

Extended Detection and Response Market - Global Industry Size, Share, Trends, Opportunity, and Forecast Segmented By Component (Solution, Service), By Deployment Model (On Premise, Cloud), By Enterprise Size (Large Enterprises, SMEs), By Industry Vertical (BFSI, Government, Manufacturing, Energy and Utilities, Healthcare, Retail and E Commerce, IT and Telecom, Others), By Region & Competition, 2021-2031F

<https://marketpublishers.com/r/E3E844590529EN.html>

Date: January 2026

Pages: 180

Price: US\$ 4,500.00 (Single User License)

ID: E3E844590529EN

Abstracts

The Global Extended Detection and Response Market is projected to experience significant growth, rising from USD 2.07 Billion in 2025 to USD 7.04 Billion by 2031, representing a CAGR of 22.63%. XDR functions as a centralized security framework that consolidates data from endpoints, cloud workloads, and networks to enable automated threat detection and swift mitigation. This market expansion is primarily fueled by the increasing volume of complex cyber threats and the critical need for unified security visibility across dispersed enterprise environments, alongside regulatory compliance mandates that compel organizations to uphold strict security standards and comprehensive incident reporting protocols.

However, the broad implementation of these solutions is significantly hindered by an acute shortage of skilled professionals needed to manage such complex security operations. This workforce deficit restricts the ability of organizations to maximize the potential of XDR capabilities. As highlighted in the 'ISC2 Cybersecurity Workforce Study' of '2024', the global cybersecurity workforce gap widened by 19%, resulting in a total of 4.8 million unfilled positions, which underscores the severity of this impediment

to market growth.

Market Driver

The rising frequency and complexity of advanced cyber threats act as a major catalyst for the adoption of Extended Detection and Response solutions. As threat actors employ increasingly sophisticated techniques to evade standard perimeter defenses, organizations are forced to invest in platforms that provide extensive visibility and deep analytical capabilities. This surge in malicious behavior necessitates systems that can detect anomalies across diverse vectors simultaneously to avert data breaches. According to SonicWall's '2024 Mid-Year Cyber Threat Report' from August 2024, global malware attacks rose by 30% in the first half of the year compared to 2023, emphasizing the vital need for the integrated threat intelligence offered by XDR frameworks.

Concurrently, the market is driven by a strategic shift toward unifying isolated security solutions to overcome operational inefficiencies. Enterprises often face fragmented visibility and slower response times due to the management of disjointed tools, prompting the adoption of XDR to consolidate control points and reduce vendor sprawl. This issue is corroborated by Cisco's '2024 Cybersecurity Readiness Index' from March 2024, where 80% of organizations reported that juggling multiple point solutions hindered their incident response capabilities. Furthermore, the urgency for robust defenses is reflected in broader risk assessments; Allianz ranked cyber incidents as the top global business risk in 2024, a concern identified by 36% of respondents.

Market Challenge

The pervasive shortage of skilled cybersecurity professionals poses a critical challenge that directly hampers the expansion of the Global Extended Detection and Response (XDR) Market. XDR frameworks are designed to aggregate and correlate massive volumes of telemetry from endpoints, networks, and cloud environments, a process that demands experienced analysts to interpret complex threat data and execute precise responses. When organizations lack the necessary human expertise to oversee these comprehensive platforms, the functional value of XDR is significantly diminished, often resulting in underutilization and a lower return on investment.

This workforce gap creates a substantial bottleneck in market growth, as enterprises hesitate to acquire advanced security solutions they cannot effectively staff. The operational deficit limits the scalable adoption of XDR, as companies struggle to secure

the personnel required to monitor and act upon the automated insights these tools generate. As reported by ISACA in 2024, 57% of organizations indicated that their cybersecurity teams were understaffed. This persistent lack of qualified resources forces many businesses to delay or limit their deployment of integrated security technologies, thereby slowing the overall momentum of the market.

