



*Transforming security data into
actionable security intelligence*

nFX Open Security Platform

The world's most powerful and proven security information management solution



Next Generation Information Security Solutions for The Highest Level of Security Decision Support

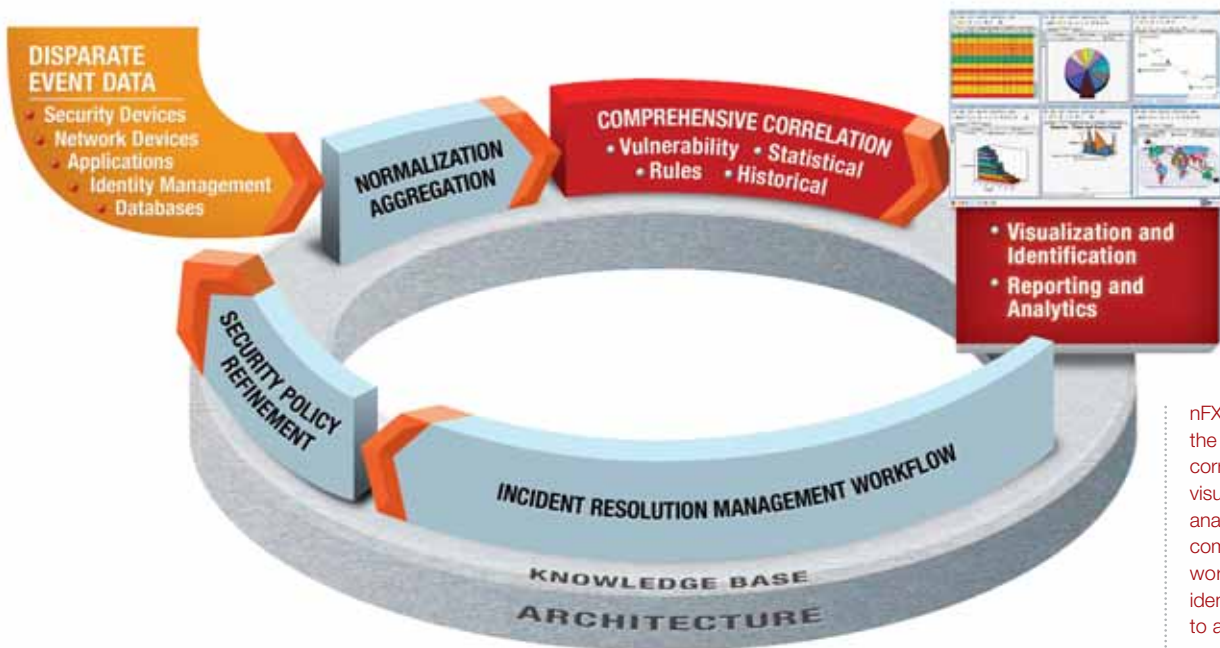
From inside the enterprise to the edge, from applications and databases to network and security devices, netForensics transforms security-related data into actionable security intelligence. Our next-generation, enterprise-class **Security Information Management (SIM)** technology today enables more than 450 organizations worldwide to achieve compliance, reduce risk, ensure continuity of business processes, and accelerate response to threats through comprehensive security decision support.

Powered by the World's Most Powerful, Proven SIM Platform

Every enterprise today faces escalating challenges to maintain secure and risk-free operations:

- Regulatory compliance pressure
- The constant, growing number of attacks explicitly aimed at sensitive data
- The growth in access to this sensitive data caused by the rapid increase and distribution of applications and databases – within the enterprise and beyond
- The heightened imperative to show return on security programs in the form of materially reduced risk

It's the reason that new solutions are called for. These solutions must protect against internal and external threats by allowing the monitoring of applications and databases as well as perimeter devices. These solutions must also provide real-time visibility into the risk posture of key compliance-related assets, delivering truly comprehensive security decision support. Across the board and enterprise-wide, netForensics is answering with **Actionable Security Intelligence (ASI) Solutions** enabled by the award-winning **nFX Open Security Platform (OSP)**.



nFX OSP brings together the industry's most robust correlation technology, richest visualization, reporting, and analytic environment, and most complete incident resolution workflow to take threat identification and eradication to an entirely new level.

