

# Global Network Forensics Market - 2025 -2032

<https://marketpublishers.com/r/G165317519FFEN.html>

Date: October 2025

Pages: 180

Price: US\$ 4,350.00 (Single User License)

ID: G165317519FFEN

## Abstracts

Global network forensics market reached US\$ 2.79 billion in 2024 and is expected to reach US\$ 6.81 billion by 2032, growing with a CAGR of 12.01% during the forecast period 2025-2032.

The network forensics market is driven by the rising frequency and sophistication of cyberattacks, compelling organizations to adopt advanced threat detection and response solutions. The growing demand for real-time network monitoring to ensure data protection and regulatory compliance is a key catalyst. The expansion of IoT and connected devices increases the potential attack surface, necessitating robust network analysis tools.

Government investments, such as multi-million-dollar funding toward next-generation cybersecurity and forensic tools, indicate a strong trend of prioritizing national infrastructure security, especially in energy, utilities, and critical systems. The US Department of Energy (DOE) has announced a US\$30 million funding initiative to develop next-generation cybersecurity tools to protect clean energy infrastructure. This type of funding supports the development of next-gen forensic tools tailored to energy systems, encouraging innovation and commercial adoption.

### Network Forensics Market Trend

The growing establishment of cyber forensics labs and training centers—particularly in developing countries—is emerging as a key trend in the global network forensics market. This trend reflects a strategic shift toward building localized cybersecurity capacity, with a focus on education, skill development, and hands-on training. In October 2024, Algorithma Security launched a 'Make in India' Cyber Forensics Lab in Lucknow to equip Indian students with hands-on experience in cybersecurity. Aimed at educational institutions, the lab offers tools for threat intelligence, dark web monitoring, anti-

ransomware, and advanced areas like deepfake detection and blockchain forensics. This aligns with global efforts to reduce talent gaps, strengthen national cybersecurity infrastructures, and foster innovation through self-reliant technology ecosystems.

## Market Dynamics

### Rising Frequency & Sophistication of Cyber Attacks

The rising frequency and sophistication of cyberattacks are significantly propelling growth in the global network forensics market. Modern cyber threats have evolved into highly targeted, stealthy, and persistent attacks—ranging from ransomware and phishing to zero-day exploits and nation-state operations—making them harder to detect and contain with conventional security tools. For example, in India alone, cyberattacks on government entities surged by a staggering 138% between 2019 and 2023, rising from 85,797 incidents to 204,844, according to the Indian Ministry of Electronics and IT. This dramatic rise underscores the urgent need for advanced forensic capabilities to trace the origins and pathways of such intrusions.

Similarly, in the UK, the Cyber Security Breaches Survey shows that 32% of businesses and 24% of charities experienced breaches or attacks in the past 12 months—a figure that jumps to 59% for medium-sized businesses, 69% for large enterprises, and 56% for high-income charities. These statistics reveal how widespread and persistent cyber threats have become across sectors and geographies. Network forensics solutions are being adopted to provide deep visibility into network traffic, reconstruct attack timelines, and support legal investigations. The ability to identify, analyze, and respond to attacks in real-time has become mission-critical. As the digital threat landscape continues to intensify, enterprises are prioritizing forensic readiness as a cornerstone of their cybersecurity strategy.

### Shortage of Skilled Professionals

The shortage of skilled professionals is significantly restraining the growth of the global network forensics market, as the technology requires deep expertise in analyzing complex data flows, detecting advanced threats, and preserving digital evidence. According to the 2023 ISC2 Cybersecurity Workforce Study, there is a global shortfall of nearly 4 million cybersecurity professionals, with a notable 12.6% gap between demand and supply. This severe talent deficit makes it difficult for organizations to find qualified experts to manage and operate forensic tools effectively.

Moreover, for the first time since the onset of the global pandemic, the study anticipates a decline in cybersecurity hiring in 2024, driven by budget cuts, pay freezes, and economic uncertainties. These financial constraints are particularly burdensome for small and mid-sized enterprises, which often lack the resources to attract or retain top talent. Compounding the issue is the rapid evolution of technologies such as AI, cloud environments, and encrypted communications, which demand continuously updated skills that the current workforce struggles to keep pace with.

