

## **Network Forensics - Market Share Analysis, Industry Trends & Statistics, Growth Forecasts (2025 - 2030)**

Market Report | 2025-06-01 | 126 pages | Mordor Intelligence

### **AVAILABLE LICENSES:**

- Single User License \$4750.00
- Team License (1-7 Users) \$5250.00
- Site License \$6500.00
- Corporate License \$8750.00

### **Report description:**

Network Forensics Market Analysis

The network forensics market size is valued at USD 2.59 billion in 2025 and is forecast to reach USD 5.07 billion by 2030, advancing at a 14.41% CAGR. The adoption curve is steep because packet-level visibility has become indispensable for rapid breach diagnosis, regulatory reporting and cyber-insurance compliance. Spending momentum is especially strong where hybrid-cloud traffic, 5G roll-outs and encrypted east-west flows expose blind spots that traditional perimeter tools overlook. Vendors are therefore embedding forensic functionality into Network Detection and Response (NDR) platforms, shrinking tool sprawl and lowering mean-time-to-respond. Demand is also lifted by insurers that now require packet evidence for claims validation and by regulators such as the SEC and the EU's Digital Operational Resilience Act, which mandate timely, well-documented incident disclosure.

Global Network Forensics Market Trends and Insights

Proliferation of Cloud & Hybrid IT Traffic Visibility Needs

Cloud migration has outpaced traditional monitoring, leaving 73% of enterprises unable to derive actionable insight from existing toolsets. East-west traffic among ephemeral workloads often vanishes before legacy collectors capture it, prompting demand for cloud-native capture engines that automate evidence gathering across multiple IaaS and PaaS domains. Emerging offerings integrate packet capture, artifact preservation and timeline reconstruction in a single workflow, improving investigative efficiency

**Scotts International. EU Vat number: PL 6772247784**

tel. 0048 603 394 346 e-mail: [support@scotts-international.com](mailto:support@scotts-international.com)

[www.scotts-international.com](http://www.scotts-international.com)

and supporting consistent policy enforcement across on-premises, public cloud and hybrid environments. Providers have begun to embed smart storage tiering, enabling long-term retention without linear cost escalation and ensuring regulators can audit forensic evidence on demand.

### Escalating Frequency & Sophistication of Cyber-Attacks

Global breach costs climbed to USD 4.88 million in 2024, while credential-theft incidents surged 84%, fueling adoption of network analytics that surface anomalous authentication spikes and lateral-movement beacons. Healthcare institutions remain under siege as 93% encountered a breach within three years, pushing them to deploy continuous packet capture that pinpoints dwell time and attack provenance. Enterprises now integrate enriched network telemetry into threat-hunting routines that cross-reference endpoint, identity and cloud logs, raising the bar for adversaries and accelerating post-incident forensics for legal, regulatory and insurance stakeholders.

### Shortage of Skilled Packet-Level Investigators

Demand for information-security analysts is projected to expand 32% between 2022-2032, yet universities and training pipelines lag, leaving 54% of employers unable to fill packet-analysis roles. The deficit inflates salary baselines beyond USD 119,000 and amplifies operational risk when alerts outstrip triage capacity. Organizations respond by shifting routine parsing to AI-assisted playbooks, outsourcing level-1 monitoring to managed service partners and prioritizing tool usability so non-specialists can navigate packet timelines with minimal ramp-up.

Other drivers and restraints analyzed in the detailed report include:

5G Standalone Roll-outs Expanding East-West Traffic Capture / Cyber-Insurance Policies Mandating Packet-Level Evidence / High CAPEX of >40 Gbps Capture Appliances /

For complete list of drivers and restraints, kindly check the Table Of Contents.

### Segment Analysis

Solutions generated 62% of network forensics market revenue in 2024, a position powered by demand for high-speed packet capture, behavioural analytics and encrypted-traffic visibility. Feature velocity is brisk, with vendors embedding machine-learning algorithms that establish baseline traffic profiles and surface deviations in seconds. The services segment is smaller today yet expands at an 18% CAGR because organizations need integration, tuning and continuous investigation support while talent remains scarce. Providers bundle assessment, incident-response retainers and managed detection to convert one-time licences into recurring revenue streams. Over the forecast horizon, joint go-to-market programs between hardware vendors and global system integrators will further amplify adoption, especially in regulated industries that require 24-hour evidence retrieval.

Investment patterns suggest that automation-ready solutions will dominate capital budgets, while advisory services grow as strategic overlays that maximize tooling value. The blended model supports life-cycle management from deployment to incident post-mortems, ensuring the network forensics market retains strong pull across diverse buyer personas.

On-premise deployments maintained 53% share of network forensics market size in 2024 because many financial, government and defense entities require local custody of evidence. Nevertheless, cloud-native deployments soar at a 22.5% CAGR as traffic migrates to SaaS, IaaS and containerised stacks. Cloud collectors orchestrate evidence gathering across regions, auto-scale during volumetric events and decouple storage from compute, slashing upfront expense. Hybrid architectures emerge where sensitive data stays on site, yet burst workloads and less regulated segments leverage cloud collectors.