Transforming Security Data into Actionable Security Intelligence

By combining the **high-performance correlation processing power** and **distributed architecture** to handle the vast data volume — and complexity — needed to monitor user and network activity from devices, databases and applications, **nFX OSP** serves as the decision support foundation for a powerful array of **Actionable Security Intelligence Solutions**.

Threat Management

Threats are as likely to come from within – from insiders – as from external sources. netForensics provides intelligence from applications, databases, network devices and security devices to counter **all** threats.

Risk Management

As the volume of security attacks grows, the best way to manage and mitigate risk is to establish a risk baseline and determine how effective you are at lowering it over time. The best means to this end are Risk Management solutions enabled by netForensics.

Insider Threat

netForensics is enabling hundreds of large enterprises around the world to more effectively manage internal threats by gaining complete visibility into **all** of their critical compliance-related technologies and assets.

Application Security Monitoring

In any enterprise, hundreds of applications and databases house sensitive financial, customer and employee data that is relevant to compliance. netForensics is uniquely positioned to monitor these applications and databases in addition to security devices.

Performance Management

With the ability to measure metrics, you can gauge the effectiveness of your security policies, better understand risk and quantify your ROI. netForensics puts the power of performance management in your hands by automating key metrics.

Unified Network and Security Management

With compliance and business continuity requirements comes the need for a unified view of the impact of security events – a view that enables a **coordinated** response to mitigate threats and bring non-compliant situations back into compliance. netForensics brings the NOC and SOC together as never before.

nFX Open Security Platform: Enterprise-Class SIM For Enterprise-Wide Security Decision Support

nFX OSP is the only SIM technology designed to handle the complexity of **correlating security events from network and application layers** – including traditional network security devices, as well as newer security technologies such as anomaly detection systems, identity management systems and application and database monitoring systems. Built on a **robust, multi-tier architecture** that can scale to deliver 24x7 security information management across a complex, distributed and heterogeneous enterprise, nFX OSP meets critical compliance, risk management and business continuity challenges at a low total cost of ownership. nFX OSP's architecture also guarantees reliable access to comprehensive, integrated SIM functionality, including sophisticated correlation, dynamic threat visualization, reporting and analytics and integrated incident resolution workflow.

The Difference Is Architecture

nFX OSP is the only SIM solution to provide multi-tier, distributed architecture with the full failover and redundancy required to make sure that analysts and operators never miss a thing. You never miss events that might constitute policy or regulatory compliance violations. You never miss events that might cause downtime and information loss.