## Segment Analysis

The global network forensics market is segmented based on type, source, application, distribution channel and region.

**Solutions Hold a Significant Share in the Market Due to Their Crucial Role in Real-Time Threat Detection and Analysis.**

The global network forensics market is significantly influenced by both software and hardware components, each playing a vital role in ensuring comprehensive threat detection and incident response. Software solutions dominate the market share due to their flexibility, scalability, and ability to integrate with existing IT infrastructures. These solutions include intrusion detection systems (IDS), security information and event management (SIEM), and packet capture and analysis tools, which are essential for real-time monitoring and forensic investigation. Hardware components, such as network taps, packet brokers, and dedicated forensic appliances, also hold a crucial share, particularly in large enterprises requiring high-speed data processing and secure data storage.

On August 22, 2024, IIMT College of Engineering, in partnership with the Future Crime Research Foundation (FCRF), will inaugurate a state-of-the-art Centre of Excellence in Digital Forensics & Incident Response (CoE-DFIR). Supported by the IIMT Ladder Business Foundation as the incubator, this initiative aims to bolster India's cybersecurity education and infrastructure. The launch event will take place at the IIMT Ladder Business Foundation in Greater Noida.

## Geographical Penetration

**Asia-Pacific Holds a Significant Share in the Market Due to Rapid Digitalization, Expanding IT Infrastructure, and Rising Cybersecurity Investments.**

The Asia-Pacific region has emerged as a key player in the global network forensics market, driven by rapid digitalization and a surge in cyber threats. Countries like China, India, Japan, and South Korea are investing heavily in cybersecurity infrastructure, fueling demand for advanced forensic tools. The region's expanding internet and smartphone usage have widened the attack surface, necessitating stronger digital defenses. In 2024, Southeast Asia saw twice as many cyberattacks as the previous year, with Vietnam, Thailand, the Philippines, and others among the most affected. Taiwan faced over 2.4 million daily cyberattack attempts from Chinese groups, with a 20% rise in successful breaches, highlighting the growing threat landscape.

Sectors such as manufacturing, government, and finance are among the most targeted, pushing public and private organizations to adopt real-time threat detection and response systems. Supporting this trend, Excite Technology Services in Australia raised US\$ 1.83 (AU\$ 2.8) million in early 2025 to expand digital forensics training for Defence and Law Enforcement. Governments across the region are introducing stringent data protection regulations, further boosting market momentum. The rise of innovative cybersecurity startups and increased public-private collaboration adds to the region's strength.

### Technological Advancement Analysis

The global network forensics market is witnessing rapid technological advancements driven by the integration of artificial intelligence (AI), machine learning (ML), and big data analytics, enabling faster detection and response to cyber threats. Modern forensic tools now offer automated packet capture and behavioral analysis, enhancing threat hunting capabilities across hybrid and cloud-based infrastructures.

Moreover, the emergence of deep packet inspection (DPI) and encrypted traffic analysis is addressing visibility challenges in secure communications. For example, in 2024, Cisco introduced AI-driven Secure Network Analytics, which leverages behavioral modeling for anomaly detection across encrypted networks. Integration with SIEM (Security Information and Event Management) platforms is further enabling seamless incident response and forensic correlation.

### Competitive Landscape

The major global players in the market include Broadcom Inc., Cisco Systems Inc., IBM Corporation, Netscout Systems Inc., Valvi Solutions Inc., FireEye, Inc., NIKSUN, Inc.,

Viavi Solutions Inc., RSA Security LLC, Palo Alto Networks, Inc.

### Key Developments

In May 2025, in India, a new R&D centre for cyber- and forensics tech was launched at the Economic Offences Unit campus, Patna, Bihar. This joint initiative by Bihar Police's EOU and CDAC will foster collaboration between investigators and researchers, offering training and innovation tailored to combat evolving cyber threats in the region.

In February 2023, IBM and Palo Alto Networks formed a partnership to enhance their skills to respond to incidents. Through this agreement, Palo Alto Networks' Cortex solutions are utilized to improve the security of IBM's X-Force. This provides customers with a comprehensive view of cyber threats, reduces the amount of time it takes to respond and strengthens the resilience of cybersecurity.

