

Endpoint Detection and Response (EDR) Market – Global Industry Size, Share, Trends, Opportunity, and Forecast Segmented By Component (Solutions and Services), By Deployment Type (Cloud-based and On-premise), By Solution Type (Workstations, Mobile Devices, Servers, and Point of Sale Terminals), By Organization Size (Small and Medium Enterprises, and Large Enterprises), By End-User Industry (BFSI, IT and Telecom, Manufacturing, Healthcare, Retail, Other), By Region & Competition, 2019-2029F

<https://marketpublishers.com/r/E7DE75098158EN.html>

Date: October 2024

Pages: 185

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

ID: E7DE75098158EN

Abstracts

Global Endpoint Detection and Response (EDR) Market was valued at USD 3.29 Billion in 2023 and is anticipated to project robust growth in the forecast period with a CAGR of 22.98% through 2029. Businesses have effectively shielded their networks against prevalent cybersecurity threats through advanced malware detection. With a significant surge in remote work, scrutiny on endpoint detection and response (EDR) providers intensifies for delivering secure and reliable endpoint software.

EDR tools represent technological platforms facilitating swift investigation and containment of endpoint threats, alerting security teams to potentially perilous activities. These endpoints encompass an array of devices, from workstations and laptops to servers, cloud systems, smartphones, and IoT devices. EDR systems aggregate endpoint data, including process executions, terminal communications, and client logins, analyzing them for anomalies and suspected threats while documenting harmful behaviors. This equips security teams with actionable insights to address concerns,

enabling manual and automated tasks to neutralize threats, such as device wiping, reimaging, or network isolation.

Key Market Drivers

Rising Cybersecurity Threats

The relentless surge in cybersecurity threats represents a powerful and enduring driver behind the remarkable growth of the Global Endpoint Detection and Response (EDR) market. As technology advances, so do the tactics and strategies employed by cybercriminals. Consequently, organizations of all sizes, spanning various sectors, are increasingly turning to EDR solutions as their frontline defense against an evolving threat landscape. Cybersecurity threats have grown in frequency and sophistication, ranging from the proliferation of ransomware attacks, which can paralyze entire organizations, to advanced persistent threats (APTs) that lurk in the shadows for extended periods, aiming to exfiltrate sensitive data or disrupt critical operations. These escalating threats are driving organizations to prioritize endpoint security, recognizing that endpoints, including computers, servers, and mobile devices, are the frontline battlegrounds in the war against cybercrime.

The EDR market's growth is intrinsically linked to the need for timely and effective threat detection and response. EDR solutions offer real-time monitoring capabilities, allowing organizations to swiftly identify anomalous activities, detect malware, and proactively respond to potential security breaches. This capability is critical in minimizing the damage and financial losses that result from cyberattacks.

EDR solutions leverage advanced technologies such as machine learning and artificial intelligence to enhance their threat detection capabilities. These technologies enable EDR tools to identify unusual patterns and behaviors indicative of cyberattacks, even those that have not been previously encountered. By staying ahead of attackers, organizations can take preemptive action, reducing their vulnerability to breaches.

The global shift to remote work models, accelerated by events like the COVID-19 pandemic, has further exacerbated the cybersecurity threat landscape. Remote and distributed workforces introduce new attack vectors, making endpoints even more vulnerable. EDR solutions are instrumental in securing remote devices and providing comprehensive visibility into these environments, ensuring that they remain protected, compliant, and resilient against cyber threats. Ultimately, the rising tide of cybersecurity threats is a significant catalyst for the growth of the EDR market. Organizations

recognize the vital importance of investing in advanced endpoint security to protect sensitive data, maintain regulatory compliance, and safeguard their reputation. As cyber threats continue to evolve, EDR solutions will play an increasingly pivotal role in helping organizations defend against these threats and remain resilient in an ever-changing digital landscape.

