+357 96 030922
info@marketpublishers.com

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

+357 96 030922
info@marketpublishers.com

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

+357 96 030922
info@marketpublishers.com

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

+357 96 030922
info@marketpublishers.com

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

+357 96 030922
info@marketpublishers.com

- 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

+357 96 030922
info@marketpublishers.com

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:

+357 96 030922
info@marketpublishers.com

Company Information

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

+357 96 030922
info@marketpublishers.com

Contents

+357 96 030922
info@marketpublishers.com

6. NORTH AMERICA EXTENDED DETECTION AND RESPONSE MARKET OUTLOOK

+357 96 030922
info@marketpublishers.com

7. EUROPE EXTENDED DETECTION AND RESPONSE MARKET OUTLOOK

+357 96 030922
info@marketpublishers.com

8. ASIA PACIFIC EXTENDED DETECTION AND RESPONSE MARKET OUTLOOK

+357 96 030922
info@marketpublishers.com

+357 96 030922
info@marketpublishers.com

10. SOUTH AMERICA EXTENDED DETECTION AND RESPONSE MARKET OUTLOOK

+357 96 030922
info@marketpublishers.com

+357 96 030922
info@marketpublishers.com

14. PORTER'S FIVE FORCES ANALYSIS

15. COMPETITIVE LANDSCAPE

16. STRATEGIC RECOMMENDATIONS

17. ABOUT US & DISCLAIMER

+357 96 030922
info@marketpublishers.com

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