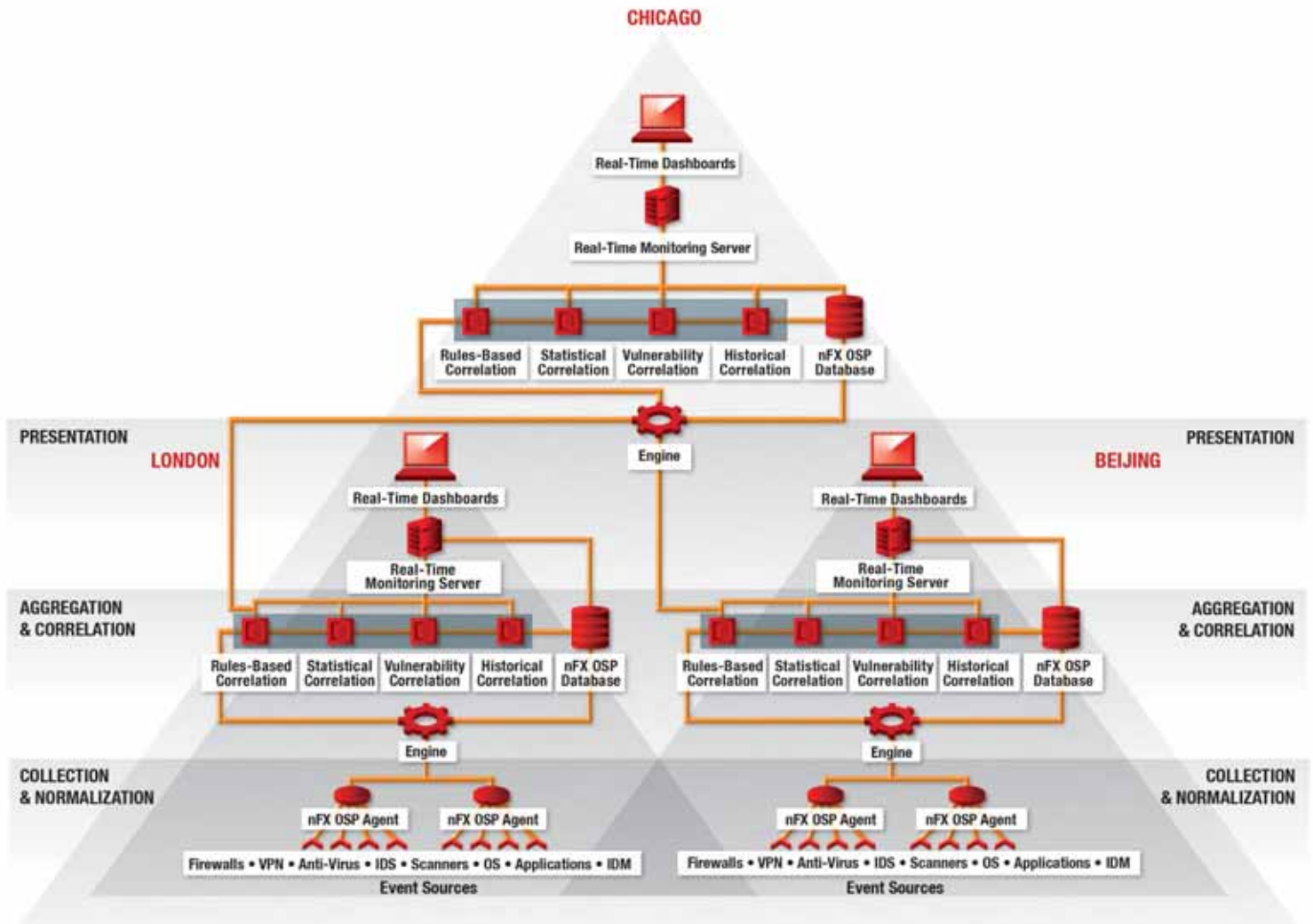
The Most Scalable Architecture, Now and in the Future

Your organization is not static. It continually expands; it constantly grows. So must your ability to efficiently and **cost-effectively** scale applications. It's why we designed the nFX OSP distributed architecture to scale right along with your requirements, dramatically reducing your total cost of ownership. nFX OSP scales in another equally essential manner, too. Comprehensive security visibility, now and in the future, calls for a SIM infrastructure that easily incorporates data from new devices, applications and databases. nFX OSP is the answer.

The Only Multi-Tier SIM Architecture

- Transforms data from disparate network devices, security devices and applications into actionable intelligence for everyone involved in securing the enterprise
- Provides the ability to distribute correlation engines to accommodate data from new device applications and databases; also provides for full failover and redundancy
- Creates an auditable security infrastructure to demonstrate compliance with regulatory mandates
- Prevents catastrophic loss by protecting critical assets and quickly identifying attack
- Enables analysts to conduct historical or “forensic” analysis when an attack occurs to determine the full extent of an attack
- Reduces the risk baseline
- Increases the value of existing information security investments
- Improves the effectiveness of security personnel by improving the efficiency of limited human resources while closing knowledge gaps
- Ensures the availability of data for performance measurement

nFX OSP Architecture



nFX OSP is built on a robust multi-tier architecture that can scale to deliver 24x7 security information management across a complex, distributed and heterogeneous enterprise at a low total cost of ownership.

The Difference Is Comprehensive Correlation

Correlating network data alone is insufficient for meeting regulatory compliance. **nFX OSP** is designed to efficiently process the high volume of data that comes from both security and network devices, core applications and databases. Only nFX OSP provides the **powerful, all-in-one correlation capability** for historical, real-time, and potential threats that fully meets your requirements today and tomorrow.

