Powerful, intelligent and adaptable network security
Finally … a network intrusion detection and prevention appliance that integrates completely into your overall information security plans, and makes your network more secure as a result.

NitroGuard is an intrusion prevention appliance that actively detects, analyzes, and protects the network from an array of security attacks, including viruses, worms, spyware, Denial-of-Service (DoS) attacks, and other forms of malware, as well as unknown or zero-day attacks. Utilizing the power of our patented relational data management engine, NitroGuard identifies and neutralizes threats and detects anomalies — in real time, before they disrupt the network and impact the business.

The ability to detect more threats with fewer false positives is possible because of NitroGuard’s ability to:

- Maintain multiple simultaneous IDS and IPS policies from a single appliance
- Facilitate policy tuning with "what if" scenario alerting
- Correlate events to network and session activity using a built-in network flow collector & firewall
- Utilize exploit, vulnerability & anomaly based detection
- Act upon locally-detected threats or network-wide threats detected using optional NitroView appliances

Used in conjunction with NitroView, NitroGuard IPS is also able to actively block activity based on network-wide analysis of network, event, user, and application behavior.
Advanced Threat Detection
In addition to over 7,000 custom detection signatures, and network-based anomaly detection, NitroGuard IPS also provides a full state-aware firewall, and provides real-time correlation of all events to network flow activity—resulting in more accurate threat detection out of the box. In addition, when used with NitroView Enterprise Security Manager, NitroGuard can act dynamically based upon global information analysis and correlation, enabling NitroGuard to block zero-days, multi-path attacks, and even insider threats.

Maximum Performance
NitroGuard is tested with the full default signature set enabled, meaning the specified throughput of each model is actually achievable. NitroGuard also multitasks, and uses customized, performance-tuned pre-processors for many common protocols—fully leveraging the capabilities of each purpose-built appliance.

Minimum False Positives
A properly tuned IDS or IPS means fewer false positives. NitroGuard’s baselining capabilities, paired with “what if” alerting options, make policy tuning easy—resulting in better overall detection capability, and fewer false positives.

Multiple Personalities
Not all networks operate the same, which is why NitroGuard IPS supports multiple virtual policies, which can be assigned by physical interface or virtual LANs to deliver tuned detection policies to specific areas within your network. This enables NitroGuard IPS to provide different levels of enforcement between internal networks than it might to DMZ or Internet-facing interfaces.

Network Flow Collection
Because Intrusion Prevention Systems are often deployed in-line, they’re perfectly situated for the collection of network flow information. NitroGuard monitors network activity and correlates it directly to observed event activity, and also provides flow data to NitroView ESM for analysis and retention.

Built for Reliability
NitroGuard was designed with redundancy and reliability in mind—enough to earn Common Criteria EAL3 certification and FIPS 140-2 Level 2 validation, meaning NitroGuard is suitable for deployment within the most critical networks. All appliances are custom-built and fully hardened, and include built-in network bypass. In addition, all events and flows are backed up locally on the appliance, ensuring that NitroView receives all event data even if there’s an interruption in network communication between the devices.
## NitroGuard Intrusion Prevention System Specifications

<table>
<thead>
<tr>
<th>Model</th>
<th>Description</th>
<th>Throughput</th>
<th>Interfaces</th>
</tr>
</thead>
<tbody>
<tr>
<td>NS-IPS-5450-R</td>
<td>NitroGuard IPS 5000, 3U IPS appliance supporting approximately 5 Gbps &amp; 1.2m connections. Includes redundant power supply and network bypass capability.</td>
<td>5 Gbps</td>
<td>4 or 10Gbps fiber, or 12 x 1Gbps copper</td>
</tr>
<tr>
<td>NS-IPS-4245-R</td>
<td>NitroGuard IPS 4000, 1U IPS appliance supporting approximately 2 Gbps &amp; 1.2m connections. Includes redundant power supply and network bypass capability.</td>
<td>2 Gbps</td>
<td>2 or 4 x 1Gbps fiber, or 2, 4 or 8 x 1Gbps copper</td>
</tr>
<tr>
<td>NS-IPS-2250-R</td>
<td>NitroGuard IPS 2000, 1U IPS appliance supporting approximately 750 Mbps &amp; 1.2m connections. Includes redundant power supply and network bypass capability.</td>
<td>750 Mbps</td>
<td>2 or 4 x 1Gbps fiber, or 2, 4 or 8 x 1Gbps copper</td>
</tr>
<tr>
<td>NS-IPS-2230-R</td>
<td>NitroGuard IPS 2000, 1U IPS appliance supporting approximately 500 Mbps &amp; 1.2m connections. Includes redundant and network bypass capability.</td>
<td>500 Mbps</td>
<td>2 or 4 x 1Gbps fiber, or 2, 4 or 8 x 1Gbps copper</td>
</tr>
<tr>
<td>NS-IPS-1225</td>
<td>NitroGuard IPS 1000, 1U IPS appliance supporting approximately 250 Mbps &amp; 1.2m connections. Includes single power supply and network bypass capability.</td>
<td>250 Mbps</td>
<td>2 or 4 x 1Gbps fiber, or 2, 4 or 8 x 1Gbps copper</td>
</tr>
</tbody>
</table>

NitroGuard supports out-of-band (IDS) and/or in-line (IPS) detection of:

- Exploits and vulnerabilities
- Malware, trojans, viruses, and worms
- Scans, sweeps, and backdoors
- Denial of Service (DoS) attacks
- Network anomalies

When used with NitroView ESM, NitroGuard can also block:

- Complex attacks, including multi-path and multi-stage attacks
- Insider theft
- Compliance policy violations
- Data leakage
- Suspicious traffic based on user and application behavior anomalies
Integrating inline intrusion detection & prevention with powerful analytics, application monitoring, and database activity monitoring

Because security best practices recommend defense-in-depth, NitroGuard IPS was designed to work in concert with other information monitoring solutions to provide dynamic and adaptive security that takes all aspects of information security into account.

When used with NitroView ESM, NitroGuard IPS can blacklist traffic based upon much larger threats, detected through multi-device event correlation, direct database monitoring, or even application content inspection. Every one of our appliances is fully integrated, providing central device and policy management in addition to a better overall security profile—all in a “single pane of glass.”

NitroView Enterprise Security Manager (ESM) and NitroView Enterprise Log Manager (ELM)

NitroView ESM is the world’s fastest and most scalable SIEM, providing an enterprise-class security information and event management system that identifies, correlates, and remediates threats in minutes instead of hours. Tightly integrated with NitroView ELM for compliant log retention and management, NitroView bridges the gap between log management and SIEM, providing powerful risk and threat detection, event analysis, full forensic capability, and compliance reporting—all from a single highly integrated system.

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 for your 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.

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