful Correlation

When NitroView Receiver collects an event, it parses all relevant details into a fully normalized event taxonomy, and then provides full correlation against all events to detect larger incidents. All details of parsed events and correlated events are preserved, and stored in a highly indexed database for fast retrieval and analysis. NitroView Receiver can even correlate events collected by other distributed Receivers for system-wide threat detection.

Optional Agents

NitroView supports agentless, agent-based, or hybrid collection models. NitroView Receiver supports a variety of third party agents in addition to the Nitro Plugin Protocol (NPP) agent, a highly reliable and encryptable agent for secure log and event collection. NPP has been validated under the strict requirements of FIPS 140-2, and is suitable for use in almost any network.

¹ For a complete list of supported devices, please visit nitrosecurity.com/products/supported-devices/

NitroView Enterprise Security Manager & Receiver Specifications

Model	Description	Collection Rates	Analytical Performance	Local Storage
Dedicated NitroView ESM Appliances				
NS-ESM-X5	NitroView ESM X5 Enterprise Security Manager provides Log Analysis, SIEM, and Network Analysis functions for large enterprise networks. 7TB local storage plus 500GB of in-memory storage for extremely high performance. One 3U appliance, plus one 2U Appliance.	300,000 per second ¹	Less than 10 seconds ³	7 TB ⁴ + 500GB RAM ⁵
NS-ESM-X3	NitroView ESM X3 Enterprise Security Manager provides Log Analysis, SIEM, and Network Analysis functions for large enterprise networks. 7TB local storage plus 320GB of SSD storage for extremely high performance. One 3U appliance.	150,000 per second ¹	Less than 30 seconds ³	7 TB ⁴ + 320 GB SSD
NS-ESM-5750-R	NitroView ESM 5000 Enterprise Security Manager provides Log Analysis, SIEM, and Network Analysis functions for medium to large enterprise networks. 7TB local storage. 3U Appliance.	70,000 per second ¹	Less than 1 minute ³	7 TB ⁴
NS-ESM-5510-R	NitroView ESM 5000 Enterprise Security Manager provides Log Analysis, SIEM, and Network Analysis functions. 3.75TB local storage, 3U appliance.	60,000 per second ¹	Less than 2 minutes ³	3.75 TB ⁴
NS-ESM-5205-R	NitroView ESM 5000 Enterprise Security Manager provides Log Analysis, SIEM and Network Analysis functions. 2.5TB local storage. 3U appliance.	50,000 per second ¹	Less than 3 minutes ³	2.5 TB ⁴
All-in-one NitroView ESM and Receiver Appliances				
NS-ESMRCV-5205-R	NitroView ESM 5000 Enterprise Security Manager provides Log Analysis, SIEM and Network Analysis functions. Includes integrated NitroView Receiver for collection of third party feeds. 2.5 TB local storage. 3U appliance. Rated for 5,000 events per second.	5,000 per second ²	Less than 4 minutes ³	2.5 TB ⁴
NS-ESMRCV-4245-R	NitroView ESM 4000 Enterprise Security Manager provides Log Analysis, SIEM and Network Analysis functions. Includes integrated NitroView Receiver for collection of third party feeds. 1.5 TB local storage. 1U appliance. Rated for 1,000 events per second and manages up to (3) NitroSecurity devices (IPS, DAM, or ADM).	1,000 per second ²	Less than 5 minutes ³	1.5 TB ⁴
Dedicated NitroView Receiver Appliances				
NS-NRC-4500	NitroView Receiver, collects 3rd party logs, events and flow data for correlation and analysis by NitroView ESM. 1U Appliance. Supports up to tens of thousands of data sources.	20,000 per second ²	-	1 TB ⁴
NS-NRC-4245	NitroView Receiver, collects 3rd party logs, events and flow data for correlation and analysis by NitroView ESM. 1U Appliance. Supports up to tens of thousands of data sources.	18,000 per second ²	-	1 TB ⁴
NS-NRC-2250	NitroView Receiver, collects 3rd party logs, events and flow data for correlation and analysis by NitroView ESM. 1U Appliance. Supports up to tens of thousands of data sources.	15,000 per second ²	-	1 TB ⁴
NS-NRC-2230	NitroView Receiver, collects 3rd party logs, events and flow data for correlation and analysis by NitroView ESM. 1U Appliance. Supports up to tens of thousands of data sources.	10,000 per second ²	-	1 TB ⁴
NS-NRC-1225	NitroView Receiver, collects 3rd party logs, events and flow data for correlation and analysis by NitroView ESM. 1U Appliance. Supports up to tens of thousands of data sources.	5,000 per second ²	-	500 GB ⁴
Virtual NitroView Receiver Appliances				
NS-NRC-VM-500	NitroView Virtual Receiver, for medium sized environments of up to 500 data sources.	1,000 per second ²	-	-
NS-NRC-VM-25	NitroView Virtual Receiver, for small environments of up to 25 data sources	250 per second ²	-	-

