

Security Orchestration Automation Response (SOAR) Market Set to Reach USD 5.7 Billion by 2033

The global Security Orchestration Automation Response (SOAR) market is projected to grow from USD 1.5 billion in 2024 to USD 5.7 billion by 2033

VANCOUVER, BRITISH COLUMBIA,
CANADA, May 14, 2025

/EINPresswire.com/ -- The latest report titled Global [Security Orchestration Automation Response Market](#) contains an in-depth analysis of the fundamental parameters contributing to the global Security Orchestration Automation Response market

scenario. This research report offers readers an in-depth interpretation of the dynamics of the Security Orchestration Automation Response market, including key drivers, opportunities, threats, and challenges. The report also briefly discusses key business strategies, supply-demand ratios, key regions, prominent market players, and offers a future outlook for the overall Security Orchestration Automation Response industry.

The global Security Orchestration Automation Response (SOAR) market is projected to grow from USD 1.5 billion in 2024 to USD 5.7 billion by 2033, expanding at a steady CAGR of 16.00%, according to a new market analysis.

This strong growth is being fueled by an increasing number of cybersecurity threats and the rising need for quicker, more efficient incident responses. Organizations today face complex and frequent security incidents, making it harder for security teams to manage threats using traditional methods. SOAR platforms help fill this gap by automating routine tasks and bringing different security tools together in one place, allowing faster and more accurate responses.

You Can Download Free Sample PDF Copy Of This Report At
<https://www.emergenresearch.com/request-sample/4556>



One of the main drivers behind the market growth is the shortage of skilled cybersecurity professionals. With limited human resources, businesses are turning to automation to keep up with evolving threats. A recent SANS Institute survey revealed that nearly 60% of cybersecurity professionals believe automating security workflows is essential to improve operations. The use of AI and machine learning in SOAR tools also enhances threat detection and decision-making, giving companies a more proactive way to protect their systems.

SOAR platforms are increasingly being adopted across industries like finance, healthcare, and government. These sectors are investing in advanced security tools not just to stay protected but also to meet strict compliance and data protection regulations. According to the Ponemon Institute, over half of financial institutions spend more time dealing with manual processes than addressing security risks, and about 75% face challenges in prioritizing critical patches due to disconnected systems.

Phishing emails and ransomware attacks are also contributing to the growing demand for SOAR tools. With attackers using more sophisticated tactics, businesses are struggling to keep up. SOAR solutions help by automatically identifying threats, blocking suspicious messages, and acting quickly to isolate affected systems. Data from CERT-In shows ransomware attacks rose 53% in 2022, highlighting the urgent need for faster response capabilities.

However, the market does face challenges. Many organizations are cautious about using third-party applications due to concerns about data security and privacy. This is especially true in highly regulated sectors such as healthcare and finance. Trust issues around data sharing and software vulnerabilities can slow down the adoption of SOAR tools. To overcome this, providers must ensure strong data protection measures and comply with strict industry standards.

In terms of market segments, SOAR platforms and solutions accounted for the largest share in 2024. Businesses, especially larger enterprises, are prioritizing investment in centralized tools that improve incident response and integrate easily with existing security systems. These platforms often come equipped with AI-driven features, automated workflows, and case management capabilities that help security teams respond faster and more effectively.

Meanwhile, the services segment is expected to grow the fastest during the forecast period. As companies continue to struggle with a lack of in-house cybersecurity expertise, they are seeking help from professionals for solution deployment, integration, and management. Cloud-based SOAR tools have also boosted the need for ongoing support and consulting services, as businesses aim for smooth and secure implementation.

Request Customization: <https://www.emergenresearch.com/request-for-customization/4556>

Competitive Terrain:

The global Security Orchestration Automation Response industry is highly consolidated owing to

the presence of renowned companies operating across several international and local segments of the market. These players dominate the industry in terms of their strong geographical reach and a large number of production facilities. The companies are intensely competitive against one another and excel in their individual technological capabilities, as well as product development, innovation, and product pricing strategies.

Some major companies included in the Security Orchestration Automation Response market report are:

IBM

Cisco

Rapid7

Palo Alto Networks

Splunk

Swimlane

Tufin

Fortinet

ThreatConnect

Trellix

Sumo Logic

Siemplify

The report further divides the Security Orchestration Automation Response market into key segments such as types, applications, end-user industries, technologies, and key regions of the market. The report also sheds light on the segment and region exhibiting promising growth in the Security Orchestration Automation Response market.

Security Orchestration Automation Response Market Segmentation Analysis

By Offering Outlook (Revenue, USD Billion; 2020-2033)

Platform and Solutions

Services

Professional Services

Managed Services

By Deployment Mode Outlook (Revenue, USD Billion; 2020-2033)

Cloud

On-premises

By Organization Size Outlook (Revenue, USD Billion; 2020-2033)

SIMES

Large Enterprises

By Application Outlook (Revenue, USD Billion; 2020-2033)

Threat Intelligence

Network Forensics

Incident Response

Compliance

Workflow Management

Other Applications

By Vertical Outlook (Revenue, USD Billion; 2020-2033)

BFSI

Government

Energy and Utilities

Healthcare

Retail and eCommerce

IT and ITES

Other Verticals

Browse Full Report: <https://www.emergenresearch.com/industry-report/security-orchestration-automation-response-market>

Regional Outlook:

North America (the U.S., Canada, Mexico)

Europe (the U.K., Germany, France, Italy)

Asia Pacific (India, China, Japan, Korea)

Latin America (Brazil, Argentina, Ecuador, Chile)

Middle East & Africa (Egypt, Turkey, Saudi Arabia, Iran)

Key Questions Answered by the Report:

Which region is expected to dominate the market in the coming years?

What are the recent technological and product advancements occurring in the market?

What are the key strategies adopted by the prominent players in the Security Orchestration Automation Response market?

What are the key product types and applications of the Security Orchestration Automation Response industry?

What is the outcome of SWOT analysis and Porter's Five Forces analysis?

How is the competitive landscape of the Security Orchestration Automation Response market?

Who are the key players in the industry?

What is the growth rate of the industry over the coming years?

What will be the valuation of the Security Orchestration Automation Response Market by 2033?

Thank you for reading our report. For further details or to inquire about customization, please let us know and we will offer you the report as per your needs.

Eric Lee

Emergen Research

+ +91 90210 91709

sales@emergenresearch.com

Visit us on social media:

[LinkedIn](#)

[Facebook](#)

[X](#)

This press release can be viewed online at: <https://www.einpresswire.com/article/812606581>

EIN Presswire's priority is source transparency. We do not allow opaque clients, and our editors try to be careful about weeding out false and misleading content. As a user, if you see something we have missed, please do bring it to our attention. Your help is welcome. EIN Presswire, Everyone's Internet News Presswire™, tries to define some of the boundaries that are reasonable in today's world. Please see our Editorial Guidelines for more information.

© 1995-2025 Newsmatics Inc. All Right Reserved.