## Contents

### **1. METHODOLOGY AND SCOPE**

- 1.1. Research Methodology
- 1.2. Research Objective and Scope of the Report

### **2. DEFINITION AND OVERVIEW**

### **3. EXECUTIVE SUMMARY**

- 3.1. Snippet by Component
- 3.2. Snippet by Deployment Mode
- 3.3. Snippet by Organization Size
- 3.4. Snippet by Application
- 3.5. Snippet by End-User
- 3.6. Snippet by Region

### **4. DYNAMICS**

- 4.1. Impacting Factors
  - 4.1.1. Drivers
    - 4.1.1.1. Rising Frequency & Sophistication of Cyber Attacks
  - 4.1.2. Restraints
    - 4.1.2.1. Shortage of Skilled Professionals
  - 4.1.3. Opportunity
  - 4.1.4. Impact Analysis

### **5. INDUSTRY ANALYSIS**

- 5.1. Porter's Five Force Analysis
- 5.2. Supply Chain Analysis
- 5.3. Pricing Analysis
- 5.4. Regulatory and Compliance Analysis
- 5.5. Technological Analysis
- 5.6. DMI Opinion

### **6. BY COMPONENT**

## 6.1. Introduction

6.1.1. Market Size Analysis and Y-o-Y Growth Analysis (%), By Component

6.1.2. Market Attractiveness Index, By Component

## 6.2. Solutions\*

6.2.1. Introduction

6.2.2. Market Size Analysis and Y-o-Y Growth Analysis (%)

6.2.3. Software

6.2.4. Hardware

## 6.3. Services

# 7. BY DEPLOYMENT MODE

## 7.1. Introduction

7.1.1. Market Size Analysis and Y-o-Y Growth Analysis (%), By Deployment Mode

7.1.2. Market Attractiveness Index, By Deployment Mode

## 7.2. Cloud-Based\*

7.2.1. Introduction

7.2.2. Market Size Analysis and Y-o-Y Growth Analysis (%)

## 7.3. On Premises

# 8. BY ORGANIZATION SIZE

## 8.1. Introduction

8.1.1. Market Size Analysis and Y-o-Y Growth Analysis (%), By Organization Size

8.1.2. Market Attractiveness Index, By Organization Size

## 8.2. SMEs\*

8.2.1. Introduction

8.2.2. Market Size Analysis and Y-o-Y Growth Analysis (%)

## 8.3. Large Enterprises

# 9. BY APPLICATION

## 9.1. Introduction

9.1.1. Market Size Analysis and Y-o-Y Growth Analysis (%), By Application

9.1.2. Market Attractiveness Index, By Application

## 9.2. Data Center Security\*

9.2.1. Introduction

9.2.2. Market Size Analysis and Y-o-Y Growth Analysis (%)

## 9.3. Endpoint Security

- 9.4. Network Security
- 9.5. Application Security
- 9.6. Others

## **10. BY END-USER**

- 10.1. Introduction
  - 10.1.1. Market Size Analysis and Y-o-Y Growth Analysis (%), By End-User
  - 10.1.2. Market Attractiveness Index, By End-User
- 10.2. BFSI\*
  - 10.2.1. Introduction
  - 10.2.2. Market Size Analysis and Y-o-Y Growth Analysis (%)
- 10.3. Healthcare
- 10.4. IT & Telecom
- 10.5. Manufacturing
- 10.6. Retail
- 10.7. Others

## **11. BY REGION**

- 11.1. Introduction
  - 11.1.1. Market Size Analysis and Y-o-Y Growth Analysis (%), By Region
  - 11.1.2. Market Attractiveness Index, By Region
- 11.2. North America
  - 11.2.1. Introduction
  - 11.2.2. Key Region-Specific Dynamics
  - 11.2.3. Market Size Analysis and Y-o-Y Growth Analysis (%), By Component