¹ Based on typical network environments using average event and flow aggregation.

² Represents raw event rates, without compression or aggregation.

³ Indicates the average response time to generate a monthly report consisting of all events that occurred over a period of 30 days.

⁴ Represents usable event and flow storage, after RAID configuration.

⁵ NitroView ESM X5 utilizes a dedicated half terabyte RAM array for fast access to event and flow data.

NitroView Enterprise Log Manager (ELM)

Compliant Log Collection, Storage and Management

NitroView Enterprise Log Manager (ELM) automates the log management and analysis for all log types, including Windows Event logs, Database Logs, Application Logs, and Syslogs. Logs are signed and validated, ensuring authenticity and integrity—a necessity for regulatory compliance. Out-of-the-box, compliance rule sets and reports ensure that it is simple to prove your organization is in compliance and policies are being enforced.

Fully Integrated

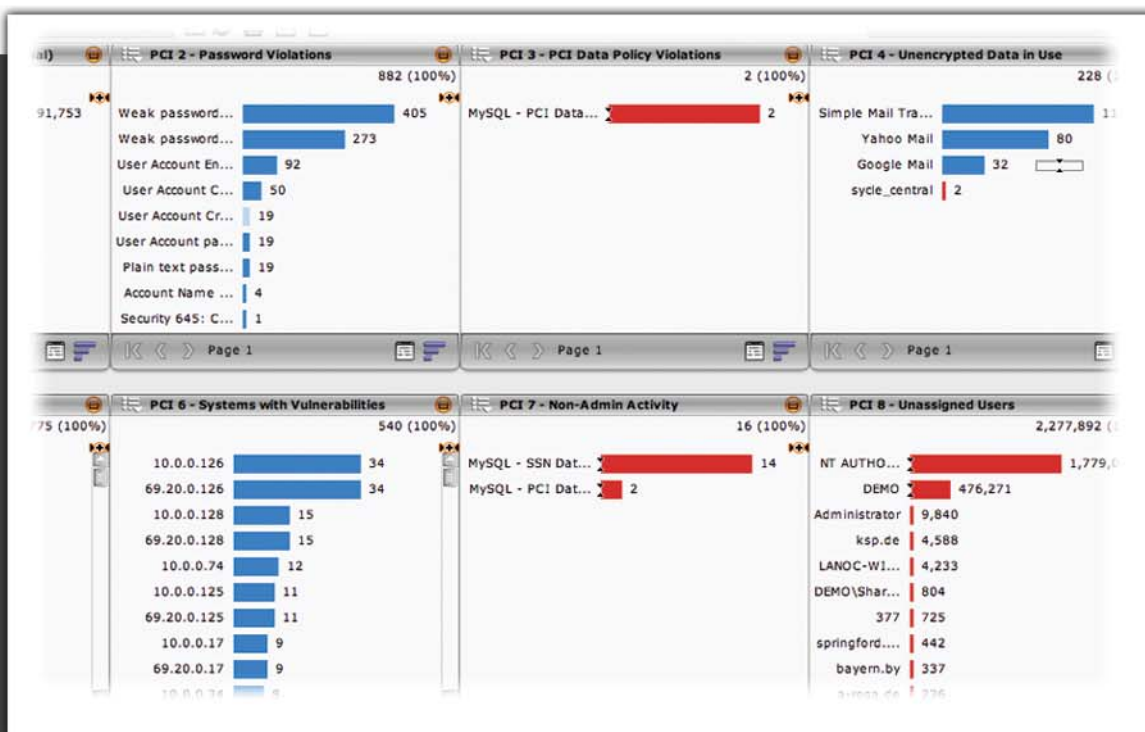
NitroView's performance and scalability allow security information and log management functions to be tightly integrated. When a security event is generated, the parsed event files are linked directly to the source log file and even to the specific log record—for instant access during the event management and forensic processes. There's no extra step, extra application to launch, or extra time to waste by searching through logs manually.

