Network Forensics Market - Global Industry Size, Share, Trends, Opportunity, and Forecast, Segmented By Component (Solution, Services), By Deployment Mode (On-Premises, Cloud-Based), By Application (Data Center Security, Endpoint Security, Intrusion Detection, Network Security, Others), By Region & Competition, 2020-2030F

Market Report | 2025-09-30 | 185 pages | TechSci Research

AVAILABLE LICENSES:

- Single User License $4500.00
- Multi-User License $5500.00
- Custom Research License $8000.00

Report description:

Market Overview
Global Network Forensics Market was valued at USD 2.77 billion in 2024 and is expected to reach USD 6.39 billion by 2030 with a CAGR of 14.78% during the forecast period.
The Network Forensics Market refers to the industry focused on monitoring, capturing, storing, and analyzing network traffic for the purpose of detecting and investigating cyber threats, data breaches, and malicious activities. It plays a crucial role in modern cybersecurity infrastructure, enabling organizations to trace the origin and impact of cyber incidents and enhance their response capabilities. As businesses and governments increasingly rely on digital infrastructures, the attack surface has widened, making network forensics an essential component of incident response strategies.
The market includes software and hardware solutions designed to inspect packets, reconstruct sessions, and identify unauthorized access or data exfiltration. Network forensics is particularly vital in sectors such as banking, financial services, healthcare, telecommunications, and government, where the confidentiality and integrity of data are paramount. The rising sophistication of cyberattacks, including ransomware, phishing, and advanced persistent threats, is driving enterprises to adopt proactive and real-time forensic tools. Additionally, the shift towards cloud computing, the Internet of Things, and remote working environments is further complicating network architectures, leading to greater demand for scalable and intelligent forensic solutions.
Artificial intelligence and machine learning are also being integrated into network forensics platforms to automate anomaly detection and threat analysis, thus improving accuracy and reducing response times. Regulatory requirements and compliance

mandates, such as the General Data Protection Regulation and the Health Insurance Portability and Accountability Act, are compelling organizations to invest in forensic capabilities to ensure transparency and accountability.

Moreover, the emergence of zero-trust architectures and endpoint detection and response systems is enhancing the relevance of network forensics as part of a layered defense strategy. As cyber threats continue to evolve, organizations are expected to allocate increased budgets toward advanced forensic solutions that provide deep visibility, rapid breach detection, and actionable insights. This dynamic environment, coupled with technological advancements and growing security awareness, will propel the steady growth of the global Network Forensics Market in the coming years..

Key Market Drivers

Rising Sophistication of Cyberattacks Necessitating Advanced Network Forensics Solutions

The escalating complexity and frequency of cyberattacks are a primary driver for the network forensics market, as organizations seek advanced tools to investigate and mitigate sophisticated threats. Cybercriminals are leveraging advanced techniques such as ransomware, distributed denial-of-service (DDoS) attacks, and advanced persistent threats (APTs) to exploit vulnerabilities in networked environments. These attacks often leave minimal traces on individual devices, making network forensics critical for capturing and analyzing network traffic to identify attack vectors, reconstruct attack timelines, and trace malicious activities back to their source.

Network forensics solutions enable organizations to monitor real-time data packets, logs, and flow data from routers, firewalls, and intrusion detection systems (IDS), providing granular visibility into network activities. This capability is essential for detecting anomalies, such as unusual traffic spikes or unauthorized access, which may indicate a breach. The proliferation of cloud computing, Internet of Things (IoT) devices, and 5G networks has exponentially increased network traffic, amplifying the need for robust forensics tools to handle large-scale, dynamic data.

By analyzing network-based evidence, organizations can uncover hidden threats, such as encrypted malicious communications or data exfiltration attempts, which traditional endpoint security might miss. Furthermore, network forensics supports proactive threat hunting by correlating attack patterns with historical data to predict and prevent future incidents. The integration of artificial intelligence (AI) and machine learning (ML) into network forensics platforms enhances their ability to process vast datasets, detect anomalies in real time, and automate incident response.

As cyber threats continue to evolve, organizations across industries, including banking, financial services, and insurance (BFSI), healthcare, and government, are investing heavily in network forensics to safeguard critical infrastructure and sensitive data. This driver underscores the pivotal role of network forensics in strengthening cybersecurity frameworks and ensuring rapid response to complex cyber incidents.

A 2024 cybersecurity report indicated that 67% of organizations faced advanced cyberattacks, with 52% relying on network forensics for incident investigation. DDoS attacks increased by 35% year-over-year, contributing to a 40% rise in network traffic analysis tool adoption. Approximately 70% of enterprises reported a 25% improvement in threat detection times using AI-driven network forensics, with 80% of BFSI firms citing network forensics as critical for ransomware mitigation.