Incident Detection and Response

Incident Detection and Response (IDR) plays a pivotal role in driving the growth of the Global Endpoint Detection and Response (EDR) market. In today's complex and ever-evolving cybersecurity landscape, organizations are acutely aware of the urgent need to swiftly and effectively detect and respond to security incidents. As a result, EDR solutions, designed to provide real-time monitoring, threat detection, and rapid response capabilities for endpoints, have become an indispensable component of modern cybersecurity strategies. One of the primary drivers behind the EDR market's expansion is the imperative to reduce the time it takes to identify and mitigate security incidents. Traditional antivirus software is often ill-equipped to handle advanced and persistent threats that target endpoints. EDR solutions, on the other hand, offer advanced capabilities for identifying suspicious or malicious activities, thereby shortening the dwell time of threats within an organization's network.

These solutions leverage a combination of technologies, including machine learning, artificial intelligence, behavior analytics, and threat intelligence integration, to identify anomalies and potential threats. Machine learning and AI enable EDR tools to detect patterns and behaviors indicative of cyberattacks, even those that have never been seen before. This proactive approach enhances an organization's ability to thwart attacks in their early stages, reducing the risk of data breaches and minimizing potential damage. Furthermore, the global adoption of remote and hybrid work models has expanded the attack surface, making endpoints more vulnerable to cyber threats. EDR solutions are essential in securing the myriad devices and endpoints used by a distributed workforce. They provide visibility into the security posture of remote devices, helping organizations ensure that their remote workforce remains protected and compliant with cybersecurity policies. As the EDR market continues to evolve, organizations are investing in these solutions to safeguard their critical data and infrastructure, comply with data protection regulations, and safeguard their reputation. In summary, the imperative to detect and respond to security incidents promptly is a driving force behind the rapid growth of the Global EDR market, and this trend is likely to persist as the threat landscape continues to evolve and pose new challenges to organizations worldwide.

Key Market Challenges

Complexity and False Positives

Complexity and the prevalence of false positives represent significant obstacles that can hamper the growth and effectiveness of the Global Endpoint Detection and Response (EDR) market. While EDR solutions are vital for identifying and mitigating cybersecurity threats, the challenges of dealing with complexity and false alarms can hinder their adoption and operational efficiency. One of the primary issues is the complexity of EDR solutions. These tools are designed to provide comprehensive protection by monitoring and analyzing a multitude of endpoints and generating alerts based on a wide range of potential threats. However, the complexity can result in several challenges.

Alert Overload: EDR solutions can generate a vast number of alerts, many of which may not necessarily indicate an actual threat. The overwhelming volume of alerts can inundate security teams, leading to alert fatigue, where security professionals may ignore or overlook critical alerts amidst the noise.

Skill and Training Requirements: Effectively managing and interpreting EDR alerts requires specialized skills and training. Organizations need security experts who can understand the intricacies of the tool, analyze alerts, and respond appropriately. Acquiring and retaining such talent can be expensive and challenging. **Customization and Configuration:** The complexity of EDR solutions often necessitates customization to align with an organization's specific threat landscape. Configuring these tools correctly can be challenging and time-consuming, requiring expertise and resources.

The prevalence of false positives is another major concern. False positives occur when an EDR solution incorrectly identifies a benign activity as a potential security threat. These false alarms can result from the complex nature of the tool, the dynamic behavior of endpoints, or misconfigurations. Dealing with false positives can lead to several detrimental consequences, **Operational Inefficiency:** Security teams may spend excessive time investigating and responding to false positives, diverting resources away from genuine threats. This inefficiency can delay incident response and weaken the overall security posture.