Maintains the log storage and retention requirements of compliance mandates, including:

- PCI-DSS
- SOX
- HIPAA
- FISMA
- NERC-CIP
- GLBA

Why is this important? Because log files alone don't tell us everything that we need: they contain important pieces of evidence and are an important link in establishing chain-of-custody, but they also raise important new questions. For example, we might see a username in an access log, but there is no information about what that user's role is, or what his or her privileges are. We also might know what system was accessed, but we're told nothing about what types of information are used by that system, or who should be accessing it.

NitroView ESM and NitroView ELM, together, provide context about each and every log—relevant information about the source or destination IP address, the username, hostname, or service being used, vulnerability information from a VA scanner, network topological information, even valuable policy and privacy information—making every parsed log record much more valuable.



NitroView Enterprise Log Manager Specifications

Model	Description	Collection Rates
Dedicated Enterprise Log management Appliances		
NS-ELM-5750-R	NitroView ELM 5000 Enterprise Log Manager provides Compliant Log Management functions. 7 TB local storage. 3U appliance.	50,000 events/sec
NS-ELM-4245-R	NitroView ELM 4000 Enterprise Log Manager provides Compliant Log Management functions. Supports network / SAN storage options. No local storage. 1U appliance.	45,000 events/sec
NS-ELM-5510-R	NitroView ELM 5000 Enterprise Log Manager provides Compliant Log Management functions. 3.75 TB local storage. 3U appliance.	35,000 events/sec
NS-ELM-5205-R	NitroView ELM 5000 Enterprise Log Manager provides Compliant Log Management functions. 2.5 TB local storage. 3U appliance.	20,000 events/sec
Combination Enterprise Log Manager and NitroView Receiver Appliances		
NS-NRCLM-4245-R	NitroView ELM Receiver provides compliant Log Management and collects flow data for correlation and analysis by NitroView ESM. 1U Appliance. Rated for 10,000 events per second.	10,000 events/sec
NS-NRCLM-2250-R	NitroView ELM Receiver provides compliant Log Management and collects flow data for correlation and analysis by NitroView ESM. 1U Appliance. Rated for 8,000 events per second.	8,000 events/sec
NS-NRCLM-2230-R	NitroView ELM Receiver provides compliant Log Management and collects flow data for correlation and analysis by NitroView ESM. 1U Appliance. Rated for 5,000 events per second.	5,000 events/sec
All-in-one NitroView ESM, ELM and Receiver Appliances		
NS-ESMLM-5510-R	NitroView ESM / ELM 5000 Enterprise Security Manager provides SIEM , Compliant Enterprise Log Management, and Network Analysis functions. Includes integrated NitroView Receiver for collection of third party feeds. 3.75 TB local storage. 3U appliance.	5,000 events/sec
NS-ESMLM-5205-R	NitroView ESM / ELM 5000 Enterprise Security Manager provides SIEM , Compliant Enterprise Log Management, and Network Analysis functions. Includes integrated NitroView Receiver for collection of third party feeds. 2.5 TB local storage. 3U appliance.	2,500 events/sec
NS-ESMLM-4245-R	NitroView ESM / ELM 4000 Enterprise Security Manager provides SIEM , Compliant Enterprise Log Management, and Network Analysis functions. Includes integrated NitroView Receiver for collection of third party feeds. 1 TB local storage. 1U appliance.	1,000 events/sec

