Contents

1 Executive Summary

1 The Information Security Landscape

1 Security Management Challenges

2 Security Decision Support Solutions

2 Maintaining the Continuity of Business Operations

2 Compliance

2 Threat and Risk Management

3 Security Performance Measurement

3 Unified Network and Security Management

3 Security Information Management: The Backbone of Security Decision Support

4 Actionable Security Intelligence and nFX One solutions

4 Actionable Security Intelligence

4 Enterprise-Class Security Decision Support

4 Scalable, Robust SIM Architecture

4 Correlation Technology and Processing Power

4 Visualization, Reporting, and Analysis

5 Incident Resolution Management Workflow and Embedded Security Knowledge

5 Database and Application Security Monitoring

5 Conclusions

5 About netForensics
Executive Summary

Today, enterprises around the globe face unprecedented demands to comply with strict security and privacy legislation. At the same time, companies continue to search for the most reliable and efficient means for protecting critical business information in the interest of intelligent business management. To accomplish both, companies must take a comprehensive approach to security management, aligning business security programs with compliance initiatives.

A centralized, integrated approach to security management enables organizations to effectively manage isolated silos of data and diverse security management technologies. Building an effective security decision support solution requires a proactive strategy that includes threat and vulnerability identification, comprehensive insight into security posture, automated incident response processes, and continuous improvements to security posture and policies.

Enterprise security information management (SIM) is the backbone to an effective, comprehensive security decision support program. With SIM, companies can rationalize volumes of security data from disparate networks and devices, then rapidly deliver usable information to the right people and technology domains across the enterprise. nFX SIM One transforms security data into actionable security intelligence, delivering comprehensive security decision support that provides a strong, proactive risk management platform while helping companies manage and maintain continuity of operations.

The Information Security Landscape

The information security landscape has changed dramatically in recent years. While the network hacker continues to pose a threat to application and data integrity, regulatory compliance has shifted the information security focus from external to internal. Whether contending with the Sarbanes-Oxley Act (SOX), the Health Insurance Portability and Accountability Act (HIPAA), the Gramm-Leach-Bliley Act (GLBA), the Federal Information Security Management Act (FISMA), 32 state laws, or other compliance challenges, companies must prove diligence in managing information security risk.

Maintaining secure, risk-free operations continues to increase in complexity, consuming valuable resources in the process. Service-oriented architectures are increasing the pace of application development and deployment. Networks are comprised of more and more applications and data with greater distribution across the enterprise and beyond, creating more access points to critical data. Though visibility into real-time threats and vulnerabilities is called for, most organizations lack the comprehensive tools, skills and technology needed to leverage information security data for actionable security intelligence.

Security Management Challenges

Developing and implementing an effective security management system comes with many challenges for organizations, particularly with the recent explosion of legislation regarding the privacy and security of information. Executives and information technology groups find themselves more accountable for security requirements and compliance auditing than in the past. Closely examining the details of company security postures is exposing potential vulnerabilities and inefficient processes previously unimportant or even unrecognized, including the following:

- **Disconnect Between Security Programs and Business Processes** – Immature information security programs are often not well integrated into standard business processes, creating an enterprise-wide information disconnect along with enormous process inefficiencies.

- **Fragmented Security Information, Processes, and Operations** – Information security often takes place in organizations within silos. For instance, separate databases and unrelated processes might be utilized for a company’s audit assessments, intrusion detection efforts, and antivirus technology. For these organizations, developing an integrated approach to SIM can be a great challenge.

- **Security Performance Measurement Difficulties** – Many organizations struggle with performance measurement and management, and developing a standardized approach to information security accountability can be a daunting task.

- **Broken or Nonexistent Remediation Processes** – Previously, compliance and regulatory requirements called for organizations to simply log and archive security-related information. Now, auditors are requesting in-depth process documentation, showing not only evidence of the threat response, but exactly what was responded to and precisely how. The connection between threat identification and the remediation or mitigation is becoming increasingly important, along with the ability to prove it.
Abnormal User Activity and Data Leakage Identification –

With today’s security requirements, organizations need to quickly and efficiently add processes that can facilitate incident identification and the detection of anomalous behavior.

Clearly, organizations are discovering that being prepared to react to security threats is not enough. A proactive approach is necessary, given the complexities and challenges now inherent in security management.

Security Decision Support Solutions

A proactive, comprehensive approach to security involves many components to be successful. Several, though, are key to addressing the critical elements of SIM: business services continuity, compliance, threat and risk management, and security performance measurement.

Maintaining the Continuity of Business Operations

Continuity of the security management program across an organization and within its strategic business applications is key to proactive risk management and compliance success, and can be accomplished with an effective security decision support solution. Organizations must be able to predict where most threats might occur, and how they might impact the ability to keep business processes moving, to service customers, and to run a profitable business. Yet data is constantly in motion, continually consumed by users and applications across the enterprise. Additionally, the increased deployment of service-oriented applications increases the number of users with potential access to enterprise data. Service-oriented applications have many moving parts, and monitoring security information at the application layer is considerably more difficult than monitoring network activity, given the complexity of the data. A security decision support solution should provide monitoring of applications and their data, in addition to monitoring security devices. Then, when immediate and unexpected threats occur – in networks, applications, and databases – organizations have the capability to react quickly with a well-tuned, comprehensive incident response plan, so that systems and business processes continue running smoothly.

