

Endpoint Detection And Response (EDR) - Market Share Analysis, Industry Trends & Statistics, Growth Forecasts (2026 - 2031)

Market Report | 2026-01-16 | 161 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:

Endpoint Detection And Response (EDR) Market Analysis

The endpoint detection and response market size in 2026 is estimated at USD 6.33 billion, growing from 2025 value of USD 5.1 billion with 2031 projections showing USD 18.68 billion, growing at 24.15% CAGR over 2026-2031. Growth is propelled by binding U.S. federal mandates that require all civilian agencies to deploy EDR by September 2024 and, from January 2025, to extend coverage to cloud workloads and identity systems. Ransomware-as-a-service commercialization, the pivot to zero-trust security operations centers, and strong demand for unified-agent architectures further accelerate platform adoption. Vendor consolidation, highlighted by Sophos and Palo Alto Networks acquisitions, is reshaping competitive dynamics while managed service channels expand reach into the cost-sensitive SME segment. Technical headwinds such as kernel-level EDR-killer toolkits and AI-driven alert floods temper margins yet have not derailed overall momentum.

Global Endpoint Detection And Response (EDR) Market Trends and Insights

Soaring Federal EDR Mandates (EO 14028)

Executive Order 14028 forced more than 300 U.S. federal agencies to implement full-spectrum EDR by September 2024, then broadened the scope in January 2025 to include cloud workloads and identity telemetry. Contractors to the defense industrial base mirrored these requirements, quadrupling EDR budgets in 2024, while critical-infrastructure operators adopted FedRAMP-authorized solutions to align with new CISA performance goals. State and local governments are now harmonizing with

Scotts International. EU Vat number: PL 6772247784

tel. 0048 603 394 346 e-mail: support@scotts-international.com

www.scotts-international.com

federal benchmarks to secure grant eligibility. Vendors holding government cloud certifications, therefore, enjoy preferential shortlists. As mandates spill into allied nations, the endpoint detection and response market gains an enduring compliance-driven stimulus.

Ransomware-as-a-Service Explosion

Commercialized ransomware kits such as LockBit 3.0 and BlackCat lowered the barrier to entry for cybercriminals, driving 2,323 reported ransomware events in 2024 and lifting average ransom demands to USD 5.3 million. Healthcare bore 389 of those incidents affecting 45 million patient records, causing regulators to tighten HIPAA security-rule interpretations that now favour mandatory EDR. CFOs increasingly view EDR spend as operational-risk insurance because business interruption costs reach 23 times the ransom payout. This economics shift sustains double-digit expansion of the endpoint detection and response market across all verticals.

Credential-Stealing EDR-Killer Toolkits

Open-source frameworks like EDRKillShifter and Terminator exploit kernel hooks to blind or uninstall endpoint agents, achieving up to 90% bypass success in lab evaluations. Availability for as little as USD 500 widens attacker access, forcing vendors into costly tamper-proof engineering sprints and lengthening release cycles. Temporary procurement delays arise when buyers wait for proof that new defenses defeat these toolkits, trimming short-term expansion yet reinforcing long-term innovation in the endpoint detection and response market.

Other drivers and restraints analyzed in the detailed report include:

Shift to Identity-Centred Zero-Trust SOC
Demand for Unified Agent Platform (Cost Down)
Mis-Configured AI Models Causing Alert Flood

For complete list of drivers and restraints, kindly check the Table Of Contents.

Segment Analysis

Endpoint Prevention Platform accounted for 42.62% of 2025 revenue, underscoring enterprise reliance on single-vendor suites that unify antivirus, firewall, and advanced detection. Cloud-native EDR bundled with cloud workload protection is the fastest-growing subsegment at 26.20% CAGR, benefiting from microservice adoption and serverless compute that traditional agents cannot secure. Identity threat detection integration signals the market's evolution toward holistic exposure management, while managed EDR and MDR channels bring enterprise-grade coverage to smaller firms. The endpoint detection and response market size tied to unified agents is projected to multiply as organizations decommission overlapping point solutions in favour of a consolidated stack.

Second-order effects include heightened competition for data-sharing APIs that enable identity, cloud workload, and endpoint telemetry fusion, as well as rising demand for behavioural analytics that operate across these data planes. Vendors able to deliver lightweight agents with cross-domain visibility earn favoured-supplier status in renewal cycles. Conversely, point-product specialists risk commoditization unless they integrate or merge into broader XDR ecosystems. This dynamic is reshaping differentiation criteria inside the endpoint detection and response market.

Cloud-delivered solutions controlled 66.48% of the endpoint detection and response market size in 2025 and will continue expanding at a 25.90% CAGR to 2031 as remote work normalizes decentralized IT. Automatic updates, centralized policy, and elastic threat-intelligence feeds provide compelling advantages for distributed workforces. On-prem and air-gapped deployments

Scotts International. EU Vat number: PL 6772247784

tel. 0048 603 394 346 e-mail: support@scotts-international.com

www.scotts-international.com

persist in defense and regulated finance, driving hybrid offerings that reconcile data-sovereignty mandates with modern detection capabilities.

