Endpoint Detection and Response - Market Share Analysis, Industry Trends & Statistics, Growth Forecasts 2021 - 2029

Market Report | 2024-02-17 | 120 pages | Mordor Intelligence

AVAILABLE LICENSES:

- Single User License $4750.00
- Team License (1-7 Users) $5250.00
- Site License $6500.00
- Corporate License $8750.00

Report description:

The Endpoint Detection and Response Market size is estimated at USD 4.58 billion in 2024, and is expected to reach USD 13.37 billion by 2029, growing at a CAGR of 23.88% during the forecast period (2024-2029).

Key Highlights
-Businesses have been able to safeguard their networks from common cyber security threats due to sophisticated malware detection. Because of the considerable increase in remote working activities, organizations in the endpoint detection and response (EDR) sector are under scrutiny for offering safe and trustworthy endpoint software.
-EDR tools are technological platforms that enable rapid investigation and containment of endpoint threats and warn security teams of potentially dangerous behaviors. Endpoints include an employee's workstation or laptop, a server, a cloud system, a smartphone, or an IoT device. Endpoint data such as process execution, terminal communication, and client logins are often aggregated by EDR systems, which then analyze the data to detect anomalies and suspected threats and record data regarding harmful behavior. This provides security teams with the knowledge they need to investigate and resolve concerns. They also enable manual and automated tasks on the endpoint to neutralize threats, such as wiping and reimaging the device or isolating it from the network.
-With a strategy to secure their IT processes and systems, secure customer critical data, and comply with government regulations, public and private banking institutes are focusing on implementing the latest technology to prevent cyber attacks. Besides, with greater customer expectations, rising technological capabilities, and regulatory requirements, banking institutions are pushed to adopt a proactive security approach. With the growing technological penetration and digital channels, such as internet banking, mobile banking, etc., online banking has become customers' preferred choice for banking services. There is a significant need for banks to leverage advanced authentication and access control processes.
-With the increasing adoption of cloud and cloud-based operations, poorly secured cloud databases remain weak for

organizations, ranging from simple misconfiguration issues to vulnerabilities in hardware chips. Multiple tools are available widely, which enable potential attackers to identify misconfigured cloud resources on the internet. Hence, for organizations, adopting effective security solutions is of utmost importance. Moreover, quick detection and response also play a vital role in addressing such threats.
-The lockdown imposed by many governments has positively affected the adoption of endpoint detection and response (EDR). Following the effects of COVID-19, businesses are focused on advanced solutions to safely and securely undertake contactless activities. AI-powered solutions, computing technology, automation, and cloud-based endpoint detection and response are examples of these technologies used in industries such as BFSI, healthcare, government, and others. Furthermore, as businesses digitalize, there is an increasing demand for an EDR solution that is dependable, AI-integrated, and has real-time reporting capabilities.
-Outsourcing security activities to a third-party EDR network operator has several drawbacks, including the security of the third-party infrastructure and a loss of control. If the service company's cyber architecture is to be effective in combating the most recent sophisticated threats, it must be safe and up-to-date. The infrastructure of an EDR service provider may contain sensitive customer and employee information from multiple companies, making it more vulnerable to frequent and complex attacks. As a result, businesses may be hesitant to give these service providers access to valuable data.

Endpoint Detection and Response (EDR) Market Trends

Bring your Own Device (BYOD) Adoption and Increased Remote Working

- Due to the growing popularity and quick adoption of hybrid work models, employees are empowered to perform their job from wherever they are and on whatever device they have. On the other hand, hybrid and remote work policies underline the significance of effective data protection and endpoint security solutions.
- As indicated by the federal government's push to implement CMMC 2.0, the ability of both commercial and public sector organizations to achieve compliance and adopt the cybersecurity and data protection standards established in industry frameworks is more important than ever.
- Bring-your-own device (BYOD) models pose several threats to the enterprise in which they are implemented. Some are about corporate data, while others are about privacy concerns. The following are some of the most typical hazards of implementing BYOD: Unauthorized programs placed on a device might raise security concerns since they jeopardize the integrity, availability, and confidentiality of an organization's information and systems. Threat actors can utilize programs to carry out the malicious purpose and potentially get access to the device's location, network settings, files, applications, and data. Crypto virus can disrupt data availability and integrity. Such threats are expected to drive the studied market.
- Businesses should evaluate security requirements while developing rules to protect devices and data. For example, in many companies, compliance is a significant concern; implementing risk and compliance solutions on endpoints may be crucial for appropriately protecting sensitive information. Furthermore, BYOD rules should include a planned reaction to various crisis scenarios, such as lost devices or fired staff.
- According to CapRelo, last year, 48.4% of global respondents said the opportunity to work remotely is significant when making future job decisions. 87.4% of respondents responded that remote work is essential to future career decisions.
- Further, according to HP, Inc., 41% of remote employees worldwide said they had access to client data last year. Other forms of data commonly accessible when working remotely are operational data, financial information, and human resource data. Because the corporate firewall did not secure distributed workers, this caused IT security vulnerabilities. This would drive the demand for the studied market.