Market Trends

The incorporation of generative artificial intelligence represents a major trend within the XDR landscape, fundamentally transforming how platforms process and investigate threat telemetry. Vendors are rapidly integrating Large Language Models into their architectures to automate the interpretation of complex attack chains, allowing analysts to use natural language for data queries and receive immediate remediation suggestions. This technological advancement reduces the manual effort required for investigations and speeds up root cause identification. As noted in IBM's 'Cost of a Data Breach Report 2024' from July 2024, organizations utilizing extensive security AI and automation saved an average of USD 2.22 million in breach costs compared to those without, validating the financial and operational benefits of these features.

Simultaneously, the market is seeing a strategic broadening of detection coverage to include Operational Technology and Internet of Things assets. As industrial environments increasingly connect to corporate networks, XDR platforms are evolving to ingest proprietary industrial protocols and correlate them with standard IT security events to eliminate visibility blind spots. This convergence is essential for protecting infrastructure where legacy devices often lack native security controls and are prone to lateral movement attacks. The necessity for this unified monitoring is highlighted by Fortinet's '2024 State of Operational Technology and Cybersecurity Report' from May 2024, which found that 73% of organizations suffered intrusions affecting OT systems or both IT and OT environments.

Key Market Players

Bitdefender

BROADCOM

Cybereason

Cynet Systems Private Limited

Fidelis Cybersecurity

MCAFEE

Microsoft Corporation

Palo Alto Networks

RED PIRANHA LIMITED

Sophos Ltd

Report Scope

In this report, the Global Extended Detection and Response Market has been segmented into the following categories, in addition to the industry trends which have also been detailed below:

Extended Detection and Response Market, By Component

Solution

Service

Extended Detection and Response Market, By Deployment Model

On Premise

Cloud

Extended Detection and Response Market, By Enterprise Size

Large Enterprises

SMEs

Extended Detection and Response Market, By Industry Vertical

BFSI

Government

Manufacturing

Energy and Utilities

Healthcare

Retail and E Commerce

IT and Telecom

Others

Extended Detection and Response Market, By Region

North America

United States

Canada

Mexico

Europe

France

United Kingdom

Italy

Germany

Spain

Asia Pacific

China

India

Japan

Australia

South Korea

South America

Brazil

Argentina

Colombia

Middle East & Africa

South Africa

Saudi Arabia

UAE

Competitive Landscape

Company Profiles: Detailed analysis of the major companies present in the Global Extended Detection and Response Market.

Available Customizations:

Global Extended Detection and Response 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:

Extended Detection and Response Market - Global Industry Size, Share, Trends, Opportunity, and Forecast Segmen...

Company Information

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

Contents

1. PRODUCT OVERVIEW

- 1.1. Market Definition
- 1.2. Scope of the Market
 - 1.2.1. Markets Covered
 - 1.2.2. Years Considered for Study
 - 1.2.3. Key Market Segmentations

2. RESEARCH METHODOLOGY

- 2.1. Objective of the Study
- 2.2. Baseline Methodology
- 2.3. Key Industry Partners
- 2.4. Major Association and Secondary Sources
- 2.5. Forecasting Methodology
- 2.6. Data Triangulation & Validation
- 2.7. Assumptions and Limitations

3. EXECUTIVE SUMMARY

- 3.1. Overview of the Market
- 3.2. Overview of Key Market Segmentations
- 3.3. Overview of Key Market Players
- 3.4. Overview of Key Regions/Countries
- 3.5. Overview of Market Drivers, Challenges, Trends

4. VOICE OF CUSTOMER

5. GLOBAL EXTENDED DETECTION AND RESPONSE MARKET OUTLOOK

- 5.1. Market Size & Forecast
 - 5.1.1. By Value
- 5.2. Market Share & Forecast
 - 5.2.1. By Component (Solution, Service)
 - 5.2.2. By Deployment Model (On Premise, Cloud)
 - 5.2.3. By Enterprise Size (Large Enterprises, SMEs)
 - 5.2.4. By Industry Vertical (BFSI, Government, Manufacturing, Energy and Utilities,

