

# **Security Analytics Market Forecasts to 2032 – Global Analysis By Component (Solutions and Services), Deployment Mode (On-Premises and Cloud-Based), Organization Size, Application, End User and By Geography**

<https://marketpublishers.com/r/S64F4A3ACDD5EN.html>

Date: April 2025

Pages: 150

Price: US\$ 4,150.00 (Single User License)

ID: S64F4A3ACDD5EN

## **Abstracts**

According to Statistics MRC, the Global Security Analytics Market is accounted for \$23.3 billion in 2025 and is expected to reach \$74.8 billion by 2032 growing at a CAGR of 18.15% during the forecast period. Security Analytics refers to the process of collecting, analyzing and interpreting data from various sources to detect and respond to security threats. It involves the use of advanced technologies like machine learning, artificial intelligence, and big data analytics to identify patterns and anomalies within network traffic, system logs, and user behavior. By leveraging security analytics, organizations can proactively identify potential security breaches, mitigate risks, and strengthen their defense mechanisms.

According to IBM's 2018 report, the average cost of a data breach for businesses was approximately USD 3.86 million.

Market Dynamics:

Driver:

Increase in Cybersecurity Threats

The increase in cybersecurity threats has significantly boosted the security analytics market. As cyberattacks become more sophisticated, organizations are prioritizing advanced security measures to protect their data and assets. This heightened demand

for real-time threat detection, monitoring, and response drives the growth of security analytics solutions. Companies are investing in AI-driven analytics tools to improve threat intelligence, enhance risk management, and ensure compliance. The evolving landscape of cyber threats creates a continuous need for innovation and strengthens the security analytics sector.

Restraint:

### High Implementation Costs

High implementation costs in security analytics create a significant barrier for many organizations, limiting their ability to adopt advanced security solutions. These costs hinder market growth, especially for small and medium-sized enterprises (SMEs) with constrained budgets. As a result, businesses may delay or forgo implementing crucial security measures, leaving them vulnerable to cyber threats and limiting the overall effectiveness of the security analytics market.

Opportunity:

### Growth of IoT and Cloud Adoption

The rise of IoT and cloud use is greatly boosting the security analytics market. Large volumes of data are produced by IoT devices, and when analyzed by cloud systems, they provide real-time insights into possible security risks. Scalable and economical approaches to breach detection and response are made possible by cloud-based security analytics. The growth of the security analytics market is positively impacted by this integration since it enables enterprises to strengthen overall cybersecurity posture, expedite incident response, and improve threat detection.

Threat:

### Data Privacy Concerns

Data privacy concerns have hindered the growth of the security analytics market, as organizations face challenges in balancing security measures with user privacy rights. Stringent regulations like GDPR have raised compliance risks, discouraging some businesses from fully embracing advanced analytics tools. These concerns create hesitancy around data collection and processing, limiting the effectiveness of security solutions and slowing down the adoption of security analytics technologies in privacy-

sensitive industries.

### Covid-19 Impact

The COVID-19 pandemic significantly impacted the security analytics market, driving an increased demand for advanced security solutions due to the surge in cyber threats. With businesses shifting to remote work, there was a higher need for robust data protection, real-time monitoring, and threat detection. This accelerated the adoption of security analytics tools, as organizations sought to safeguard sensitive information and ensure operational continuity in an increasingly digital environment.

The healthcare & life sciences segment is expected to be the largest during the forecast period

The healthcare & life sciences segment is expected to account for the largest market share during the forecast period, due to demand for advanced cybersecurity solutions. With the increasing digitization of patient data and the rise of healthcare-related cyber threats, organizations are prioritizing robust security measures. Security analytics helps detect anomalies, prevent data breaches, and ensure compliance with stringent regulations like HIPAA. This heightened focus on data protection and risk management fosters innovation in security technologies, expanding market growth and enhancing overall industry resilience.

The incident forensics segment is expected to have the highest CAGR during the forecast period

Over the forecast period, the incident forensics segment is predicted to witness the highest growth rate, as it enhances the ability to investigate and respond to cyber threats in real-time. It provides deep insights into security breaches, helping organizations identify vulnerabilities, trace malicious activities, and strengthen defenses. As cyber threats grow in complexity, incident forensics enables organizations to improve threat detection, reduce response times, and refine proactive security measures. This contributes to a more resilient security posture, propelling demand for advanced security analytics solutions across various industries.

