



## Federal Solutions

Our Security Information and Event Management (SIEM) solutions provide a top layer of correlation, analysis and intelligence across the portfolio of deployed security systems and devices, providing much-needed context and support for security decision-making. SIEM transforms noisy, low-level security event information generated by firewalls, intrusion-detection systems (IDS), and other devices into alerts and work-flows that can be readily comprehended by security analysts. Further, netForensics SIEM drastically reduces false positives based on its ability to correlate with multiple sources of security information. Security is enhanced while analyst efficiency is improved.

### Who We Are

Founded in 1999, netForensics pioneered the security information management technology sector and continues to operate in the vanguard of the industry today. Our team of leading experts understands the ever-evolving security threat and compliance needs of both private and public organizations. For over ten years, we have delivered reliable, innovative products that security and business managers stake their careers on every day. From the largest government agencies, companies, and service providers running complex networks, to small and mid-tier businesses, customers across the globe rely on netForensics for cost-effective security information management solutions. We help companies in every industry see and eliminate threats, secure valuable assets, and solve pressing compliance challenges.

Regulatory compliance is another key netForensics value. Support for FISMA, DIACAP, PCI, GLBA, and SOX are built into our analysis and reporting engines. According to a recent Forrester survey of 1,335 security decision-makers, 32% buy SIEM technology for compliance and reporting. There is little alternative to SIEM when a holistic approach to compliance reporting and incident management is critical. netForensics makes it easy for you with pre-designed compliance frameworks and reporting.

netForensics provides a breadth of SIEM technologies. These technologies include nFX SIM One, built for high-end SIEM applications appropriate for large-agency data centers; and our appliance-based solution - nFX Cinxi One, which provides an integrated log management solution along with correlation and remediation functions. netForensics also has strategic relationships with some of the nation's largest and most experienced security service outsourcers and can work with its federal customers to find a managed service provider that is best-suited to the need. And finally, netForensics provides a complete suite of professional services to assist federal agencies with their security initiatives via our SOC One team of security professionals.

netForensics is fully committed to working with the federal government and continually tunes its technology and operations to federal needs. Our federal credentials include:

- Providing support for monitoring, incident response, and risk management—as mandated by NIST and Federal Information Processing Standards (FIPS) Publications 199 and 200
- Army CON (Certificate of Networkiness) certification for our CINXI technology. We are deployed in various NECs and Test Centers. netForensics is in full compliance with the Army Enterprise Infrastructure's strict standards for security, compatibility, and sustainability.
- nFX SIM One adheres to the new SP-800 reporting framework and is the industry's first solution that connects the Federal Enterprise Architecture with the Information Security Management via seamless integration with the uCmdb. This integration makes it easier for agencies to adopt the new 6 step Risk Management-based framework process outlined in Special Publication 800-37 that is required for certification and accreditation.

Also, the nFX SIM One FISMA compliance framework provides a multitude of views and reports that support the SP 800-60 guidelines from the FISMA Federal Enterprise Architecture Business Reference Model and SP 800-53A controls. This FISMA-related information is easy to find, launch, and use, and includes reports to address each of the eleven different controls in the Business Reference Model.

- nFX One supports open source, GOTS and COTS, as well as the real-time monitoring of mobile, tactical, and field operations. All data can be forwarded to regional hubs and security operations centers.
- FIPS 140-2 Certification for Encryption for Communication Channels pending
- netForensics hold the U.S. Patent for SIEM technology.
- Certifications
  - *CVE Compliant*
  - *FIPS 140-2 Certified Encryption for Communication Channels*
  - *NIAP EAL-2+ IDS Analyzer, Protection Profile Certification*

## Federal Experience

netForensics is an active participant in the federal community with many customers and forums for dialog that shape our approach, including the annual nFX Federal User Group. Designed exclusively for netForensics' federal customers, it brings together industry experts and the netForensics' executive team for two days of education, strategy, peer networking, and training.

Our federal customer list includes:

- Department of Energy
- Environmental Protection Agency
- Various Army NECs and Test Centers
- USDA Forest Services
- Defense Threat Reduction Agency
- Small Business Administration

### Our Mission

netForensics secures our federal customers by providing complete situational awareness and severity of all threats generating actionable security intelligence for attack remediation and compliance reporting - from the edge, to the data center, to the cloud.

## Why netForensics

Protecting valuable federal data, sustaining the availability of the nation's critical infrastructure, streamlining federal compliance reporting, and helping security analysts focus on the top priority problems, are some of the key benefits of working with netForensics.

In addition, we can address a broad range of needs and price-points with a product line that scales from departmental level to the largest agency-wide data center environment. Further, we are the only SIEM vendor to implement a fully federated architecture that allows you to add "satellite" devices, such as collectors and correlation engines, to accommodate growth, without having to re-engineer the database and reporting engine. This saves you money and enables you to move quickly to address an expansion in your environment.

netForensics can interoperate with hundreds of other security products and systems, allowing you to select best-of-breed for your array of IT defenses; and does so without putting a performance load on those third-party devices.

Commitment, federal experience, a solution for better security, tools to address compliance, and an architecture that ensures high-performance at all levels of scale, are all reasons why netForensics is the best choice in SIEM for federal government.

## Contact Us

For more information on how netForensics solutions helps address Federal security and compliance requirements contact:

**Dhani Abey - Federal Accounts Manager**  
**Phone: 1-732-393-6036**  
**Mobile: 1-732-241-2152**  
**Fax: 1-732-393-6025**  
**Email: [dhani@netforensics.com](mailto:dhani@netforensics.com)**

