



NFX FOR MSP SOLUTION BRIEF

SP Monitor™

Jump Start Security-as-a-Service

Designed to give you everything you need to get started immediately providing security-as-a service, SP Monitor is a real-time event monitoring platform coupled with a full complement of customer-ready reports and procedures to get you up and running quickly. This award-winning software powers security in the cloud for some of the world's leading service providers, yet it is cost-effective enough to support the demands of any sized environment.

SP Monitor serves as the base module for easily adding additional security modules from our nFX One solutions suite, such as global threat detection, integrated trouble ticketing, compliance reporting, and much more. The first step to security is monitoring. Add even more value once you have this critical component in place.

SP Monitor: A Powerful Platform for On-Demand Monitoring and Reporting

Capabilities Overview

Our **nTier Architecture** means nFX One scales by distributing agents on the customer site with no hardware. nFX One's nTier scales both horizontally and vertically—a critical feature in volatile cloud deployments. Vertically, nFX One leverages and optimizes high performance hardware such as multiple, multi-core CPUs and high performance RAM at the cloud site. Horizontally, nearly unlimited numbers of data collectors, engines, or combinations of both can be added as your MSP security environment grows.

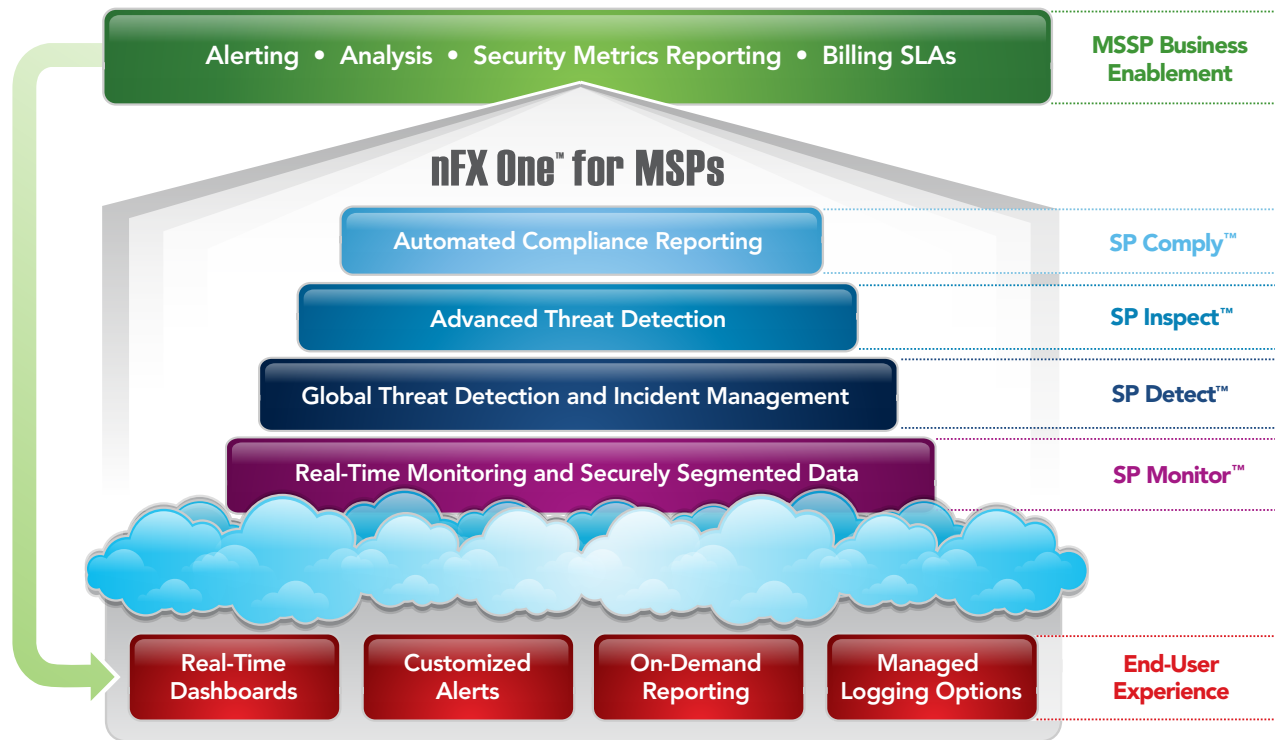
nFX One gives MSPs the agility and power they need to confidently grow their security services business.