Threat and Risk Management

As businesses mature and networks grow to vast webs of dynamic information and assets, organizations shift their security regiments from trying to address all security issues to establishing security protocol priorities. The larger, more complex organizations choose to focus on the most important assets, the most damaging threats, the potential intrusions that will have the greatest financial impact, and those security issues that can cause the most disruption to business processes within the organization. In the post-Internet era, the focus for security organizations has been on stopping threats from outside the enterprise. Yet data leakage and inappropriate user activity from inside the enterprise are often bigger threats, since the potential hacker, fraud, error or mistakes from insiders is so much closer to the data. Organizations today are forced to reconsider their approach to managing risk from insiders.

To successfully mitigate insider threat, a security solution must do more than monitor network activity using network behavior anomaly-detection technology or host-based intrusion-detection systems. Organizations must secure databases, application servers, and ultimately applications themselves through proactive monitoring of logs and user activities from identity management systems and within applications.

According to Amrit T. Williams, Research Director, Gartner, Inc., “Application-level security logging is increasingly important because of regulations, increased incidents of data theft, and changes in the threat landscape that lead to more targeted...”
attacks and attacks focusing on the application layer… Organizations should implement centralized application security logging to address a changing threat environment and to support regulatory compliance. 

Effective management of insider threats begins with obtaining complete visibility into all technologies and assets. Security decision support solutions can help businesses factor into their security programs the likelihood of a compromise happening – from both external as well as internal sources – and the severity of potential threats. With a solid decision support solution, organizations can continuously monitor risk levels, where assets could at any moment come under attack, and measure deviations against an established baseline of acceptable security risk.

Security Performance Measurement

Given that organizations cannot manage what they cannot measure, the ability to perform security assessments and benchmarking are key aspects of an effective security decision support solution. Organizations need to understand their security posture at any point in time, and then have the ability to use that as a security baseline to measure against. Also, executive management needs a fast, straightforward, and credible way to have visibility into the organization’s security posture. Rather than pore through a lengthy vulnerability assessment report, with the right security solution executives can view key security information through dashboards that might for instance summarize via graphs or pie charts vulnerabilities within a specific time period or in real-time.

An effective security decision support solution will seamlessly connect people, processes, technology and relevant intelligence across the enterprise. Together, these solutions comprise the SIM technology known today as the next generation in compliance and risk management.

Unified Network and Security Management

Too often, identifying, managing and eliminating threats across the enterprise is a fragmented and ineffective process for businesses and can lead to damaging outcomes. Taking an ad-hoc, trial-and-error approach to identifying, containing, and mitigating threats can result in prolonged network and application outages, lost data, lost revenue, potential compliance violations, and frustrated users. To meet compliance needs and maintain business services continuity, organizations need the capacity for a coordinated response across a unified network and security management infrastructure.

An effective security decision support solution enables a comprehensive, unified view of the impact of security events on key business services, and an effective response mechanism. With coordinated incident response, companies can rapidly detect, contain, and respond to threats, preventing loss, downtime, and compliance violations. With improved collaboration between network and security teams, systems are quickly returned to operational standards following an attack. Organizations can be more proactive, correlating vulnerabilities against high-value assets. SIM capabilities and security intelligence are incorporated into the network management environment in the interest of maintaining business continuity and meeting service-level agreements. With a security decision support solution that supports a unified network and security management practice, organizations can derive more value from existing investments in network management and security technology.

Security Information Management: The Backbone of Security Decision Support

Security decision support can provide a flexible yet comprehensive solution for proactively addressing risk management and compliance challenges. SIM technology is positioned at the heart of the security infrastructure and inherent in the most effective security decision support solutions. A SIM platform transform all information security-related data into actionable security intelligence that can facilitate decisions regarding appropriate mitigation and remediation. Security metrics enable management to take decisive action. SIM also accelerates incident response via a consistent workflow that is repeatable from business unit to business unit.

SIM technology enables organizations to aggregate and rationalize security information from strategic applications and critical compliance-related assets, as well as from the perimeter devices that protect them. Security information is made available to the security organization and beyond, to individuals and technology domains across the enterprise, while supporting IT governance, enterprise compliance, and risk management initiatives.

---

1 Quote from Amrit T. Williams, Research Director, Gartner, Inc.
Organizations must have processes in place that automatically identify not only external security threats, but especially internal threats, since most vulnerabilities lie within an organization’s perimeter. Though businesses rely on perimeter defenses to ward off viruses and worms, unintentional internal data leakage is common. Both the perimeter and internal security information can be managed together to uncover security threat patterns. Information from all deployed devices, such as routers and hosts, is integrated with application and database information, then tied to network information, offering a clear, concise, and relevant view of security information and current security posture. Through an integrated, comprehensive approach to security management, companies can gauge whether they are improving their overall risk posture.

