



nFX Log | One

Finally, powerful log management... that's simple

nFX Log One from netForensics makes managing the overwhelming volume of event logs from across your enterprise easy – giving you streamlined, automated, end-to-end log management for all of your risk management and compliance needs. nFX Log One simplifies compliance, reporting, and audit documentation, providing security insight and support for regulatory measures like PCI, SOX, HIPAA, FISMA, ISO 17799, GLBA, and Basel II. Now, you can collect, secure, store, and take action on your log data easily – and in real time. The result? Better visibility, improved operations, and reduced costs – along with the power to transform your log data into actionable intelligence.

Strong log management – for rigorous security and smooth operations

Chances are, your organization is subject to security-related regulations or industry standards, so effective log management is critical to you. If so, you face audit and control reviews at least once a year and are accountable for any policy violations, as well as breaches in the use of sensitive customer, cardholder, or patient information. So you need to collect and archive your log data efficiently, while alerting and reporting intelligently. Ultimately, you need a log management solution that enables you to address three primary concerns:

- **Compliance and policy readiness**
- **Security incident identification, reporting, and forensics**
- **Efficient, streamlined, end-to-end log management operations**

To meet these objectives, you need to regularly review logs, securely store logs, and report on log management activities. Yet these tasks can be complicated and resource intense, especially as log volume grows. Most low-cost log management solutions lack the extended features and automation capabilities you need. And full-featured solutions are typically expensive and difficult to deploy. nFX Log One is the single answer to all of your log management challenges.

With nFX Log One, you now have the complete and scalable solution you need – all at an affordable price. nFX Log One:

- Combines centralized log and event alerting with powerful archival, forensics, and trending analysis tools
- Features a flexible, multi-tier architecture that scales to effectively collect massive volumes of data from operating systems, business applications, network devices, security devices, mainframes, access control systems, Web services, and databases
- Offers a centralized repository to efficiently store log data, and features an innovative Web-based console for easy log analysis, reporting, and audit purposes
- Uses event normalization to convert event log data into a common format for quick analysis and reporting
- Maintains secure audit trails for compliance, audit, and policy enforcement
- Warns you, in real-time, when suspicious activities are detected

The industry's most complete and cost-effective log management solution

With nFX Log One, you can now address all of your log-related security concerns with a single solution. You can tackle compliance, identify and report on security incidents, take appropriate action, and enjoy smooth, end-to-end log management operations in the process. A key product

in netForensics' nFX One suite of security compliance management solutions, nFX Log One not only incorporates all the comprehensive log management capabilities you need, but is also flexible, scalable, and affordable – and surprisingly easy to use and maintain.

Flexible, Scalable, End-to-End Log Collection and Storage

- Collects log data from a wide range of systems, applications, databases, and devices, including traditional log data such as Windows Events and syslog, plus binary or proprietary applications and systems
- Captures important audit information such as user access, application and network data, and much more
- Offers advanced filtering and configuration options at the agent level that provide administrators more flexibility in customizing their data collection methods to meet compliance and storage requirements
- Maintains the integrity of the raw logs through sophisticated compression, digital signing, and validation, allowing you to apply centrally managed policies to the consolidated repository
- Compresses data up to 95% to use less bandwidth, speed data transfer, and reduce storage
- Stores normalized and filtered data in a centralized, scalable database for robust, single-source reporting
- Provides 64-bit support to leverage enhanced capabilities of Windows platforms

Continuous Monitoring and Alerting on Suspicious Activity and Policy Violations

- Provides continuous log aggregation and monitoring
- Automatically highlights any vulnerabilities, weaknesses, noncompliant activities, and policy violations
- Supports the requirements of recurring security risk assessments
- Alerts in real-time for critical security events, service interruptions, and performance threshold breaches
- Automatically sends alerts to security consoles, email, pager, or cell phone of the appropriate IT staff

Actionable Reporting, Visualization, and Alerting

- Offers reporting for audit, management, and forensics
- Features an enhanced, intuitive Web-based console for complete log visibility, efficient reports administration, and timely security and compliance report updates
- Visually tracks and summarizes activity to ensure managers are aware of security and compliance hot spots
- Delivers summary-level reports to keep executives informed of overall trends
- Includes drill-down capability for routine management, and query-based data mining for trend analysis and reporting
- Replays user sessions for forensic analysis

Powerful Audit and Compliance Readiness Capabilities

- Provides audit trails and reporting to ensure you meet and demonstrate compliance
- Automatically alerts you to noncompliant activities
- Meets an array of regulatory requirements and industry standards (such as SOX, HIPAA, FISMA, FDIC, GLBA, ISO 17799, and PCI)
- Pre-packaged with a comprehensive set of compliance reports

Flexible, Easy-to-Use Rules and Policy Management

- Includes predefined security rule sets and reports for quick startup
- Enables new rules that are easy to create and rule sets that can easily evolve along with best practices, industry standards, and regulatory requirements
- Helps ensure that internal security controls and sound security policies are in place
- Continuously and automatically evaluates your systems for policy violations

nFX One Solutions

netForensics delivers security compliance management solutions to meet security challenges in a new and comprehensive way. With solutions for monitoring both internal and external threats, organizations can gain visibility across the entire enterprise – from the perimeter to the core – for an innovative, intelligent approach to the sweeping challenge of maintaining information security while in the process ensuring compliance with regulatory mandates.

Contact us to learn more about these other netForensics products:

nFX SIM One, with patented, high-performance SIM technology, empowers organizations to transform huge volumes of complex security-related event data into understandable, actionable information. This streamlined, easy-to-deploy SIM solution allows organizations to respond to security events in real time – for active compliance management from the perimeter to the core.

nFX Data One gives enterprises of all sizes a new level of insight into user access, so you'll know who's touching critical data in your databases and applications – at all times across the enterprise. nFX Data One protects organizations from data breaches and insider threats by monitoring and alerting on any malicious and unauthorized activity that may jeopardize your data.

About netForensics

netForensics delivers security compliance solutions that help stop the ever-increasing attacks that threaten organizations. Through its patented nFX technology, netForensics not only solves security compliance challenges, but provides the proof needed to address the myriad of regulatory and internal governance requirements. The netForensics' suite of solutions enables governments and organizations to address external and internal threats, mitigation, log management and reporting. Governments and companies of all sizes around the world rely on netForensics to gain unparalleled security visibility, prevent costly downtime, and achieve and maintain compliant operations.

For more information on nFX Log One – and the suite of nFX One security and compliance solutions – please call 732-393-6000 or e-mail info@netforensics.com