Armed and ready to meet the challenges of security in the cloud, nFX One is the only technology designed to handle the complexity of collecting, correlating and processing security events across multi-tenant environments. nFX One gives both you and your customer understandable, actionable security intelligence. Other nFX One benefits include:

- **Robust, multi-tier architecture that easily scales for growth**
- **Unparalleled visibility across all customer environments**
- **Identifies the most stealth external or internal threats**
- **Reduces volumes of security noise, identifying true threats**
- **Proactively monitors customer sites to help stop attacks in their tracks**
- **On-demand reporting , real-time alerting and incident management**
- **Meets customer demands for compliance, audit and governance reporting**

Monitor. Detect. Inspect. Comply. The full suite of nFX One SP solutions act as an integrated platform to give you and your customers a full range of security and compliance options. Implement only the modules you need. Add functionality as you grow. Every module is time-tested in data centers and MSP SOC's around the world. Now you can offer top-tier security services with confidence and expand your service business with little up-front cost or extensive training.

The nFX One architecture is fully federated for high performance and scalability across any network, regardless of the number of customers or locations. This also means there is no single point of failure, and the application is automatically distributed to optimize performance based on users and event volume. The multi-tier architecture also allows you to minimize hardware requirements on your end. Affordably expand your infrastructure only as you grow your customer base and business.



The nFX One SP Solutions Suite brings a comprehensive set of security competencies together for a complete solution.

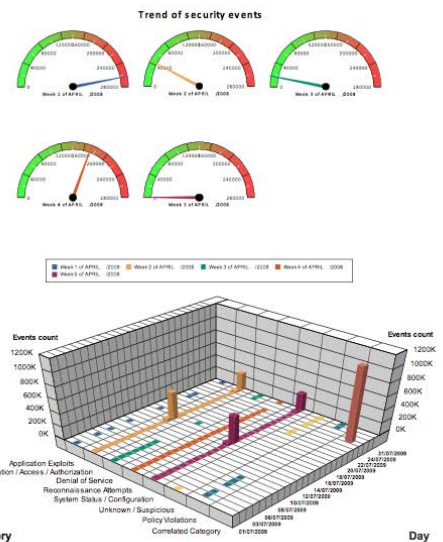
Multi-Device Integration supports a broad array of device types for true end-to-end security visibility across your customers' network. nFX One integrates natively with hundreds of network and security devices, applications and databases, and most importantly, these connections don't require installation on the actual devices themselves and can be administered remotely. In rare cases, where a device or application is unsupported, netForensics can assist you in developing and maintaining new collectors to incorporate customer device data into your nFX One platform. nFX One captures 100% device event data from every field in every event. You have full granularity and accuracy of security information at your fingertips.

Account Segregation System silos data for the complete privacy, protection and integrity of individual customer information. Customer data is never exposed. With its comprehensive permissioning and segregation system, nFX One keeps each of your customers' data protected and separate. Single-customer-views give your analysts instant access to their data, but they can also view information across multiple customer locations as well. This segregation also extends to customer device types, as well as your analyst team access. Analyst permissions can be tailored not only to customer data but also to specific devices and device types within the customer site, delivering the market's most fortified security platform for MSPs today.

Account Visualization System makes it easier and less costly for your analysts to identify and investigate suspicious activity across your customer base. Graphical dashboards and charts that illustrate dependencies help analysts quickly identify incidents. Analysts can create custom views of individual customer accounts using our standard visuals and templates. These views can be customer-specific or used with multiple customers. All dashboards are layered with key information that simplifies managing customer networks. Analysts can easily drill-down through high level summary information to retrieve more detailed views, or set up alarms that direct them to do so when needed – enabling them to quickly identify malicious activity.

Virtual Account Views give customers real-time insight into their own security posture through a web-based portal without calling on your analysts. Customers can view scheduled reports, or you can grant them their own limited view to the actual nFX One platform.