Healthcare, Retail and E Commerce, IT and Telecom, Others)

5.2.5. By Region

5.2.6. By Company (2025)

5.3. Market Map

6. NORTH AMERICA EXTENDED DETECTION AND RESPONSE MARKET OUTLOOK

6.1. Market Size & Forecast

6.1.1. By Value

6.2. Market Share & Forecast

6.2.1. By Component

6.2.2. By Deployment Model

6.2.3. By Enterprise Size

6.2.4. By Industry Vertical

6.2.5. By Country

6.3. North America: Country Analysis

6.3.1. United States Extended Detection and Response Market Outlook

6.3.1.1. Market Size & Forecast

6.3.1.1.1. By Value

6.3.1.2. Market Share & Forecast

6.3.1.2.1. By Component

6.3.1.2.2. By Deployment Model

6.3.1.2.3. By Enterprise Size

6.3.1.2.4. By Industry Vertical

6.3.2. Canada Extended Detection and Response Market Outlook

6.3.2.1. Market Size & Forecast

6.3.2.1.1. By Value

6.3.2.2. Market Share & Forecast

6.3.2.2.1. By Component

6.3.2.2.2. By Deployment Model

6.3.2.2.3. By Enterprise Size

6.3.2.2.4. By Industry Vertical

6.3.3. Mexico Extended Detection and Response Market Outlook

6.3.3.1. Market Size & Forecast

6.3.3.1.1. By Value

6.3.3.2. Market Share & Forecast

6.3.3.2.1. By Component

6.3.3.2.2. By Deployment Model

6.3.3.2.3. By Enterprise Size

6.3.3.2.4. By Industry Vertical

7. EUROPE EXTENDED DETECTION AND RESPONSE MARKET OUTLOOK

7.1. Market Size & Forecast

7.1.1. By Value

7.2. Market Share & Forecast

7.2.1. By Component

7.2.2. By Deployment Model

7.2.3. By Enterprise Size

7.2.4. By Industry Vertical

7.2.5. By Country

7.3. Europe: Country Analysis

7.3.1. Germany Extended Detection and Response Market Outlook

7.3.1.1. Market Size & Forecast

7.3.1.1.1. By Value

7.3.1.2. Market Share & Forecast

7.3.1.2.1. By Component

7.3.1.2.2. By Deployment Model

7.3.1.2.3. By Enterprise Size

7.3.1.2.4. By Industry Vertical

7.3.2. France Extended Detection and Response Market Outlook

7.3.2.1. Market Size & Forecast

7.3.2.1.1. By Value

7.3.2.2. Market Share & Forecast

7.3.2.2.1. By Component

7.3.2.2.2. By Deployment Model

7.3.2.2.3. By Enterprise Size

7.3.2.2.4. By Industry Vertical

7.3.3. United Kingdom Extended Detection and Response Market Outlook

7.3.3.1. Market Size & Forecast

7.3.3.1.1. By Value

7.3.3.2. Market Share & Forecast

7.3.3.2.1. By Component

7.3.3.2.2. By Deployment Model

7.3.3.2.3. By Enterprise Size

7.3.3.2.4. By Industry Vertical

7.3.4. Italy Extended Detection and Response Market Outlook

- 7.3.4.1. Market Size & Forecast
 - 7.3.4.1.1. By Value
- 7.3.4.2. Market Share & Forecast
 - 7.3.4.2.1. By Component
 - 7.3.4.2.2. By Deployment Model
 - 7.3.4.2.3. By Enterprise Size
 - 7.3.4.2.4. By Industry Vertical
- 7.3.5. Spain Extended Detection and Response Market Outlook
 - 7.3.5.1. Market Size & Forecast
 - 7.3.5.1.1. By Value
 - 7.3.5.2. Market Share & Forecast
 - 7.3.5.2.1. By Component
 - 7.3.5.2.2. By Deployment Model
 - 7.3.5.2.3. By Enterprise Size
 - 7.3.5.2.4. By Industry Vertical