Loss of Trust: Frequent false positives can erode trust in the EDR solution. Security teams may begin to disregard alerts, potentially missing real threats in the process. To mitigate these challenges, organizations must invest in comprehensive training and

education for their security teams to enhance their proficiency in handling EDR solutions effectively. Additionally, they should focus on fine-tuning and customizing the EDR tools to reduce false positives and align them more closely with their specific environment. EDR vendors can contribute by improving the accuracy of their solutions, reducing false positives through better threat intelligence, and enhancing user-friendly interfaces to streamline alert investigation. By addressing these challenges, the EDR market can offer more accessible, efficient, and reliable solutions to organizations seeking to bolster their endpoint security.

Resource Intensiveness

Resource intensiveness is a significant challenge that can impede the growth of the Global Endpoint Detection and Response (EDR) market. EDR solutions, while crucial for enhancing an organization's cybersecurity posture, require substantial resources in terms of time, personnel, and financial investment. These resource demands can pose barriers to adoption and limit the accessibility of EDR solutions, particularly for smaller organizations and those with limited budgets. **Human Resources:** Implementing and maintaining EDR solutions often requires skilled cybersecurity professionals who can effectively operate and manage these tools. Organizations need staff who can interpret alerts, investigate potential threats, and respond to incidents. The shortage of cybersecurity talent globally exacerbates this resource challenge, making it difficult for many organizations to find and retain qualified personnel.

Training and Skill Development: Even when organizations have the staff in place, they need to invest in ongoing training to keep their security teams up to date with the latest EDR tools and techniques. This can be time-consuming and costly, and the rapid evolution of cyber threats and EDR technology compounds this challenge. **Infrastructure and Hardware:** Deploying EDR solutions can strain an organization's infrastructure and budget. It may require investments in additional hardware and storage capacity to support the collection and analysis of data from endpoints. For smaller organizations, these costs can be prohibitive.

Licensing and Subscription Costs: EDR solutions often come with licensing or subscription fees, which can be costly. These ongoing expenses can become a significant portion of an organization's cybersecurity budget, especially when considering other security tools and services. **Customization and Tuning:** To make EDR solutions effective, organizations must invest time in customizing and fine-tuning the tools to fit their specific needs. This process demands additional resources, as it involves understanding the organization's unique threat landscape and configuring the

EDR solution accordingly.

Scalability: As organizations grow or change, EDR solutions must scale to accommodate an increasing number of endpoints. Scalability challenges can strain both human and financial resources, requiring adjustments in staffing and infrastructure.

The resource intensiveness associated with EDR solutions can be a deterrent for some organizations, particularly small and medium-sized enterprises (SMEs) with limited budgets and resources. As a result, these organizations may opt for less comprehensive security solutions, potentially leaving them more vulnerable to cyber threats. To address this challenge and foster broader EDR adoption, organizations should carefully assess their resource capabilities and cybersecurity needs. Managed EDR services, where organizations outsource their endpoint security to expert providers, can help alleviate some of the resource burdens while still benefiting from robust security. Additionally, governments, industry associations, and EDR vendors can play a role in promoting cost-effective EDR solutions and supporting organizations in overcoming resource challenges to enhance their cybersecurity defenses.

Integration Challenges

Integration challenges represent a significant obstacle in the path of the Global Endpoint Detection and Response (EDR) market. While EDR solutions are essential for organizations to defend against a broad range of cyber threats, their effectiveness hinges on seamless integration with an organization's existing security infrastructure. The complexities of integration can hamper adoption and limit the potential benefits of EDR solutions. One of the primary integration challenges stems from the diverse and often heterogeneous nature of an organization's security stack. EDR solutions must interoperate with various security tools, including firewalls, intrusion detection systems, SIEMs (Security Information and Event Management), and other endpoint security technologies. Achieving this harmonious integration can be complex, as each tool may have its own data format, protocols, and APIs.

Interoperability issues can result in operational inefficiencies. For instance, a lack of integration may lead to the duplication of efforts, such as manual data entry or the need for security analysts to switch between multiple platforms to investigate and respond to threats. This can slow down incident response times and increase the risk of overlooking critical security events. Furthermore, EDR integration challenges can hinder real-time threat detection and response. EDR solutions rely on the exchange of data and alerts with other security systems. If integration is not seamless, delays in data

sharing can occur, potentially allowing threats to go unnoticed or unmitigated for extended periods.