Rules-Based Correlation

The nFX OSP rules-based correlation engine can perform 100 million state checks per second to handle the volume of data required in order to monitor applications and databases as well as perimeter devices in real time. Importantly, nFX OSP allows users to apply conditional logic to identify likely attack scenarios. nFX OSP is the only SIM solution to implement multi-state rules that require a series of conditions to be met within a specified time period prior to an alert being issued. This reduces the number of rules security analysts must write and maintain – since rules for a particular vulnerability can be nested – and also reduces the number of false positives.

Vulnerability Correlation

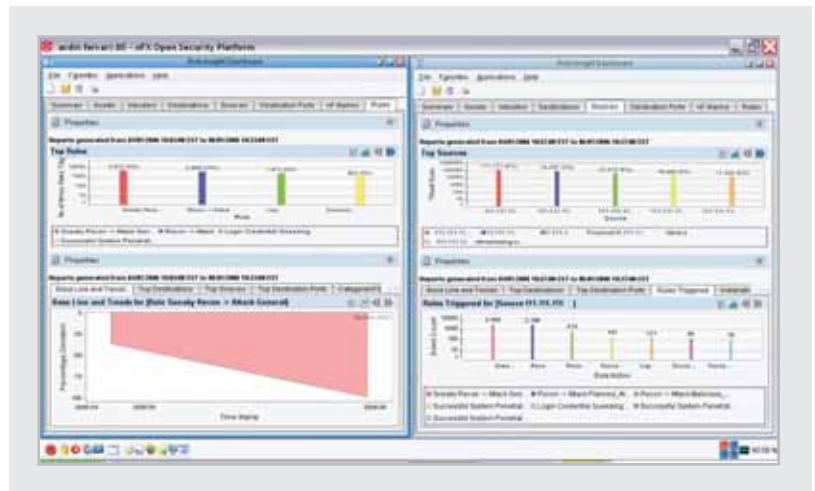
nFX OSP is one of the only SIM solutions that supports vulnerability correlation without writing rules. Security teams can immediately reap the benefits of vulnerability correlation – identifying potential threats to high-value assets by correlating scanner and IDS data and also prioritizing patching efforts – without losing time writing and maintaining rules. Vulnerability correlation also allows organizations to take a proactive approach to enterprise security by correlating vulnerabilities with high value assets and prioritizing patch management efforts to reduce risk.

Statistical Correlation

nFX OSP applies statistical algorithms out of the box to automatically determine incident severity and then assigns a threat score based on asset value. Statistical correlation analyzes network behavior and identifies threats based on the presence and severity of anomalous event patterns.

Historical Correlation

With historical correlation, security analysts can identify repeating patterns of attacks as well as automated and slow attacks that may be veiled within millions of raw security events. Historical correlation allows for quick detection of previously unrecognized malicious events, adding another level of defense to your security program. By enabling review of past events, analysts are better positioned for real-time detection of future zero day attacks.



Risk Insight Dashboards make security information actionable via a complete view of enterprise security posture that presents real-time changes in risk to key compliance-related assets based on deviations to a historical baseline.

The Difference Is Threat Visualization

nFX OSP delivers a suite of visual tools on top of tabular reports and sophisticated analytics so you can access information faster, get **high-level views of overall security health** for compliance and risk management purposes, differentiate false positives from real threats, understand the exact nature and scope of a threat, and make sure that vulnerabilities are mitigated before a threat can proliferate.

Risk Insight Dashboards

With Risk Insight Dashboards, you gain access to real-time snapshots of your organization's overall security health based on security related data from across the enterprise. You can measure deviations from the risk baseline – and get instant, visually intuitive access to the metrics, reporting, baseline and investigative information needed to manage risk and ensure that security standards are met.

Link Maps

This invaluable tool allows you to visualize relationships among different assets under attack to identify the target, type and method of the attack. Importantly, you can see the course of an attack in real-time as it propagates across a network, and also drill down on a specific asset at any time to get more detailed information.

Geo Map

The Geo Map monitors events by country and city, flags suspicious traffic from specific countries, and pinpoints suspicious sources down to a specific longitude and latitude.