Enterprises shifting workloads to infrastructure-as-a-service platforms seek parity of protection across endpoints and virtual machines, amplifying demand for SaaS-delivered detection. Consumption-based pricing converts capital outlays into predictable operating expenses, a key benefit for cost controllers. The endpoint detection and response market, therefore, mirrors the broader cloud adoption curve, with specialized on-prem nodes retaining relevance only where regulation explicitly forbids cloud processing.

The Endpoint Detection and Response Market Report is Segmented by Solution Type (Endpoint Prevention Platform, Cloud-Native EDR/CWP-Integrated, and More), Deployment Model (Cloud-Delivered, On-prem/Air-gapped), End-User Vertical (BFSI, Healthcare, and More), Enterprise Size (Small and Medium Enterprises, Large Enterprises), and Geography. The Market Forecasts are Provided in Terms of Value (USD).

Geography Analysis

North America held a 37.02% endpoint detection and response market share in 2025 owing to Executive Order 14028 compliance and sophisticated private-sector threat intelligence sharing. The January 2025 order that added cloud workloads and identity systems effectively doubled the addressable endpoint universe, enhancing vendor revenue outlook. Programs such as CISA's Automated Indicator Sharing feed enrich SOC telemetry, sharpening detection without excessive analyst workload.

Asia-Pacific is projected to log a 26.10% CAGR through 2031 as China, Japan, India, and South Korea roll out nationwide cybersecurity modernization programs. Cloud-first infrastructure deployments, mobile-first workforces, and escalating state-sponsored attack activity pivot organizations toward SaaS-delivered EDR. Domestic compliance statutes such as China's Data Security Law and India's Digital Personal Data Protection Act compel continuous endpoint visibility. Vendors with regional data centers and local threat hunting teams gain competitive traction in this high-growth quadrant of the endpoint detection and response market.

Europe delivers steady expansion under the NIS2 Directive, which broadened mandatory cyber controls across 18 critical sectors in October 2024. GDPR's breach-notification fines further elevate EDR to boardroom priority. Germany and France spearhead adoption via BSI and ANSSI frameworks, while the U.K.'s post-Brexit strategy emphasizes sovereign resilience and multilateral partnerships. Eastern Europe accelerates through EU funding tranches that subsidize detection technology upgrades. These policy-driven dynamics maintain a healthy pipeline for the endpoint detection and response industry despite macroeconomic pressures.

List of Companies Covered in this Report:

CrowdStrike Holdings Inc. Microsoft Corporation (Defender for Endpoint) SentinelOne Inc. VMware by Broadcom (Carbon Black) Trend Micro Inc. Cisco Systems Inc. Palo Alto Networks Inc. (Cortex XDR) Sophos Group plc Bitdefender SRL Check Point Software Technologies Ltd. Kaspersky Lab JSC McAfee LLC Elastic N.V. Cybereason Inc. Trellix (Musarubra US LLC) Fortinet Inc. (FortiEDR) ESET spol. s r.o. WithSecure Plc Red Canary Inc. Huntress Labs Inc.

Additional Benefits:

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

Table of Contents:

Scotts International. EU Vat number: PL 6772247784

tel. 0048 603 394 346 e-mail: support@scotts-international.com

www.scotts-international.com

1 INTRODUCTION

1.1 Study Assumptions and Market Definition

1.2 Scope of the Study

2 RESEARCH METHODOLOGY

3 EXECUTIVE SUMMARY

4 MARKET LANDSCAPE

4.1 Market Overview

4.2 Market Drivers

4.2.1 Soaring Federal EDR Mandates (EO 14028)

4.2.2 Ransomware-as-a-Service Explosion

4.2.3 Shift to Identity-centred Zero-Trust SOC

4.2.4 Demand for Unified Agent Platform (Cost Down)

4.2.5 Surge in Cloud Workload Protection Integration

4.2.6 SMB-led MSP/MDR Channel Pull

4.3 Market Restraints

4.3.1 Credential-stealing EDR-killer Toolkits

4.3.2 Mis-configured AI Models causing Alert Flood

4.3.3 CrowdStrike-style Agent Update Outages

4.3.4 Open-source Agent Forks Driving Price Pressure

4.4 Industrial Value-Chain Analysis

4.5 Regulatory Landscape

4.6 Technological Outlook - Graph-based Correlation, Gen-AI SOC

4.7 Porter's Five Forces Analysis

5 MARKET SIZE AND GROWTH FORECASTS (VALUE)

5.1 By Solution Type

5.1.1 Endpoint Prevention Platform (EPP + EDR)

5.1.2 Cloud-native EDR / CWP-Integrated

5.1.3 Identity-Threat Detection and Response (ITDR)

5.1.4 Managed EDR / MDR

5.2 By Deployment Model

5.2.1 Cloud-Delivered

5.2.2 On-prem / Air-gapped

5.3 By End-User Vertical

5.3.1 BFSI

5.3.2 Healthcare

5.3.3 IT and Telecom

5.3.4 Industrial and Defense

5.3.5 Retail and e-Commerce

5.3.6 Energy and Utilities

5.3.7 Manufacturing

5.3.8 Other End-User Vertical

5.4 By Enterprise Size

5.4.1 Small and Medium Enterprises (SME)

Scotts International. EU Vat number: PL 6772247784

tel. 0048 603 394 346 e-mail: support@scotts-international.com

www.scotts-international.com

- 5.4.2 Large Enterprises
- 5.5 By Geography
 - 5.5.1 North America
 - 5.5.1.1 United States
 - 5.5.1.2 Canada
 - 5.5.1.3 Mexico
 - 5.5.2 Europe
 - 5.5.2.1 United Kingdom
 - 5.5.2.2 Germany
 - 5.5.2.3 France
 - 5.5.2.4 Italy
 - 5.5.2.5 Rest of Europe
 - 5.5.3 Asia-Pacific
 - 5.5.3.1 China
 - 5.5.3.2 Japan
 - 5.5.3.3 India
 - 5.5.3.4 South Korea
 - 5.5.3.5 Rest of Asia-Pacific
 - 5.5.4 Middle East
 - 5.5.4.1 Israel
 - 5.5.4.2 Saudi Arabia
 - 5.5.4.3 United Arab Emirates
 - 5.5.4.4 Turkey
 - 5.5.4.5 Rest of Middle East
 - 5.5.5 Africa
 - 5.5.5.1 South Africa
 - 5.5.5.2 Egypt
 - 5.5.5.3 Rest of Africa
 - 5.5.6 South America
 - 5.5.6.1 Brazil
 - 5.5.6.2 Argentina
 - 5.5.6.3 Rest of South America

6 COMPETITIVE LANDSCAPE

- 6.1 Market Concentration
- 6.2 Strategic Moves
- 6.3 Market Share Analysis
- 6.4 Company Profiles (includes Global level Overview, Market level overview, Core Segments, Financials as available, Strategic Information, Market Rank/Share, Products and Services, Recent Developments)
 - 6.4.1 CrowdStrike Holdings Inc.
 - 6.4.2 Microsoft Corporation (Defender for Endpoint)
 - 6.4.3 SentinelOne Inc.
 - 6.4.4 VMware by Broadcom (Carbon Black)
 - 6.4.5 Trend Micro Inc.
 - 6.4.6 Cisco Systems Inc.
 - 6.4.7 Palo Alto Networks Inc. (Cortex XDR)
 - 6.4.8 Sophos Group plc

Scotts International. EU Vat number: PL 6772247784

tel. 0048 603 394 346 e-mail: support@scotts-international.com

www.scotts-international.com

- 6.4.9 Bitdefender SRL
- 6.4.10 Check Point Software Technologies Ltd.
- 6.4.11 Kaspersky Lab JSC
- 6.4.12 McAfee LLC
- 6.4.13 Elastic N.V.
- 6.4.14 Cybereason Inc.
- 6.4.15 Trellix (Musarubra US LLC)
- 6.4.16 Fortinet Inc. (FortiEDR)
- 6.4.17 ESET spol. s r.o.
- 6.4.18 WithSecure Plc
- 6.4.19 Red Canary Inc.
- 6.4.20 Huntress Labs Inc.

7 MARKET OPPORTUNITIES AND FUTURE OUTLOOK

7.1 White-space and Unmet-Need Assessment

Scotts International. EU Vat number: PL 6772247784

tel. 0048 603 394 346 e-mail: support@scotts-international.com

www.scotts-international.com

Endpoint Detection And Response (EDR) - Market Share Analysis, Industry Trends & Statistics, Growth Forecasts (2026 - 2031)

Market Report | 2026-01-16 | 161 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*	<input type="text"/>	Phone*	<input type="text"/>
First Name*	<input type="text"/>	Last Name*	<input type="text"/>
Job title*	<input type="text"/>		
Company Name*	<input type="text"/>	EU Vat / Tax ID / NIP number*	<input type="text"/>
Address*	<input type="text"/>	City*	<input type="text"/>
Zip Code*	<input type="text"/>	Country*	<input type="text"/>
		Date	<input type="text" value="2026-03-06"/>
		Signature	

Scotts International. EU Vat number: PL 6772247784

tel. 0048 603 394 346 e-mail: support@scotts-international.com

www.scotts-international.com