Customer Alerting informs your team of critical activity on a customer-by-customer basis. Realistically, your security teams can't effectively watch security events streaming in real-time across multiple customer networks. Without an automated solution, even the most skilled analysts can have a difficult time telling the difference between true attacks and noise, and watching monitors all day is a waste of their valuable time. nFX One's automated alerting enables your top analysts to do more consultative, preventative, higher-valued work on behalf of their accounts, knowing that when a malicious activity occurs, they will receive an automated alert (e-mail, SMS, page) to immediately respond. The analysts can choose how and when to be notified based on each of their managed customer accounts.



nFX One's real-time console is easy to use, yet powerful, with drill-down and drag-and-drop capabilities at the workstation. The powerful GUI enables visibility and management of individual end-user customer environments. Your customers gain valuable insight into their security posture with no impact to your support team's operations.

With the complete suite of SP Monitor reports, you have numerous ways to demonstrate to customers the value you provide in protecting them from potentially damaging threats.

Customer-Ready Security Reports offer robust yet streamlined reporting and analytic tools for security, risk management, performance management and operations. Through an assortment of comprehensive reports, nFX One leverages data from devices, applications, and databases, for the most granular cloud security reporting suite available today. Robust reporting incorporates real-time and historical data for a comprehensive understanding of your organization's security picture at any point in time.

SP Monitor reports include:

- All events and their severity, time period and trends
- Top attackers by source and country
- Top IDS/IPS signatures identified
- Most frequently attacked hosts, device types and destination ports
- Incidents by type of attack including:
 - *authentication, access and authorization violations*
 - *policy violations*
 - *application exploits*
 - *denial of service*
 - *reconnaissance attempts*
 - *application exploits*

...and other types of events

Remote Updates and Patch Management: nFX One features a unique remote, centralized update and patch management technology that centralizes the update process to a server and allows that server to decide when to push the patch to each component. By eliminating the need to install and run the application on your customers' servers, nFX One alleviates the CPE burden of maintenance and ongoing support, not to mention the inevitable service calls for broken or mis-configured equipment.

Fault Tolerance and Load Sharing: provides multiple forms of failover that guarantee nFX One will be up and running regardless of the size and traffic flow in your infrastructure. Unlike an appliance or a two-tiered SIEM architecture that features tightly coupled application and database layers, nFX One gives customers the flexibility to create redundancy at every level of the platform within one site or across a distributed installation. nFX One provides agent collector-to-engine, engine-to-engine, and database-to-database failover to create redundancy across the entire distributed installation. This provides an important alternative to SIEM solutions that have a single point of failure, and guarantees that operators have continuous access to real-time and historical security information with zero down time.

Extend Your Offerings with Logging-as-a-Service: With SP Monitor, you have the option of adding managed logging services that address customer requirements for local control of security event data. By adding Cinxi log management appliances at your customer's site, you can quickly deliver a cost-effective solution for on-premise log retention and management. In addition to storing logs locally, they are also forwarded to your central nFX One platform. Cinxi data is presented in a "single pane of glass" view, giving your team clear visibility into the activities at each customer site. netForensics' award-winning Cinxi appliances are available in a variety of pre-configured models that are easy to set up and manage.

nFXpert Services: Accelerating Time-to-Value

The SP Monitor module of nFX One includes in-depth configuration, design and implementation services. Our nFX experts will work side-by-side with your team to thoroughly test your new monitoring platform before it ever sees its first customer. Designed to accelerate your new service offerings, we get you up-and-running and delivering reports to your customers fast. SP Monitor customers get nFX Bootcamp training to accelerate the learning curve for your staff. Using our best proactive methodologies and expertise, we help you achieve service efficiencies and make sure you have all the tools in place to easily on-board new customers, add additional devices and lay the groundwork for adding even more security offerings.



About netForensics

For over a decade, netForensics security solutions have helped managed service providers, enterprises, and government agencies around the world to manage risk, protect critical assets, and maintain compliant operations. netForensics' nFX One solution suite has been designed to address the unique needs of MSPs by providing flexible, on-demand delivery models that automate threat detection and incident management in high volume, multi-tenant environments. Many of the world's leading service providers rely on netForensics to grow their security business and reduce the cost of providing security-as-a-service.

For more information on netForensics and the suite of nFX One solutions for MSPs, please call us at **732-393-6000** or e-mail info@netforensics.com



netForensics, Inc. | 200 Metroplex Drive • Edison, NJ 08817 | T 732.393.6000 F 732.393.6090 | info@netforensics.com

netForensics, the netForensics logo, nFX, nFX SIM One and nFX Data One are trademarks of netForensics, Inc. Other third-party trademarks are the property of their respective owners.
© 2008 netForensics, Inc. All Rights Reserved.