Region with largest share:

During the forecast period, the Asia Pacific region is expected to hold the largest market share as digital transformation accelerates, businesses are relying on advanced

analytics to detect threats, reduce risks, and maintain data integrity. The market encourages the adoption of cutting-edge technology like artificial intelligence (AI) and machine learning, stimulates economic growth, and fosters innovation. A safer, more secure digital environment is supported by increased investment in security infrastructure, which also increases regional resilience against cyber threats.

Region with highest CAGR:

Over the forecast period, the North America region is anticipated to exhibit the highest CAGR, because of the increase in cyber threats, businesses and government agencies are implementing advanced analytics to proactively identify and respond to dangers. This market helps businesses adhere to strict rules, encourages innovation, and supports the integration of AI and machine learning for threat detection. Consequently, it promotes economic growth, improves overall digital security, and guarantees a more secure and robust digital environment.

Key players in the market

Some of the key players profiled in the Security Analytics Market include IBM Corporation, Cisco Systems, Inc., Splunk Inc., Palo Alto Networks, Inc., Fortinet, Inc., McAfee Corp., Microsoft Corporation, RSA Security LLC, Rapid7, Inc., Exabeam, Inc., LogRhythm, Inc., Sumo Logic, Inc., Huntsman Security, Gurucul, Varonis Systems, Inc., Devo Technology and Graylog, Inc.

Key Developments:

In March 2025, IBM announced the availability of Intel® Gaudi® 3 AI accelerators on IBM Cloud. This offering delivers Intel Gaudi 3 in a public cloud environment for production workloads. Through this collaboration, IBM Cloud aims to help clients more cost-effectively scale and deploy enterprise AI.

In March 2025, Vodafone and IBM announced a collaboration aimed at protecting customers and their data from future risks related to quantum computers when browsing the Internet on their smartphones.

In August 2024, Intel and IBM have announced a collaboration to deploy Intel® Gaudi® 3 AI accelerators as a service on IBM Cloud, aimed at improving cost-effectiveness and performance for enterprise AI workloads.

**Components Covered:**

Solutions

Services

**Deployment Modes Covered:**

On-Premises

Cloud-Based

**Organization Sizes Covered:**

Small & Medium Enterprises (SMEs)

Large Enterprises

**Applications Covered:**

Threat Intelligence & Detection

Behavioral Analytics

Log Management & Security Information and Event Management (SIEM)

Data Loss Prevention

Incident Forensics

Risk & Compliance Management

Other Applications

**End Users Covered:**

Banking, Financial Services & Insurance (BFSI)

IT & Telecommunications

Retail & E-commerce

Healthcare & Life Sciences

Government & Defense

Energy & Utilities

Manufacturing

Education

Other End Users

#### Regions Covered:

North America

US

Canada

Mexico

Europe

Germany

UK

Italy

France

Spain

Rest of Europe

Asia Pacific

Japan

China

India

Australia

New Zealand

South Korea

Rest of Asia Pacific

South America

Argentina

Brazil

Chile

Rest of South America

Middle East & Africa

Saudi Arabia

UAE

Qatar

South Africa

## Rest of Middle East & Africa

What our report offers:

- Market share assessments for the regional and country-level segments
- Strategic recommendations for the new entrants
- Covers Market data for the years 2022, 2023, 2024, 2026, and 2030
- Market Trends (Drivers, Constraints, Opportunities, Threats, Challenges, Investment Opportunities, and recommendations)
- Strategic recommendations in key business segments based on the market estimations
- Competitive landscaping mapping the key common trends
- Company profiling with detailed strategies, financials, and recent developments
- Supply chain trends mapping the latest technological advancements

Free Customization Offerings:

All the customers of this report will be entitled to receive one of the following free customization options:

### Company Profiling

Comprehensive profiling of additional market players (up to 3)

SWOT Analysis of key players (up to 3)

### Regional Segmentation

Market estimations, Forecasts and CAGR of any prominent country as per the client's interest (Note: Depends on feasibility check)

### Competitive Benchmarking

Benchmarking of key players based on product portfolio, geographical presence, and strategic alliances

## Contents

### **1 EXECUTIVE SUMMARY**

### **2 PREFACE**

- 2.1 Abstract
- 2.2 Stake Holders
- 2.3 Research Scope
- 2.4 Research Methodology
  - 2.4.1 Data Mining
  - 2.4.2 Data Analysis
  - 2.4.3 Data Validation
  - 2.4.4 Research Approach
- 2.5 Research Sources
  - 2.5.1 Primary Research Sources
  - 2.5.2 Secondary Research Sources
  - 2.5.3 Assumptions