**Scotts International. EU Vat number: PL 6772247784**

tel. 0048 603 394 346 e-mail: [support@scotts-international.com](mailto:support@scotts-international.com)

[www.scotts-international.com](http://www.scotts-international.com)

Platform providers now ship lightweight sensors deployable in Kubernetes clusters or as side-cars, ensuring parity of telemetry between virtual networks and physical switch spans. Compliance teams value the immutable audit trails that cloud object stores enable, while finance teams appreciate opex-based consumption that aligns spend with seasonal traffic variance. Together these dynamics reinforce an enduring pivot toward distributed collection topologies within the broader network forensics market.

Network Forensic Market is Segmented by Component (Solution and Services), by Deployment Model (On-Premise, Cloud), by Organization Size (Small and Medium Enterprises (SMEs) and Large Enterprises), by Application (Endpoint Security, Data Center Security, Network Security, and More), by End-User Industry (IT and Telecom, BFSI, and More), and by Geography. The Market Forecasts are Provided in Terms of Value (USD).

### Geography Analysis

North America held 40% share in 2024, driven by SEC disclosure rules that enforce four-day breach reporting and by an advanced cyber-insurance ecosystem that ties coverage to evidence quality. U.S. enterprises deploy AI-enabled analysis to overcome skills shortages and maintain comprehensive logs for potential litigation or regulatory inquiry. Canada follows a comparable trajectory, underpinned by mandatory privacy breach notifications and concentrated presence of critical infrastructure operators.

Europe captured 28% of network forensics market revenue in 2024, benefiting from GDPR enforcement and the January 2025 start of DORA. Banking hubs in the United Kingdom, Germany and France doubled packet-capture budgets to achieve 24-hour incident notification. Public-sector projects focused on 5G corridors channel EUR 865 million (USD 931 million) into network build-outs, prompting new security monitoring layers. Cross-border data-sharing frameworks inside the EU also stimulate demand for standardized forensic workflows that meet multi-jurisdictional evidence admissibility criteria.

Asia-Pacific is the fastest-growing theatre with a 17.9% 2025-2030 CAGR. China's digital-finance expansion, India's 5G auctions and Australia's critical-infrastructure reforms create sustained opportunities. South Korea's digital forensics sector alone is projected at USD 3.52 billion by 2025, reflecting public-private investment in national cyber-resilience. While skills shortages remain acute, managed security services offset local gaps and accelerate uptake among medium-sized enterprises. The region's exposure to state-sponsored campaigns further elevates the relevance of network forensics market tools that can reconstruct sophisticated, multi-stage intrusions.

### List of Companies Covered in this Report:

Broadcom (Symantec) / Cisco Systems / IBM Corporation / Netscout Systems / Trellix (FireEye) / RSA Security / AccessData (OpenText) / LogRhythm / LiveAction / NIKSUN / Rapid7 / Palo Alto Networks / Darktrace PLC / ExtraHop Networks / Vectra AI / CrowdStrike Holdings / Fortinet Inc. / Check Point Software Tech. / Sophos Group / Gigamon /

### Additional Benefits:

- <ul> The market estimate (ME) sheet in Excel format /
- 3 months of analyst support / </ul>

### Table of Contents:

- 1 INTRODUCTION
- 1.1 Study Deliverables
- 1.2 Scope of the Study
- 1.3 Study Assumptions