**Actionable Security Intelligence and nFX One solutions**

netForensics offers organizations of all sizes a comprehensive set of security solutions. Powerful and flexible, these solutions provide greater visibility, better intelligence, and more effective response. nFX One SIM solutions feature a variety of tools and technologies to help organizations address even the most complex compliance and risk management objectives.

nFX SIM One is an enterprise-class software solution that transforms volumes of disparate, security-related data into actionable intelligence. Developed for large organizations and managed service providers, SIM One centrally gathers, correlates and reports on security activities across complex and distributed networks. With an integrated knowledgebase, incident remediation workflow and compliance framework, SIM One is uniquely equipped to help organizations maintain a secure posture and audit-readiness.

The nFX Cinxi One family of security monitoring and log management appliances provide organizations of all sizes with an easy, cost-effective means to address data protection and compliance challenges. Particularly well-suited for companies with budgetary and resource constraints, Cinxi combines today’s essential security technologies in a single, high-performance solution that is simple to deploy and use, yet only a fraction of the cost of other solutions.

**Actionable Security Intelligence**

With actionable security intelligence, organizations have a foundation from which to maintain compliant operations. Organizations can better respond to security threats and ensure business continuity. When empowered with actionable security intelligence, organizations can maintain a continuous process of threat collection, identification, and remediation.

**Enterprise-Class Security Decision Support**

With security decision support, businesses can meet compliance requirements through automated threat identification, by reporting against controls, and via incident resolution management. Organizations can maintain business process continuity by leveraging netForensics robust, scalable architectures application monitoring, and unified security and network management. Additionally, they can resolve incidents as they occur. Performance measurement is enabled with metrics to provide baselines for security and performance gauges at the analytical and executive dashboard levels.

**Scalable, Robust SIM Architecture**

The extensive scalability of the netForensics SIM software and appliance architecture cost-effectively supports growth – and reduces the total cost of ownership for the SMB environment. nFX One architectures incorporate data from security and network devices, applications, scanners, and databases to deliver global visibility into all security-related activities, regardless of numbers. Plus, nFX SIM One offers the only multi-tier SIM architecture with full failover to ensure business services continuity and compliance.

**Correlation Technology and Processing Power**

The industry’s most comprehensive correlation technologies go beyond simply logging security information, and instead speed threat identification and provide an accurate picture of risk. These technologies are architected to handle the massive volume of security information from network-related sources as well as server logs, applications, databases, and identity management systems, and pinpoint attacks from the inside and beyond based
on a thorough understanding of network and user activity. The correlation technologies process large volumes of data from the perimeter down to the core to identify real-time threats and historical patterns. Organizations can leverage their broad security knowledge base and correlate the information to uncover threats that would otherwise go undetected, facilitating proactive security management.

Visualization, Reporting, and Analytics

With the netForensics solutions, organizations can visualize threats as well as the security information underlying the threats. Security teams can assimilate information faster and then focus on the real security threats, mitigating vulnerabilities before threats proliferate. The deep level of analytics enables companies to measure compliance, risk, and operational performance so that security analysts, operators, and executives can determine the security posture and take any necessary steps to improve it. Through the in-depth reporting functionality, key stakeholders and especially auditors have ready access to comprehensive compliance data.

Incident Resolution Management Workflow and Embedded Security Knowledge

Compliance success relies more than anything on an organization’s ability to show proof of a repeatable process for effectively responding to threats. nFX SIM One offers guidance through a repeatable incident response workflow, allowing companies to effectively eradicate threats and prevent reoccurrences. Business continuity is achieved with the capacity to follow incidents from identification through resolution. Through actionable security intelligence, the incident remediation process is documented for security policy management and improvement purposes, as well as for regulatory audits. The embedded knowledge base integrates third-party security information that includes a pre-populated database of incidents and how to resolve them.

Database and Application Security Monitoring

nFX One provides the monitoring of database and application activity, in addition to security devices. nFX One, designed with monitoring at the application layer, provides comprehensive database and application security monitoring. The multi-tier architecture can be distributed to where enterprise applications and databases reside. Flexible deployment options allow nFX One to be configured optimally to handle application events, while failover and redundancy guarantee the availability of events from identity management systems, server logs, and traditional network security devices. Dashboards and reports allow everyone involved in the process of enterprise security, including the security team, network operations group, compliance, audit, and line of business managers, and the CIO and CISO, to understand the impact of an application-level incident on business continuity.

Conclusions

Maintaining secure business operations continues to increase in complexity for organizations. To address these complex security challenges, successfully manage risk, and meet today’s compliance demands, organizations require a proactive security strategy and comprehensive insight into security posture. nFX One, with its award-winning SIM technologies, provides actionable security intelligence to ensure continuous business operations, meet risk management needs and address compliance.

About netForensics

netForensics delivers security compliance solutions that help stop the ever-increasing attacks that threaten organizations. Through its patented nFX technologies, 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 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 maintain compliant operations.