### **3 MARKET TREND ANALYSIS**

- 3.1 Introduction
- 3.2 Drivers
- 3.3 Restraints
- 3.4 Opportunities
- 3.5 Threats
- 3.6 Application Analysis
- 3.7 End User Analysis
- 3.8 Emerging Markets
- 3.9 Impact of Covid-19

### **4 PORTERS FIVE FORCE ANALYSIS**

- 4.1 Bargaining power of suppliers
- 4.2 Bargaining power of buyers
- 4.3 Threat of substitutes
- 4.4 Threat of new entrants
- 4.5 Competitive rivalry

## **5 GLOBAL SECURITY ANALYTICS MARKET, BY COMPONENT**

- 5.1 Introduction
- 5.2 Solutions
  - 5.2.1 Network Security Analytics
  - 5.2.2 Endpoint Security Analytics
  - 5.2.3 Cloud Security Analytics
  - 5.2.4 Application Security Analytics
- 5.3 Services
  - 5.3.1 Professional Services
  - 5.3.2 Managed Services

## **6 GLOBAL SECURITY ANALYTICS MARKET, BY DEPLOYMENT MODE**

- 6.1 Introduction
- 6.2 On-Premises
- 6.3 Cloud-Based

## **7 GLOBAL SECURITY ANALYTICS MARKET, BY ORGANIZATION SIZE**

- 7.1 Introduction
- 7.2 Small & Medium Enterprises (SMEs)
- 7.3 Large Enterprises

## **8 GLOBAL SECURITY ANALYTICS MARKET, BY APPLICATION**

- 8.1 Introduction
- 8.2 Threat Intelligence & Detection
- 8.3 Behavioral Analytics
- 8.4 Log Management & Security Information and Event Management (SIEM)
- 8.5 Data Loss Prevention
- 8.6 Incident Forensics
- 8.7 Risk & Compliance Management
- 8.8 Other Applications

## **9 GLOBAL SECURITY ANALYTICS MARKET, BY END USER**

- 9.1 Introduction
- 9.2 Banking, Financial Services & Insurance (BFSI)

- 9.3 IT & Telecommunications
- 9.4 Retail & E-commerce
- 9.5 Healthcare & Life Sciences
- 9.6 Government & Defense
- 9.7 Energy & Utilities
- 9.8 Manufacturing
- 9.9 Education
- 9.10 Other End Users

## **10 GLOBAL SECURITY ANALYTICS MARKET, BY GEOGRAPHY**

- 10.1 Introduction
- 10.2 North America
  - 10.2.1 US
  - 10.2.2 Canada
  - 10.2.3 Mexico
- 10.3 Europe
  - 10.3.1 Germany
  - 10.3.2 UK
  - 10.3.3 Italy
  - 10.3.4 France
  - 10.3.5 Spain
  - 10.3.6 Rest of Europe
- 10.4 Asia Pacific
  - 10.4.1 Japan
  - 10.4.2 China
  - 10.4.3 India
  - 10.4.4 Australia
  - 10.4.5 New Zealand
  - 10.4.6 South Korea
  - 10.4.7 Rest of Asia Pacific
- 10.5 South America
  - 10.5.1 Argentina
  - 10.5.2 Brazil
  - 10.5.3 Chile
  - 10.5.4 Rest of South America
- 10.6 Middle East & Africa
  - 10.6.1 Saudi Arabia
  - 10.6.2 UAE

- 10.6.3 Qatar
- 10.6.4 South Africa
- 10.6.5 Rest of Middle East & Africa

## **11 KEY DEVELOPMENTS**

- 11.1 Agreements, Partnerships, Collaborations and Joint Ventures
- 11.2 Acquisitions & Mergers
- 11.3 New Product Launch
- 11.4 Expansions
- 11.5 Other Key Strategies

## **12 COMPANY PROFILING**

- 12.1 IBM Corporation
- 12.2 Cisco Systems, Inc.
- 12.3 Splunk Inc.
- 12.4 Palo Alto Networks, Inc.
- 12.5 Fortinet, Inc.
- 12.6 McAfee Corp.
- 12.7 Microsoft Corporation
- 12.8 RSA Security LLC
- 12.9 Rapid7, Inc.
- 12.10 Exabeam, Inc.
- 12.11 LogRhythm, Inc.
- 12.12 Sumo Logic, Inc.
- 12.13 Huntsman Security
- 12.14 Gurukul
- 12.15 Varonis Systems, Inc.
- 12.16 Devo Technology
- 12.17 Graylog, Inc.