The EDR market's growth can be stifled by the expense and complexity associated with integration. Organizations may need to invest in specialized personnel and expertise to manage integration effectively. This incurs additional costs and can be particularly challenging for smaller businesses with limited resources. Moreover, the fast-paced evolution of the threat landscape and the emergence of new security technologies further complicate integration. EDR solutions must adapt to support emerging threat detection methods, threat intelligence feeds, and the integration of cloud-based security services.

To overcome these challenges and ensure the successful implementation of EDR solutions, organizations must invest time and resources in planning and executing integration effectively. They should also prioritize open standards and flexible APIs, ensuring that EDR solutions can work with a wide range of existing security tools. The industry must collectively address integration issues through improved vendor collaboration and standardized approaches to data sharing, ultimately paving the way for more robust and streamlined EDR solutions that can better protect organizations against the ever-evolving threat landscape.

Key Market Trends

Rapid Market Growth

The Global Endpoint Detection and Response (EDR) market is currently experiencing rapid growth, driven by an array of factors that underscore the critical importance of EDR solutions in modern cybersecurity strategies. This remarkable expansion is a testament to the escalating cyber threat landscape and the necessity for robust endpoint security.

One of the primary drivers of this growth is the relentless evolution and proliferation of cyber threats. Sophisticated malware, ransomware, and advanced persistent threats (APTs) continue to pose severe risks to organizations. As a result, EDR solutions have emerged as indispensable tools for threat detection, response, and mitigation, thus significantly boosting their adoption. The global shift towards remote and hybrid work models, accelerated by the COVID-19 pandemic, has further amplified the demand for EDR solutions. With a larger attack surface due to remote endpoints, organizations are increasingly recognizing the need for robust endpoint security to protect sensitive data,

secure remote devices, and ensure compliance.

The competitive landscape within the EDR market is fostering innovation, with numerous vendors continuously enhancing and expanding their EDR offerings. This competition results in more advanced, feature-rich solutions, making EDR an attractive choice for organizations. As organizations strive to reduce response times, improve threat detection, and maintain regulatory compliance, the EDR market's rapid growth is set to continue. It is evident that the ever-changing threat landscape and the increasing awareness of endpoint security are propelling the global EDR market to new heights, making it an indispensable component of contemporary cybersecurity strategies.

AI and Machine Learning Integration

The integration of Artificial Intelligence (AI) and Machine Learning (ML) technologies is poised to be a driving force behind the continued growth and effectiveness of the Global Endpoint Detection and Response (EDR) market. As the cybersecurity threat landscape becomes increasingly complex and dynamic, EDR solutions equipped with AI and ML capabilities are better positioned to identify and respond to evolving threats. AI and ML enable EDR solutions to analyze vast datasets generated by endpoint activities in real-time. They can discern patterns and anomalies, helping to differentiate between legitimate user actions and potential security threats. Moreover, AI-driven EDR solutions excel in recognizing previously unseen or zero-day threats, enhancing organizations' ability to preemptively respond to emerging dangers.

These technologies significantly reduce false positives, allowing security teams to focus their attention on genuine threats, thus enhancing overall operational efficiency. Furthermore, AI and ML can automate response actions, swiftly containing or mitigating security incidents and minimizing potential damage. As the threat landscape continues to evolve and adversaries become more sophisticated, the integration of AI and ML into EDR solutions will play a pivotal role in bolstering endpoint security. Organizations will increasingly turn to these advanced EDR solutions to effectively protect their endpoints, respond to threats in real-time, and maintain a robust cybersecurity posture in an ever-changing digital environment.