8. ASIA PACIFIC EXTENDED DETECTION AND RESPONSE MARKET OUTLOOK

- 8.1. Market Size & Forecast
 - 8.1.1. By Value
- 8.2. Market Share & Forecast
 - 8.2.1. By Component
 - 8.2.2. By Deployment Model
 - 8.2.3. By Enterprise Size
 - 8.2.4. By Industry Vertical
 - 8.2.5. By Country
- 8.3. Asia Pacific: Country Analysis
 - 8.3.1. China Extended Detection and Response Market Outlook
 - 8.3.1.1. Market Size & Forecast
 - 8.3.1.1.1. By Value
 - 8.3.1.2. Market Share & Forecast
 - 8.3.1.2.1. By Component
 - 8.3.1.2.2. By Deployment Model
 - 8.3.1.2.3. By Enterprise Size
 - 8.3.1.2.4. By Industry Vertical
 - 8.3.2. India Extended Detection and Response Market Outlook
 - 8.3.2.1. Market Size & Forecast
 - 8.3.2.1.1. By Value
 - 8.3.2.2. Market Share & Forecast

- 8.3.2.2.1. By Component
- 8.3.2.2.2. By Deployment Model
- 8.3.2.2.3. By Enterprise Size
- 8.3.2.2.4. By Industry Vertical
- 8.3.3. Japan Extended Detection and Response Market Outlook
 - 8.3.3.1. Market Size & Forecast
 - 8.3.3.1.1. By Value
 - 8.3.3.2. Market Share & Forecast
 - 8.3.3.2.1. By Component
 - 8.3.3.2.2. By Deployment Model
 - 8.3.3.2.3. By Enterprise Size
 - 8.3.3.2.4. By Industry Vertical
- 8.3.4. South Korea Extended Detection and Response Market Outlook
 - 8.3.4.1. Market Size & Forecast
 - 8.3.4.1.1. By Value
 - 8.3.4.2. Market Share & Forecast
 - 8.3.4.2.1. By Component
 - 8.3.4.2.2. By Deployment Model
 - 8.3.4.2.3. By Enterprise Size
 - 8.3.4.2.4. By Industry Vertical
- 8.3.5. Australia Extended Detection and Response Market Outlook
 - 8.3.5.1. Market Size & Forecast
 - 8.3.5.1.1. By Value
 - 8.3.5.2. Market Share & Forecast
 - 8.3.5.2.1. By Component
 - 8.3.5.2.2. By Deployment Model
 - 8.3.5.2.3. By Enterprise Size
 - 8.3.5.2.4. By Industry Vertical

9. MIDDLE EAST & AFRICA EXTENDED DETECTION AND RESPONSE MARKET OUTLOOK

- 9.1. Market Size & Forecast
 - 9.1.1. By Value
- 9.2. Market Share & Forecast
 - 9.2.1. By Component
 - 9.2.2. By Deployment Model
 - 9.2.3. By Enterprise Size
 - 9.2.4. By Industry Vertical