## **12. MARKET SIZE ANALYSIS AND Y-O-Y GROWTH ANALYSIS (%), BY DEPLOYMENT MODE**

- 12.1. Market Size Analysis and Y-o-Y Growth Analysis (%), By Organization Size
  - 12.1.1. Market Size Analysis and Y-o-Y Growth Analysis (%), By Application
  - 12.1.2. Market Size Analysis and Y-o-Y Growth Analysis (%), By End-User
  - 12.1.3. Market Size Analysis and Y-o-Y Growth Analysis (%), By Country
    - 12.1.3.1. US
    - 12.1.3.2. Canada
    - 12.1.3.3. Mexico
- 12.2. Europe

### 12.2.1. Introduction

### 12.2.2. Key Region-Specific Dynamics

### 12.2.3. Market Size Analysis and Y-o-Y Growth Analysis (%), By Component

### 12.2.4. Market Size Analysis and Y-o-Y Growth Analysis (%), By Deployment Mode

### 12.2.5. Market Size Analysis and Y-o-Y Growth Analysis (%), By Organization Size

### 12.2.6. Market Size Analysis and Y-o-Y Growth Analysis (%), By Application

### 12.2.7. Market Size Analysis and Y-o-Y Growth Analysis (%), By End-User

### 12.2.8. Market Size Analysis and Y-o-Y Growth Analysis (%), By Country

#### 12.2.8.1. Germany

#### 12.2.8.2. UK

#### 12.2.8.3. France

#### 12.2.8.4. Italy

#### 12.2.8.5. Spain

#### 12.2.8.6. Rest of Europe

## 12.3. South America

### 12.3.1. Introduction

### 12.3.2. Key Region-Specific Dynamics

### 12.3.3. Market Size Analysis and Y-o-Y Growth Analysis (%), By Component

### 12.3.4. Market Size Analysis and Y-o-Y Growth Analysis (%), By Deployment Mode

### 12.3.5. Market Size Analysis and Y-o-Y Growth Analysis (%), By Organization Size

### 12.3.6. Market Size Analysis and Y-o-Y Growth Analysis (%), By Application

### 12.3.7. Market Size Analysis and Y-o-Y Growth Analysis (%), By End-User

### 12.3.8. Market Size Analysis and Y-o-Y Growth Analysis (%), By Country

#### 12.3.8.1. Brazil

#### 12.3.8.2. Argentina

#### 12.3.8.3. Rest of South America

## 12.4. Asia-Pacific

### 12.4.1. Introduction

### 12.4.2. Key Region-Specific Dynamics

### 12.4.3. Market Size Analysis and Y-o-Y Growth Analysis (%), By Component

### 12.4.4. Market Size Analysis and Y-o-Y Growth Analysis (%), By Deployment Mode

### 12.4.5. Market Size Analysis and Y-o-Y Growth Analysis (%), By Organization Size

### 12.4.6. Market Size Analysis and Y-o-Y Growth Analysis (%), By Application

### 12.4.7. Market Size Analysis and Y-o-Y Growth Analysis (%), By End-User

### 12.4.8. Market Size Analysis and Y-o-Y Growth Analysis (%), By Country

#### 12.4.8.1. China

#### 12.4.8.2. India

#### 12.4.8.3. Japan

#### 12.4.8.4. Australia

#### 12.4.8.5. Rest of Asia-Pacific

### 12.5. Middle East and Africa

#### 12.5.1. Introduction

#### 12.5.2. Key Region-Specific Dynamics

#### 12.5.3. Market Size Analysis and Y-o-Y Growth Analysis (%), By Component

#### 12.5.4. Market Size Analysis and Y-o-Y Growth Analysis (%), By Deployment Mode

#### 12.5.5. Market Size Analysis and Y-o-Y Growth Analysis (%), By Organization Size

#### 12.5.6. Market Size Analysis and Y-o-Y Growth Analysis (%), By Application

#### 12.5.7. Market Size Analysis and Y-o-Y Growth Analysis (%), By End-User

## 13. COMPETITIVE LANDSCAPE

### 13.1. Competitive Scenario

### 13.2. Market Positioning/Share Analysis

### 13.3. Mergers and Acquisitions Analysis

## 14. COMPANY PROFILES

### 14.1. Broadcom Inc.\*

#### 14.1.1. Company Overview

#### 14.1.2. Product Portfolio and Description

#### 14.1.3. Financial Overview

#### 14.1.4. Key Developments

### 14.2. Cisco Systems Inc.