Events
Bound to: Event Summary

Total Severity	Rule Message	Event Count	Source IP	Destination IP	Protocol	Last Time	Event Su
26650	Special privileges assigned to new logon	1066	192.168.1.55	0.0.0.0	n/a	04/29/2010 20:40:00	success
12275	Special privileges assigned to new logon	491	192.168.1.55	0.0.0.0	n/a	04/29/2010 20:38:42	success
50	Special privileges assigned to new logon	2	192.168.1.55	0.0.0.0	n/a	04/29/2010 20:21:45	success
50	Special privileges assigned to new logon	2	192.168.1.55	0.0.0.0	n/a	04/29/2010 19:26:08	success
225	Special privileges assigned to new logon	9	192.168.1.55	0.0.0.0	n/a	04/29/2010 18:59:59	success
50	Special privileges assigned to new logon	2	192.168.1.55	0.0.0.0	n/a	04/29/2010 18:15:34	success

Details | **Advanced Details** | **Geolocation** | **Description** | **Notes** | **Packet** | **ELM Archive**

Retrieve ELM Archive:

Find text:

```

192.168.1.55|Security||480463513|Security||576||52||1272573600||4||LANOC-WIN2K3-DB$|NT AUTHORITY\SYSTEM||Privilege Use||4||LANOC-WIN2K3-DB$|DEMO|(0x9,0x2406A6A)||SeSecurityPrivilege|SeBackupPrivilege|SeRestorePrivilege|SeTakeOwnershipPrivilege|SeDebugPrivilege|SeSystemEnvironmentPrivilege|SeLoadDriverPrivilege|SeImpersonatePrivilege|SeEnableDelegationPrivilege|SeAssignPrimaryTokenPrivilege|Special privileges assigned to new logon: User Name: LANOC-WIN2K3-DB$|Domain: DEMO|Logon ID: (0x9,0x2406A6A)|Privileges: SeSecurityPrivilege|SeBackupPrivilege|SeRestorePrivilege|SeTakeOwnershipPrivilege|SeDebugPrivilege|SeSystemEnvironmentPrivilege|SeLoadDriverPrivilege|SeImpersonatePrivilege|SeEnableDelegationPrivilege|SeAssignPrimaryTokenPrivilege #00
    
```

Page 1 All events

Beyond SIEM & Log Management

Complimenting powerful analytics with advanced network, database and application monitoring

While most SIEM solutions require you to “tune” existing log and event sources in order to minimize the data being managed, the value of NitroView increases as more information is added. That’s why NitroSecurity built a fully integrated suite of monitoring appliances to help obtain that information.

Every one of our appliances is fully integrated, leveraging the power and flexibility of NitroView ESM for central device and policy management in addition to information and event management, providing everything you need to deploy, maintain and operate a cohesive security monitoring and management strategy—all in a “single pane of glass.”

NitroView Application Data Monitor (ADM)

NitroView ADM provides deep packet inspection of all application traffic, providing full decode of application data and meta-data, for maximum visibility into how applications are being used in your network. All traffic is monitored for anomalies or for specific policy violations, making NitroView ADM an ideal detector of risk, fraud and data loss. All violations are logged, creating a clear audit trail to meet regulatory requirements.

NitroView Database Monitor (DBM)

NitroView DBM is a complete database protection solution that delivers non-intrusive, detailed security logging by monitoring all access to sensitive corporate and customer data. NitroView DBM's pre-defined rules and reports, privacy-friendly logging features and encrypted, time-stamped files make it easy to comply with the specific data access regulations required by PCI-DSS, HIPAA, NERC-CIP, FISMA, GLBA, SOX and others.

NitroGuard Intrusion Prevention System (IPS)

NitroGuard is an intrusion prevention appliance that actively detects, analyzes, and protects networks from security attacks, including viruses, worms, spyware, DDoS attacks, malware, and zero-day attacks.

Through its integration with NitroView ESM, NitroGuard IPS is able to dynamically react to larger indications of risk and threats that can only be detected when looking at all event and network activity holistically. Once discovered, NitroView can tell the relevant NitroGuard IPS device to blacklist that traffic, mitigating the event.



For more information
Call: 1-888-LOG-SIEM

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

nitrosecurity