## List Of Tables

### LIST OF TABLES

- 1 Global Security Analytics Market Outlook, By Region (2024-2032) (\$MN)
- 2 Global Security Analytics Market Outlook, By Component (2024-2032) (\$MN)
- 3 Global Security Analytics Market Outlook, By Solutions (2024-2032) (\$MN)
- 4 Global Security Analytics Market Outlook, By Network Security Analytics (2024-2032) (\$MN)
- 5 Global Security Analytics Market Outlook, By Endpoint Security Analytics (2024-2032) (\$MN)
- 6 Global Security Analytics Market Outlook, By Cloud Security Analytics (2024-2032) (\$MN)
- 7 Global Security Analytics Market Outlook, By Application Security Analytics (2024-2032) (\$MN)
- 8 Global Security Analytics Market Outlook, By Services (2024-2032) (\$MN)
- 9 Global Security Analytics Market Outlook, By Professional Services (2024-2032) (\$MN)
- 10 Global Security Analytics Market Outlook, By Managed Services (2024-2032) (\$MN)
- 11 Global Security Analytics Market Outlook, By Deployment Mode (2024-2032) (\$MN)
- 12 Global Security Analytics Market Outlook, By On-Premises (2024-2032) (\$MN)
- 13 Global Security Analytics Market Outlook, By Cloud-Based (2024-2032) (\$MN)
- 14 Global Security Analytics Market Outlook, By Organization Size (2024-2032) (\$MN)
- 15 Global Security Analytics Market Outlook, By Small & Medium Enterprises (SMEs) (2024-2032) (\$MN)
- 16 Global Security Analytics Market Outlook, By Large Enterprises (2024-2032) (\$MN)
- 17 Global Security Analytics Market Outlook, By Application (2024-2032) (\$MN)
- 18 Global Security Analytics Market Outlook, By Threat Intelligence & Detection (2024-2032) (\$MN)
- 19 Global Security Analytics Market Outlook, By Behavioral Analytics (2024-2032) (\$MN)
- 20 Global Security Analytics Market Outlook, By Log Management & Security Information and Event Management (SIEM) (2024-2032) (\$MN)
- 21 Global Security Analytics Market Outlook, By Data Loss Prevention (2024-2032) (\$MN)
- 22 Global Security Analytics Market Outlook, By Incident Forensics (2024-2032) (\$MN)
- 23 Global Security Analytics Market Outlook, By Risk & Compliance Management (2024-2032) (\$MN)
- 24 Global Security Analytics Market Outlook, By Other Applications (2024-2032) (\$MN)

- 25 Global Security Analytics Market Outlook, By End User (2024-2032) (\$MN)
- 26 Global Security Analytics Market Outlook, By Banking, Financial Services & Insurance (BFSI) (2024-2032) (\$MN)
- 27 Global Security Analytics Market Outlook, By IT & Telecommunications (2024-2032) (\$MN)
- 28 Global Security Analytics Market Outlook, By Retail & E-commerce (2024-2032) (\$MN)
- 29 Global Security Analytics Market Outlook, By Healthcare & Life Sciences (2024-2032) (\$MN)
- 30 Global Security Analytics Market Outlook, By Government & Defense (2024-2032) (\$MN)
- 31 Global Security Analytics Market Outlook, By Energy & Utilities (2024-2032) (\$MN)
- 32 Global Security Analytics Market Outlook, By Manufacturing (2024-2032) (\$MN)
- 33 Global Security Analytics Market Outlook, By Education (2024-2032) (\$MN)
- 34 Global Security Analytics Market Outlook, By Other End Users (2024-2032) (\$MN)

Note: Tables for North America, Europe, APAC, South America, and Middle East & Africa Regions are also represented in the same manner as above.

## I would like to order

Product name: Security Analytics Market Forecasts to 2032 – Global Analysis By Component (Solutions and Services), Deployment Mode (On-Premises and Cloud-Based), Organization Size, Application, End User and By Geography

Product link: <https://marketpublishers.com/r/S64F4A3ACDD5EN.html>

Price: US\$ 4,150.00 (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/S64F4A3ACDD5EN.html>