Key Market Challenges

Scalability and Data Volume Management

One of the most critical challenges facing the Network Forensics Market is the issue of scalability in handling the exponential growth of network data volumes. With the increasing adoption of cloud computing, Internet of Things devices, and high-bandwidth applications, organizations are witnessing a tremendous surge in data traffic across their networks. This surge generates an overwhelming quantity of logs, packets, and session data that need to be captured, stored, analyzed, and correlated in real-time. The complexity is further exacerbated by the heterogeneity of modern enterprise networks, which span across hybrid infrastructures, virtualized environments, and geographically distributed endpoints. Traditional forensics solutions often fall short in their ability to scale with this pace, thereby impairing performance, accuracy, and timeliness of forensic investigations. Moreover, maintaining real-time visibility and traceability becomes increasingly difficult, especially when network traffic is encrypted or obfuscated.

Enterprises need network forensics platforms that can seamlessly scale horizontally and vertically, while still maintaining low latency and high fidelity of captured data. However, designing and deploying such scalable architectures involves considerable investment in infrastructure, storage, bandwidth, and skilled personnel, which becomes a major barrier for small and medium

enterprises.
In addition, regulatory compliance mandates demand that organizations store network traffic data for extended periods, significantly increasing storage and retrieval costs. Thus, the inability of many network forensics tools to cost-effectively scale in response to growing network traffic is a significant constraint that continues to impede the broader adoption of advanced forensics capabilities across industries.
Key Market Trends
Rise of Cloud Based and Hybrid Network Forensics Solutions
The emergence of cloud computing and hybrid information technology environments is catalysing a shift toward cloud based network forensics solutions-a defining trend in the evolving market landscape. As organisations accelerate cloud migration and deploy infrastructure across public clouds, private data centres, and hybrid configurations, traditional on premise packet capture and forensic tools prove inadequate in offering full visibility, particularly for east west traffic inside the cloud.
Cloud based network forensics platforms address this by providing scalable, centralized capture engines capable of ingesting data from diverse environments. These solutions automate the collection, storage, and analysis of network packets across cloud native, hybrid, and multi cloud domains, effectively bridging visibility gaps that legacy tools often leave exposed. Vendors are embedding smart storage tiering and cloud burst capabilities to manage large data volumes while controlling costs.
The combination of encryption, containerization, and ephemeral workloads in hybrid ecosystems has reinforced the need for forensic platforms that can dynamically adapt and preserve forensic integrity. As businesses seek to support regulatory compliance-such as breach transparency mandates and cyber insurance evidence requirements-cloud-enabled network forensics platforms are becoming best practice in digital forensics strategies across industries.
Key Market Players
- Cisco Systems, Inc.
- IBM Corporation
- FireEye, Inc.
- NETSCOUT Systems, Inc.
- SolarWinds Corporation
- LogRhythm, Inc.
- Viavi Solutions Inc.
- RSA Security LLC
- NIKSUN, Inc.
- Zoho Corporation

Report Scope:
In this report, the Global Network Forensics Market has been segmented into the following categories, in addition to the industry trends which have also been detailed below:
- Network Forensics Market, By Component:
  - Solution
  - Services
- Network Forensics Market, By Deployment Mode:
  - On-Premises
  - Cloud-Based
- Network Forensics Market, By Application:
  - Data Center Security
  - Endpoint Security
  - Intrusion Detection
  - Network Security
  - Others
- Network Forensics Market, By Region:
  - North America

- United States
- Canada
- Mexico

o Europe

- Germany
- France
- United Kingdom
- Italy
- Spain

o South America

- Brazil
- Argentina
- Colombia

o Asia-Pacific

- China
- India
- Japan
- South Korea
- Australia

o Middle East & Africa

- Saudi Arabia
- UAE
- South Africa

Competitive Landscape

Company Profiles: Detailed analysis of the major companies present in the Global Network Forensics Market.

Available Customizations:

Global Network Forensics Market report with the given market data, TechSci Research offers customizations according to a company's specific needs. The following customization options are available for the report:

Company Information

Detailed analysis and profiling of additional market players (up to five).

Table of Contents:

Network Forensics Market - Global Industry Size, Share, Trends, Opportunity, and Forecast, Segmented By Component (Solution, Services), By Deployment Mode (On-Premises, Cloud-Based), By Application (Data Center Security, Endpoint Security, Intrusion Detection, Network Security, Others), By Region & Competition, 2020-2030F

Market Report | 2025-09-30 | 185 pages | TechSci Research

To place an Order with Scotts International:

- - Print this form
- - Complete the relevant blank fields and sign
- - Send as a scanned email to support@scotts-international.com

ORDER FORM:

Select license	License	Price
	Single User License	$4500.00
	Multi-User License	$5500.00
	Custom Research License	$8000.00
	VAT	
	Total	

*Please circle the relevant license option. For any questions please contact support@scotts-international.com or 0048 603 394 346.

** VAT will be added at 23% for Polish based companies, individuals and EU based companies who are unable to provide a valid EU Vat Numbers.

Email*		Phone*	
First Name*		Last Name*	
Job title*			
Company Name*		EU Vat / Tax ID / NIP number*	

Address*		City*	
Zip Code*		Country*	
		Date	2026-02-09
		Signature	