### 14.3. IBM Corporation

### 14.4. Netscout Systems Inc.

### 14.5. Valvi Solutions Inc.

### 14.6. FireEye, Inc.

### 14.7. NIKSUN, Inc.

### 14.8. Viavi Solutions Inc.

### 14.9. RSA Security LLC

### 14.10. Palo Alto Networks, Inc. (LIST NOT EXHAUSTIVE )

## 15. APPENDIX

### 15.1. About Us and Services

### 15.2. Contact Us

## List Of Tables

### LIST OF TABLES

Table 1 Global Network Forensics Market Value, By Component, 2024, 2028 & 2032 (US\$ Million)

Table 2 Global Network Forensics Market Value, By Deployment Mode, 2024, 2028 & 2032 (US\$ Million)

Table 3 Global Network Forensics Market Value, By Organization Size, 2024, 2028 & 2032 (US\$ Million)

Table 4 Global Network Forensics Market Value, By Application, 2024, 2028 & 2032 (US\$ Million)

Table 5 Global Network Forensics Market Value, By End-User, 2024, 2028 & 2032 (US\$ Million)

Table 6 Global Network Forensics Market Value, By Region, 2024, 2028 & 2032 (US\$ Million)

Table 7 Global Network Forensics Market Value, By Component, 2024, 2028 & 2032 (US\$ Million)

Table 8 Global Network Forensics Market Value, By Component, 2023-2032 (US\$ Million)

Table 9 Global Network Forensics Market Value, By Deployment Mode, 2024, 2028 & 2032 (US\$ Million)

Table 10 Global Network Forensics Market Value, By Deployment Mode, 2023-2032 (US\$ Million)

Table 11 Global Network Forensics Market Value, By Organization Size, 2024, 2028 & 2032 (US\$ Million)

Table 12 Global Network Forensics Market Value, By Organization Size, 2023-2032 (US\$ Million)

Table 13 Global Network Forensics Market Value, By Application, 2024, 2028 & 2032 (US\$ Million)

Table 14 Global Network Forensics Market Value, By Application, 2023-2032 (US\$ Million)

Table 15 Global Network Forensics Market Value, By End-User, 2024, 2028 & 2032 (US\$ Million)

Table 16 Global Network Forensics Market Value, By End-User, 2023-2032 (US\$ Million)

Table 17 Global Network Forensics Market Value, By Region, 2024, 2028 & 2032 (US\$ Million)

Table 18 Global Network Forensics Market Value, By Region, 2023-2032 (US\$ Million)

Table 19 North America Network Forensics Market Value, By Component, 2023-2032 (US\$ Million)

Table 20 North America Network Forensics Market Value, By Deployment Mode, 2023-2032 (US\$ Million)

Table 21 North America Network Forensics Market Value, By Organization Size, 2023-2032 (US\$ Million)

Table 22 North America Network Forensics Market Value, By Application, 2023-2032 (US\$ Million)

Table 23 North America Network Forensics Market Value, By End-User, 2023-2032 (US\$ Million)

Table 24 North America Network Forensics Market Value, By Country, 2023-2032 (US\$ Million)

Table 25 South America Network Forensics Market Value, By Component, 2023-2032 (US\$ Million)

Table 26 South America Network Forensics Market Value, By Deployment Mode, 2023-2032 (US\$ Million)

Table 27 South America Network Forensics Market Value, By Organization Size, 2023-2032 (US\$ Million)

Table 28 South America Network Forensics Market Value, By Application, 2023-2032 (US\$ Million)

Table 29 South America Network Forensics Market Value, By End-User, 2023-2032 (US\$ Million)

Table 30 South America Network Forensics Market Value, By Country, 2023-2032 (US\$ Million)

Table 31 Europe Network Forensics Market Value, By Component, 2023-2032 (US\$ Million)