Segmental Insights

Component Insights

Solution segment dominated the Global Endpoint Detection and Response (EDR)

market in 2023, driven by several key factors that emphasize the critical role of EDR solutions in modern cybersecurity strategies. EDR solutions encompass a range of software and tools designed to detect, investigate, and mitigate cyber threats targeting endpoints such as desktops, laptops, servers, and mobile devices.

One of the primary drivers of the dominance of the solution segment is the evolving threat landscape and the increasing sophistication of cyberattacks targeting endpoints. With cyber threats becoming more complex and persistent, organizations are turning to EDR solutions to bolster their defenses and improve their ability to detect and respond to advanced threats. EDR solutions leverage advanced analytics, machine learning, and behavioral analysis techniques to identify suspicious activities and indicators of compromise (IOCs) on endpoints, enabling organizations to proactively defend against emerging threats. The regulatory landscape and compliance requirements are driving the adoption of EDR solutions across industries. Regulations such as the General Data Protection Regulation (GDPR), the Health Insurance Portability and Accountability Act (HIPAA), and the Payment Card Industry Data Security Standard (PCI DSS) mandate the implementation of robust security measures to protect sensitive data and ensure regulatory compliance. EDR solutions provide organizations with the necessary capabilities to monitor and protect endpoints, detect security incidents, and facilitate incident response activities, thereby helping organizations meet regulatory obligations and avoid potential penalties and reputational damage.

The increasing adoption of remote work and mobile devices further amplifies the importance of EDR solutions in securing endpoints. The proliferation of remote workforces and the use of personal devices for work purposes introduce new security challenges and vulnerabilities, making endpoint security a top priority for organizations. EDR solutions offer visibility and control over endpoints regardless of their location, allowing organizations to extend their security perimeter and protect against threats targeting remote devices.

Integration of EDR solutions with broader cybersecurity platforms and ecosystems enhances their effectiveness and value proposition. By integrating EDR with other security technologies such as endpoint protection platforms (EPP), security information and event management (SIEM) systems, and threat intelligence platforms, organizations can achieve comprehensive threat detection and response capabilities across their entire IT environment. This integration enables organizations to correlate and analyze security data from multiple sources, automate response actions, and orchestrate incident response workflows, resulting in improved threat detection and faster incident response times.

The solution segment is expected to dominate the EDR market during the forecast period, driven by the increasing complexity of cyber threats, regulatory compliance requirements, the rise of remote workforces, and the integration with broader cybersecurity platforms. As organizations prioritize endpoint security and threat detection capabilities, EDR solutions emerge as essential components of comprehensive cybersecurity strategies, enabling organizations to detect and respond to advanced threats targeting their endpoints effectively.

Regional Insights

Asia Pacific dominated the market in 2023, reflecting a significant surge in demand for advanced cybersecurity solutions. This growth can be attributed to the increasing frequency and sophistication of cyber threats, prompting organizations to adopt proactive measures to safeguard their digital assets. Companies across various sectors are recognizing the critical need for robust endpoint security, leading to a heightened investment in EDR technologies. The rise of remote work and digital transformation initiatives has further amplified the need for EDR solutions. As organizations expand their digital footprints, they face new vulnerabilities, making endpoint protection essential. The ability of EDR systems to monitor, detect, and respond to threats in real-time has become a key factor for businesses looking to mitigate risks associated with remote operations.

Governments in the Asia Pacific region are also playing a pivotal role in driving EDR adoption. Regulatory frameworks aimed at enhancing cybersecurity resilience have prompted companies to invest in comprehensive security solutions. This regulatory push not only ensures compliance but also fosters a culture of cybersecurity awareness among businesses and their stakeholders. The competitive landscape of the EDR market in Asia Pacific is characterized by a mix of established players and emerging startups. Major cybersecurity vendors are continuously innovating their offerings, integrating advanced technologies such as artificial intelligence and machine learning to enhance threat detection capabilities. This innovation race is crucial for maintaining market leadership and meeting the evolving demands of customers.