Asia Pacific to Witness the Highest Growth

- The rise in cybercrimes in the region would provide opportunities for Endpoint detection solutions. A cyberattack was reported by Japanese video game giant Capcom. Capcom was confronted with a USD 8.8 million ransom demand in exchange for returning stolen goods, but the business refused to pay. However, it is suspected a Russian cybercriminal group called Ragnar Locker was behind the theft of around 350,000 confidential documents.
- The emphasis on POS terminals by governmental authorities is also pushing the growth of the POS terminals market in the region. For instance, deploying POS terminals in semi-urban and rural areas is central to the Indian government's Digital India initiative. Also, recently, the Reserve Bank of India earmarked USD 80 million to increase the deployment of payment terminals in rural areas, focusing on states in the country's Northeast region. These initiatives will drive the market.
- Security has been a critical consideration at each step of the cloud adoption cycle as IT provision has moved from on-premise to outside of the company's walls. Small and medium enterprises (SMEs) prefer cloud deployment as it allows them to focus on their core competencies rather than invest their capital in security infrastructure since they have limited cybersecurity budgets. Furthermore, deploying public cloud service extends the boundary of trust beyond the organization, making security a vital part of the cloud infrastructure. However, the increasing usage of cloud-based solutions has significantly simplified enterprises' adoption of cybersecurity practices.
- To meet the various demands of the customers and increase market share, endpoint detection firms are developing new solutions. As employees connect to company networks from remote locations via mobile and portable devices, endpoint security will take center stage and become the new perimeter defense.
- For instance, in November this year, Seqrite, a provider of enterprise cybersecurity solutions, unveiled the enhanced version of its flagship offering, Endpoint Security. It's called End Point Security 8.0 (EPS 8.0), and it claims to safeguard connected devices from cyber threats. Seqrite claims that this release has further improved the scale of the system to manage a high number of endpoints for the SME segment. According to the corporation, this will assist clients in reducing their deployment footprint and related maintenance tasks. This version protects Linux in real-time and includes expanded compliance reporting for regulators, auditors, and customers.

Endpoint Detection and Response (EDR) Industry Overview

The endpoint detection and response market is moderately fragmented due to the increasing number of players. For large organizations, storing personal data securely in this fast-paced world has become the most critical task. Giants like Carbon Black, Cisco Systems, and Symantec are developing EDR tools to cater to such organizations.

In October 2022, SyncDog, Inc., the Independent Software Vendor (ISV) for next-generation mobile security and data loss prevention, announced a collaboration with 3Eye Technologies to produce a smarter, more sophisticated product for its mobility and cloud strategy to drive sales objectives. SyncDog's Secure Systems Workspace provides businesses and government organizations with a more secure and scalable solution for addressing all of the challenges of enabling employees on mobile devices-with immediate opportunities to help organizations comply with the federal government's CMMC 2.0 framework and other security and regulatory privacy standards.

In August 2022, Raytheon Intelligence & Space, a Raytheon Technologies division, partnered with CrowdStrike, a cloud-delivered endpoint, cloud workload, identity, and data protection provider, to incorporate its complementary endpoint security technologies into RI&S' managed detection and response (MDR) service. With this collaboration, RI&S' MSSP services will be available to all of RI&S' federal, state, commercial, and non-profit managed services customers in conjunction with the CrowdStrike Falcon platform.

Additional Benefits:

- The market estimate (ME) sheet in Excel format
- 3 months of analyst support

Table of Contents:

Endpoint Detection and Response - Market Share Analysis, Industry Trends & Statistics, Growth Forecasts 2021 - 2029

Market Report | 2024-02-17 | 120 pages | Mordor Intelligence

To place an Order with Scotts International:

□ - Print this form

□ - Complete the relevant blank fields and sign

□ - Send as a scanned email to support@scotts-international.com

ORDER FORM:

Select license	License	Price
	Single User License	$4750.00
	Team License (1-7 Users)	$5250.00
	Site License	$6500.00
	Corporate License	$8750.00
	VAT	
	Total	

*Please circle the relevant license option. For any questions please contact support@scotts-international.com or 0048 603 394 346.

□** VAT will be added at 23% for Polish based companies, individuals and EU based companies who are unable to provide a valid EU Vat Numbers.

Email*

Phone*

First Name*

Last Name*

Job title*

Company Name*

EU Vat / Tax ID / NIP number*

Address*

City*

Zip Code*

Country*

Date 2026-03-04

Signature