

# Security Overview

## Customer Objective

Even the best perimeter defenses cannot stop all of today's external security threats, and they are virtually useless against internal threats. To truly secure your information infrastructure, you need to know exactly what is happening across your entire network and IT infrastructure, all of the time.

Network Intelligence provides the only security information and event management solution that delivers 100 percent visibility into all security threats across your entire information infrastructure — from switches and routers, to security devices, host assets, applications, servers and storage.

Network Intelligence accomplishes this through the real-time aggregation and analysis of All the Data™ from all networked elements in its LogSmart® Internet Protocol Database™ (IPDB). With the use of Network Intelligence's baseline learning system, you can see exactly what usual — or unusual — patterns are forming on your network, enabling you to identify security threats literally anywhere in your network, even in remote locations.

## Network Intelligence Security Solutions

Complexity is the enemy of security. And today, most enterprise security infrastructures are incredibly complex, with large numbers of disparate security systems distributed throughout the network.

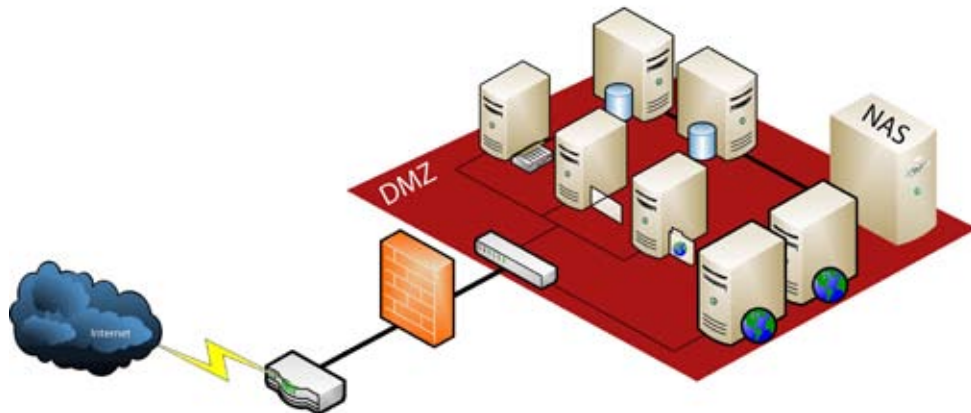
Network Intelligence provides security solutions that radically simplify security management by consolidating, normalizing and analyzing data from this complex infrastructure. For customers, this significantly improves security effectiveness because they can respond faster to external threats, and uncover internal ones by gaining unified and comprehensive visibility over their networks.

## The Network Intelligence Internet Protocol Database

Using its advanced LogSmart IPDB architecture that is deployed in hundreds of enterprises worldwide, Network Intelligence is able to capture All the Data from network, security, host, application and storage layers across the enterprise. LogSmart IPDB analyzes both real-time and historical data and presents information in views and reports designed to meet the far-ranging needs of everyone in your organization — from the IT department, to the security department, to the compliance and risk officers and executive management.

The benefits of LogSmart IPDB include:

- Designed to store and work efficiently with unstructured data natively without any filtering or data normalization
- Maintains a digital chain of custody for all data which assures that once data is committed to the database, it can never be altered — unlike most data schemas used in RDBMS-based solutions
- No agents are required
- Distributed peer-to-peer architecture enables high scalability and performance



Through the LogSmart IPDB, Network Intelligence enables customers to radically improve their security posture through:

- **Access-Control Enforcement** — Comprehensive auditing and reporting capabilities to enforce access-control policies enable customers to immediately detect when misuse occurs and enforce accountability for both privileged and non-privileged access to network, computing and object-level components.
- **False Positive Reduction** — The automatic correlation of reported attacks to asset and vulnerability data significantly reduces incident-handling costs and enables critical security-analysis resources to concentrate on serious events of interest.
- **Real-Time Monitoring** — A unified view into the relationships of the events occurring across the enterprise greatly enhances customer practices that have been defined and built around the continuous real-time monitoring of network, system and security-event information, enabling users to immediately determine “what is happening” across the enterprise.
- **Unauthorized Network Service Detection** — The detection of rogue services that utilize “open paths” through network defenses enables customers to shut down network access that would otherwise lead to information leakage, privacy liabilities and illegal content transfer across the enterprise.
- **Watchlist Enforcement** — Parameterized event and alert analysis provides significant operational efficiencies and enables customers to determine their external and internal risk exposures to offenders, who are identified by network addresses and user names that target specific service and systems in the enterprise.
- **Correlated Threat Detection** — The goal of enterprise-wide security becomes a realization through the automated process of examination of network, security and system events in terms of vulnerability, risk and threat assessments across all enterprise locations.

### About Network Intelligence Corporation

Network Intelligence is the market-proven leader in transforming enterprise-wide data into automated compliance and security information. The Company’s LogSmart® Internet Protocol Database™ (IPDB) provides the only architecture proven to efficiently collect and protect All the Data™, from any IP device, without filtering or agents. Network Intelligence takes the cost and complexity out of compliance and security for hundreds of customers worldwide, including five of the *Fortune 10*.

### A Framework for Security Operations

Security Environment				Security Objectives		Product Capabilities
Perimeter Network Operations	eCommerce Operations	Internal Systems and Application				
			<b>Access-Control Enforcement</b>	› Privileged user monitoring › Corporate policy conformance	✓ Log Management	
			<b>Real-Time Monitoring</b>	› Troubleshoot network & security events › “What is happening?”	✓ Asset Identification	
			<b>False Positive Reduction</b>	› Confirm IDS alerts › Enable critical alert escalation	✓ Baseline ✓ Report & Audit	
			<b>Correlated Threat Detection</b>	› Watch remote network areas › Consolidate distributed IDS alerts	✓ Alert ✓ Forensic Analysis	
			<b>Watchlist Enforcement</b>	› External threat exposure › Internal investigations	✓ Incident Management	
			<b>Unauthorized Network Service Detection</b>	› Shutdown rogue services › Intellectual property leakage		
			<b>SLA Compliance Monitoring</b>	› Proof of delivery › Monitor against baselines		