Interactive Charts

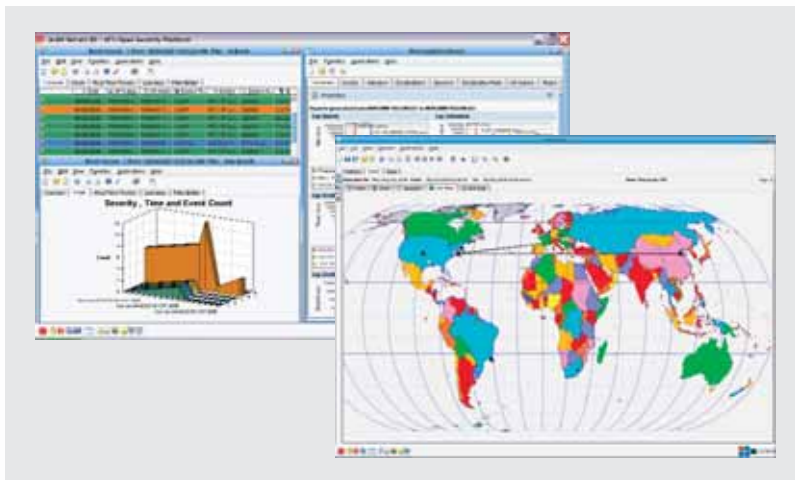
nFX OSP's interactive chart capability makes information more accessible and actionable with visual references that are easier to understand. Choose from a wide range of custom charting options to help identify threats and present summary views of data to management.

Device Status View

Easy to view and analyze, nFX OSP's device count charts provide you with real-time visibility into the status of devices across the network. The tool also allows you to configure remote devices from the security operations center.

Global Threat Dashboard

At a glance, you can view correlated attacker information in an easy-to-understand way and determine if your organization is under attack from one of the top 10 emerging attack sources.



nFX OSP provides users with multiple views of actionable information that are tightly integrated with reporting and analytics to intuitively pinpoint threats.

The Difference Is Incident Resolution Management

nFX OSP is the only SIM solution with a **fully integrated incident resolution workflow** based on industry best practices. By providing a comprehensive remediation workflow, nFX OSP guides teams through a proven, security-specific process to fully eradicate threats.

Intuitive Graphical User Interface

nFX OSP features a powerful but easy-to-use graphical user interface. From the GUI, operators and analysts can easily open, edit and close security incidents. Users are guided through the steps necessary to create and resolve virtually any security incident.

Built-in Workflow

nFX OSP integrates the SANS Institute Six-Step Incident Response process. By utilizing this flexible, comprehensive and customizable workflow, users are assured that each security incident is handled with a rigorous, defined, documented and complete process. Additionally, nFX OSP offers pre-configured incident templates and site-customizable incident resolution management procedures, which simplify the incident resolution management process.

Help Desk Integration

nFX OSP's incident resolution management process integrates with help desk products including HP Service Desk, Remedy, and Peregrine to facilitate communication with the network operations and change management groups that own the patching process. This tight integration extends the value of security intelligence by delivering security incident information directly to stakeholders outside the security organization. nFX OSP ensures effective remediation and accelerates mean-time-to-repair, while updating line-of-business, compliance and application stakeholders on security incidents.

Built-in Knowledge Base

An integrated Knowledge Base includes vendor-specific device information and a complete database of security best practices from such sources as CERT and CVE.

Evidence Retention

Virtually any document, image, report, chart or other relevant data can be attached to an individual incident case. Other files, such as scanned images, audio interview records and traffic captures may also be added to cases and are cryptographically check-summed upon insertion to assure the integrity of the evidence. Authorized users can add notes and comments to the case to alert others and to cover additional aspects of the investigation.

Role-Based Access, Incident Collaboration and Security

nFX OSP cases may be assigned to different system users as well as shared among a group of users. Case change notification is both flexible and configurable. Granular access controls are applied to case data and incident management system functionality so that several analysts may collaborate on a case while maintaining important “need to know” authorization structures. This key feature provides a secure way to store case evidence and apply tight and granular access controls to case data, while still allowing investigators to work together on a case. Additionally, all actions performed by system users on the case are recorded in the audit log. Finally, when the investigation is concluded, the case handler may choose to export the case to other systems. Final reports include all case data and may be printed or sent by email.