Table 32 Europe Network Forensics Market Value, By Deployment Mode, 2023-2032 (US\$ Million)

Table 33 Europe Network Forensics Market Value, By Organization Size, 2023-2032 (US\$ Million)

Table 34 Europe Network Forensics Market Value, By Application, 2023-2032 (US\$ Million)

Table 35 Europe Network Forensics Market Value, By End-User, 2023-2032 (US\$ Million)

Table 36 Europe Network Forensics Market Value, By Country, 2023-2032 (US\$ Million)

Table 37 Asia-Pacific Network Forensics Market Value, By Component, 2023-2032 (US\$ Million)

Table 38 Asia-Pacific Network Forensics Market Value, By Deployment Mode, 2023-2032 (US\$ Million)

Table 39 Asia-Pacific Network Forensics Market Value, By Organization Size, 2023-2032 (US\$ Million)

Table 40 Asia-Pacific Network Forensics Market Value, By Application, 2023-2032 (US\$ Million)

Table 41 Asia-Pacific Network Forensics Market Value, By End-User, 2023-2032 (US\$ Million)

Table 42 Asia-Pacific Network Forensics Market Value, By Country, 2023-2032 (US\$ Million)

Table 43 Middle East and Africa Network Forensics Market Value, By Component, 2023-2032 (US\$ Million)

Table 44 Middle East and Africa Network Forensics Market Value, By Deployment Mode, 2023-2032 (US\$ Million)

Table 45 Middle East and Africa Network Forensics Market Value, By Organization Size, 2023-2032 (US\$ Million)

Table 46 Middle East and Africa Network Forensics Market Value, By Application, 2023-2032 (US\$ Million)

Table 47 Middle East and Africa Network Forensics Market Value, By End-User, 2023-2032 (US\$ Million)

Table 48 Middle East and Africa Network Forensics Market Value, By Country, 2023-2032 (US\$ Million)

Table 49 Broadcom Inc.: Overview

Table 50 Broadcom Inc.: Product Portfolio

Table 51 Broadcom Inc.: Key Developments

Table 52 Cisco Systems Inc.: Overview

Table 53 Cisco Systems Inc.: Product Portfolio

Table 54 Cisco Systems Inc.: Key Developments

Table 55 IBM Corporation: Overview

Table 56 IBM Corporation: Product Portfolio

Table 57 IBM Corporation: Key Developments

Table 58 Netscout Systems Inc.: Overview

Table 59 Netscout Systems Inc.: Product Portfolio

Table 60 Netscout Systems Inc.: Key Developments

Table 61 Valvi Solutions Inc.: Overview

Table 62 Valvi Solutions Inc.: Product Portfolio

Table 63 Valvi Solutions Inc.: Key Developments

Table 64 FireEye, Inc.: Overview

Table 65 FireEye, Inc.: Product Portfolio

Table 66 FireEye, Inc.: Key Developments

Table 67 NIKSUN, Inc.: Overview

- Table 68 NIKSUN, Inc.: Product Portfolio
- Table 69 NIKSUN, Inc.: Key Developments
- Table 70 Viavi Solutions Inc.: Overview
- Table 71 Viavi Solutions Inc.: Product Portfolio
- Table 72 Viavi Solutions Inc.: Key Developments
- Table 73 RSA Security LLC: Overview
- Table 74 RSA Security LLC: Product Portfolio
- Table 75 RSA Security LLC: Key Developments
- Table 76 Palo Alto Networks, Inc.: Overview
- Table 77 Palo Alto Networks, Inc.: Product Portfolio
- Table 78 Palo Alto Networks, Inc.: Key Developments

## I would like to order

Product name: Global Network Forensics Market - 2025 -2032

Product link: <https://marketpublishers.com/r/G165317519FFEN.html>

Price: US\$ 4,350.00 (Single User License / Electronic Delivery)

If you want to order Corporate License or Hard Copy, please, contact our Customer Service:

[info@marketpublishers.com](mailto:info@marketpublishers.com)

## Payment

To pay by Credit Card (Visa, MasterCard, American Express, PayPal), please, click button on product page <https://marketpublishers.com/r/G165317519FFEN.html>