**Scotts International. EU Vat number: PL 6772247784**

tel. 0048 603 394 346 e-mail: support@scotts-international.com

www.scotts-international.com

## 2 RESEARCH METHODOLOGY

## 3 EXECUTIVE SUMMARY

## 4 MARKET LANDSCAPE

### 4.1 Market Overview

### 4.2 Market Drivers

4.2.1 Proliferation of cloud and hybrid IT traffic visibility needs

4.2.2 Escalating frequency and sophistication of cyber-attacks

4.2.3 Stringent breach-reporting mandates (GDPR, SEC, DORA)

4.2.4 Convergence of NDR and forensics reducing tool sprawl

4.2.5 5G standalone roll-outs expanding east-west traffic capture

4.2.6 Cyber-insurance policies mandating packet-level evidence

### 4.3 Market Restraints

4.3.1 Shortage of skilled packet-level investigators

4.3.2 High CAPEX of >40 Gbps capture appliances

4.3.3 Performance overhead in multi-cloud inline monitoring

4.3.4 Data-sovereignty limits on cross-border packet storage

### 4.4 Value / Supply-Chain Analysis

### 4.5 Regulatory Landscape

4.6 Technological Outlook (AI-driven packet analytics, TLS1.3 decryption)

### 4.7 Porter's Five Forces

4.7.1 Threat of New Entrants

4.7.2 Bargaining Power of Buyers

4.7.3 Bargaining Power of Suppliers

4.7.4 Threat of Substitutes

4.7.5 Intensity of Competitive Rivalry

### 4.8 Investment and Funding Analysis

## 5 MARKET SIZE AND GROWTH FORECASTS (VALUE)

### 5.1 By Component

5.1.1 Solutions

5.1.2 Services

### 5.2 By Deployment Mode

5.2.1 On-premise

5.2.2 Cloud-based

### 5.3 By Organization Size

5.3.1 Small and Medium Enterprises (SMEs)

5.3.2 Large Enterprises

### 5.4 By Application

5.4.1 Endpoint Security

5.4.2 Data-Center Security

5.4.3 Network Security

5.4.4 Application Security

### 5.5 By End-user Industry

5.5.1 IT and Telecom

**Scotts International. EU Vat number: PL 6772247784**

tel. 0048 603 394 346 e-mail: support@scotts-international.com

www.scotts-international.com

- 5.5.2 BFSI
- 5.5.3 Retail and E-commerce
- 5.5.4 Government and Defense
- 5.5.5 Healthcare and Life Sciences
- 5.5.6 Manufacturing
- 5.5.7 Others (Energy, Education)
- 5.6 By Geography
  - 5.6.1 North America
    - 5.6.1.1 United States
    - 5.6.1.2 Canada
    - 5.6.1.3 Mexico
  - 5.6.2 South America
    - 5.6.2.1 Brazil
    - 5.6.2.2 Rest of South America
  - 5.6.3 Europe
    - 5.6.3.1 United Kingdom
    - 5.6.3.2 Germany
    - 5.6.3.3 France
    - 5.6.3.4 Rest of Europe
  - 5.6.4 APAC
    - 5.6.4.1 China
    - 5.6.4.2 India
    - 5.6.4.3 Japan
    - 5.6.4.4 Australia
    - 5.6.4.5 Rest of APAC
  - 5.6.5 Middle East and Africa
    - 5.6.5.1 Middle East
      - 5.6.5.1.1 Saudi Arabia
      - 5.6.5.1.2 United Arab Emirates
      - 5.6.5.1.3 Turkey
      - 5.6.5.1.4 Rest of Middle East
    - 5.6.5.2 Africa
      - 5.6.5.2.1 South Africa
      - 5.6.5.2.2 Rest of Africa

## 6 COMPETITIVE LANDSCAPE

- 6.1 Market Concentration
- 6.2 Strategic Moves
- 6.3 Market Share Analysis
- 6.4 Company Profiles
  - 6.4.1 Broadcom (Symantec)
  - 6.4.2 Cisco Systems
  - 6.4.3 IBM Corporation
  - 6.4.4 Netscout Systems
  - 6.4.5 Trellix (FireEye)
  - 6.4.6 RSA Security
  - 6.4.7 AccessData (OpenText)

**Scotts International. EU Vat number: PL 6772247784**

tel. 0048 603 394 346 e-mail: [support@scotts-international.com](mailto:support@scotts-international.com)

[www.scotts-international.com](http://www.scotts-international.com)

- 6.4.8 LogRhythm
- 6.4.9 LiveAction
- 6.4.10 NIKSUN
- 6.4.11 Rapid7
- 6.4.12 Palo Alto Networks
- 6.4.13 Darktrace PLC
- 6.4.14 ExtraHop Networks
- 6.4.15 Vectra AI
- 6.4.16 CrowdStrike Holdings
- 6.4.17 Fortinet Inc.
- 6.4.18 Check Point Software Tech.
- 6.4.19 Sophos Group
- 6.4.20 Gigamon

## 7 MARKET OPPORTUNITIES AND FUTURE OUTLOOK

### 7.1 White-space and Unmet-need Assessment

**Scotts International. EU Vat number: PL 6772247784**

tel. 0048 603 394 346 e-mail: [support@scotts-international.com](mailto:support@scotts-international.com)

[www.scotts-international.com](http://www.scotts-international.com)

**Network Forensics - Market Share Analysis, Industry Trends & Statistics, Growth Forecasts (2025 - 2030)**

Market Report | 2025-06-01 | 126 pages | Mordor Intelligence

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	\$4750.00
	Team License (1-7 Users)	\$5250.00
	Site License	\$6500.00
	Corporate License	\$8750.00
		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*	<input type="text"/>	Phone*	<input type="text"/>
First Name*	<input type="text"/>	Last Name*	<input type="text"/>
Job title*	<input type="text"/>		
Company Name*	<input type="text"/>	EU Vat / Tax ID / NIP number*	<input type="text"/>
Address*	<input type="text"/>	City*	<input type="text"/>
Zip Code*	<input type="text"/>	Country*	<input type="text"/>
		Date	<input type="text" value="2026-03-04"/>
		Signature	

**Scotts International. EU Vat number: PL 6772247784**

tel. 0048 603 394 346 e-mail: support@scotts-international.com

www.scotts-international.com



**Scotts International. EU Vat number: PL 6772247784**

tel. 0048 603 394 346 e-mail: support@scotts-international.com

[www.scotts-international.com](http://www.scotts-international.com)