Incident Reporting

Robust reporting capabilities include both incident level and executive level reports. Case reports can be generated on individual cases or groups of cases. For management and executives, case monitoring and summary reports are easily generated. Additionally, nFX OSP can be configured to automatically generate incident reports to share with management or third parties.

Integrated Threat Visualization

Users can attach Link Map, Geo Map and Chart Views to cases so different members of the security team can replicate the threat identification process throughout the remediation life cycle.

Unified Policy Compliance and Remediation

nFX OSP takes information related to policy violations and closes the loop by triggering a workflow that allows teams to contain and remedy any policy violations that represent real network attacks. nFX OSP simultaneously ensures that vulnerable systems apply appropriate updates and definitions, so they can access the network safely.



The Difference Is Reporting and Analytics

nFX OSP allows users to obtain a wide and **rich range of reports** based on comprehensive data from devices, applications and databases...and then perform detailed ad hoc analyses to get the answers they need.

Richer, More Flexible Reporting

nFX OSP's rich reporting environment allows security teams to generate reports that incorporate real-time and historical data. Reports are seamlessly integrated with analytics and data visualization to provide a comprehensive understanding of an organization's security picture at any point in time.

- Nearly 400 out-of-the-box reports measure everything from risk exposure to compliance
- Custom reports allow users to get tailored report information
- Role-based dashboards meet specific information needs of analysts, operators and executives

Regulatory Compliance Reporting

nFX OSP ships with a standard suite of operational and executive reports that address key compliance regulations such as Sarbanes-Oxley, HIPAA, FISMA, GLBA and PCI.

- Operational reports create a prioritized view of threats against compliance asset groups
- Executive reports and dashboards show overall security posture, vulnerability and incident management trends

Policy Compliance Reporting

When implemented as part of an integrated policy compliance directive, such as Cisco's Network Admission Control initiative, real-time security policy compliance reporting denies vulnerable machines access to the network until appropriate patches and updates have taken place.

Powerful Analytics with Integrated Charting

Next-generation analytics allow users to slice and dice security data and view it intuitively using multiple dimensions of data in a familiar pivot table format. Data mining also allows analysis of events based on specific criteria to identify anomalous incidents. As a result, analysts can now pinpoint raw event details previously undetectable in a comprehensive, console-style view.

The Difference Is an Embedded Security Knowledge Base

The inability to quickly understand what's happening prevents you and your team from identifying an attack, understanding its characteristics and taking the proper containment and remediation steps. More knowledge means less risk, less damage, and less likelihood of a compliance shortfall. More knowledge – and **more actionable knowledge** – comes from netForensics' embedded security Knowledge Base.

The Basis for More Secure and Compliant Operations

nFX OSP eliminates the need to perform hours of research from a variety of external sources on vulnerabilities and threats. The Knowledge Base is integrated with all of the functional areas of nFX OSP to ensure that vulnerability information, compliance guidelines and remediation procedures are never more than a click away.

- Operators and analysts get a continual flow of relevant and actionable information to pinpoint attacks and provide containment and remediation steps to network and configuration managers
- Teams get even more specific response information in the event of a recurrence because the Knowledge Base can be updated with organization-specific data, such as information about a previous incident
- netForensics' dedicated team of experts publishes advisories to the Knowledge Base on latest security threats bimonthly



Only nFX Open Security Platform transforms security information into Actionable Security Intelligence for more effective security decision support and for solutions that can help your organization achieve compliance, reduce risk, and ensure business continuity.

For more information, visit us online at www.netforensics.com or call 866-525-5666.



©2006 netForensics, the netForensics logo and nFX are trademarks of netForensics, Inc. Other third-party trademarks are the property of their respective owners.



- 200 Metroplex Drive
Edison, NJ 08817
- p 732.393.6000
f 732.393.6090
- www.netforensics.com
- info@netforensics.com