9.2.5. By Country

9.3. Middle East & Africa: Country Analysis

9.3.1. Saudi Arabia Extended Detection and Response Market Outlook

9.3.1.1. Market Size & Forecast

9.3.1.1.1. By Value

9.3.1.2. Market Share & Forecast

9.3.1.2.1. By Component

9.3.1.2.2. By Deployment Model

9.3.1.2.3. By Enterprise Size

9.3.1.2.4. By Industry Vertical

9.3.2. UAE Extended Detection and Response Market Outlook

9.3.2.1. Market Size & Forecast

9.3.2.1.1. By Value

9.3.2.2. Market Share & Forecast

9.3.2.2.1. By Component

9.3.2.2.2. By Deployment Model

9.3.2.2.3. By Enterprise Size

9.3.2.2.4. By Industry Vertical

9.3.3. South Africa Extended Detection and Response Market Outlook

9.3.3.1. Market Size & Forecast

9.3.3.1.1. By Value

9.3.3.2. Market Share & Forecast

9.3.3.2.1. By Component

9.3.3.2.2. By Deployment Model

9.3.3.2.3. By Enterprise Size

9.3.3.2.4. By Industry Vertical

10. SOUTH AMERICA EXTENDED DETECTION AND RESPONSE MARKET OUTLOOK

10.1. Market Size & Forecast

10.1.1. By Value

10.2. Market Share & Forecast

10.2.1. By Component

10.2.2. By Deployment Model

10.2.3. By Enterprise Size

10.2.4. By Industry Vertical

10.2.5. By Country

10.3. South America: Country Analysis

- 10.3.1. Brazil Extended Detection and Response Market Outlook
 - 10.3.1.1. Market Size & Forecast
 - 10.3.1.1.1. By Value
 - 10.3.1.2. Market Share & Forecast
 - 10.3.1.2.1. By Component
 - 10.3.1.2.2. By Deployment Model
 - 10.3.1.2.3. By Enterprise Size
 - 10.3.1.2.4. By Industry Vertical
- 10.3.2. Colombia Extended Detection and Response Market Outlook
 - 10.3.2.1. Market Size & Forecast
 - 10.3.2.1.1. By Value
 - 10.3.2.2. Market Share & Forecast
 - 10.3.2.2.1. By Component
 - 10.3.2.2.2. By Deployment Model
 - 10.3.2.2.3. By Enterprise Size
 - 10.3.2.2.4. By Industry Vertical
- 10.3.3. Argentina Extended Detection and Response Market Outlook
 - 10.3.3.1. Market Size & Forecast
 - 10.3.3.1.1. By Value
 - 10.3.3.2. Market Share & Forecast
 - 10.3.3.2.1. By Component
 - 10.3.3.2.2. By Deployment Model
 - 10.3.3.2.3. By Enterprise Size
 - 10.3.3.2.4. By Industry Vertical

11. MARKET DYNAMICS

- 11.1. Drivers
- 11.2. Challenges

12. MARKET TRENDS & DEVELOPMENTS

- 12.1. Merger & Acquisition (If Any)
- 12.2. Product Launches (If Any)
- 12.3. Recent Developments

13. GLOBAL EXTENDED DETECTION AND RESPONSE MARKET: SWOT ANALYSIS

14. PORTER'S FIVE FORCES ANALYSIS

- 14.1. Competition in the Industry
- 14.2. Potential of New Entrants
- 14.3. Power of Suppliers
- 14.4. Power of Customers
- 14.5. Threat of Substitute Products

15. COMPETITIVE LANDSCAPE

- 15.1. Bitdefender
 - 15.1.1. Business Overview
 - 15.1.2. Products & Services
 - 15.1.3. Recent Developments
 - 15.1.4. Key Personnel
 - 15.1.5. SWOT Analysis
- 15.2. BROADCOM
- 15.3. Cybereason
- 15.4. Cynet Systems Private Limited
- 15.5. Fidelis Cybersecurity
- 15.6. MCAFEE
- 15.7. Microsoft Corporation
- 15.8. Palo Alto Networks
- 15.9. RED PIRANHA LIMITED
- 15.10. Sophos Ltd

16. STRATEGIC RECOMMENDATIONS

17. ABOUT US & DISCLAIMER

I would like to order

Product name: Extended Detection and Response Market - Global Industry Size, Share, Trends, Opportunity, and Forecast Segmented By Component (Solution, Service), By Deployment Model (On Premise, Cloud), By Enterprise Size (Large Enterprises, SMEs), By Industry Vertical (BFSI, Government, Manufacturing, Energy and Utilities, Healthcare, Retail and E Commerce, IT and Telecom, Others), By Region & Competition, 2021-2031F

Product link: <https://marketpublishers.com/r/E3E844590529EN.html>

Price: US\$ 4,500.00 (Single User License / Electronic Delivery)

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

info@marketpublishers.com

Payment

To pay by Credit Card (Visa, MasterCard, American Express, PayPal), please, click button on product page <https://marketpublishers.com/r/E3E844590529EN.html>