The growing awareness of data privacy and protection is propelling organizations to adopt EDR solutions. With increasing public scrutiny over data breaches and compliance with regulations like GDPR, businesses are prioritizing endpoint security. EDR systems provide an added layer of security, ensuring that sensitive data remains protected from unauthorized access and potential breaches. Investment in cybersecurity

education and training programs is also contributing to the growth of the EDR market. As organizations seek to build more resilient security postures, they recognize the importance of equipping their workforce with the necessary skills to effectively utilize EDR technologies. This focus on human capital complements technological advancements, creating a holistic approach to cybersecurity.

The diverse industrial landscape of the Asia Pacific region also supports the expansion of the EDR market. Sectors such as finance, healthcare, and manufacturing are increasingly adopting endpoint security solutions to protect critical infrastructure and sensitive information. The tailored applications of EDR technologies across various industries underscore their versatility and relevance in today's digital economy. The collaboration between government agencies and private sector organizations is fostering an environment conducive to EDR adoption. Initiatives aimed at sharing threat intelligence and best practices enhance the overall cybersecurity posture of the region, further driving interest in advanced security solutions. Such partnerships are vital in building a collective defense against cyber threats.

As the EDR market in Asia Pacific continues to grow, investment in research and development is expected to remain a priority. Companies are likely to focus on developing innovative features that address emerging threats and enhance user experience. This commitment to R&D will be crucial in maintaining competitive advantage in an increasingly crowded marketplace. The dominance of the Asia Pacific region in the EDR market in 2023 is a reflection of the convergence of technological advancements, regulatory initiatives, and a heightened awareness of cybersecurity risks. As businesses and governments continue to prioritize cybersecurity, the demand for sophisticated endpoint detection and response solutions is poised for sustained growth in the coming years.

Key Market Players

Cisco Systems Inc.

CrowdStrike, Inc.

Broadcom Inc.

Cybereason Inc.

Deep Instinct Ltd.

Fortra, LLC

FireEye, Inc.

OpenText Corporation

McAfee, LLC

Report Scope:

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

Endpoint Detection and Response (EDR) Market, By Component:

Solutions

Services

Endpoint Detection and Response (EDR) Market, By Deployment Type:

Cloud-based

On-premise

Endpoint Detection and Response (EDR) Market, By Solution Type:

Workstations

Mobile Devices

Servers

Point of Sale Terminals

Endpoint Detection and Response (EDR) Market, By Organization Size:

Small and Medium Enterprises

Large Enterprises

Endpoint Detection and Response (EDR) Market, By End-User Industry:

BFSI

IT and Telecom

Manufacturing

Healthcare

Retail

Other

Endpoint Detection and Response (EDR) Market, By Region:

North America

United States

Canada

Mexico

Asia-Pacific

China

India

Japan

South Korea

Indonesia

Europe

Germany

United Kingdom

France

Russia

Spain

South America

Brazil

Argentina

Middle East & Africa

Saudi Arabia

South Africa

Egypt

UAE

Israel

Competitive Landscape

Company Profiles: Detailed analysis of the major companies presents in the Global Endpoint Detection and Response (EDR) Market.

Available Customizations:

Endpoint Detection and Response (EDR) Market – Global Industry Size, Share, Trends, Opportunity, and Forecast...

Global Endpoint Detection and Response (EDR) 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:

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
- 1.3. Markets Covered
- 1.4. Years Considered for Study
- 1.5. 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

4. VOICE OF CUSTOMERS

5. GLOBAL ENDPOINT DETECTION AND RESPONSE (EDR) MARKET OUTLOOK

- 5.1. Market Size & Forecast
 - 5.1.1. By Value
- 5.2. Market Share & Forecast
 - 5.2.1. By Component (Solutions and Services)
 - 5.2.2. By Deployment Type (Cloud-based and On-premise)
 - 5.2.3. By Solution Type (Workstations, Mobile Devices, Servers, and Point of Sale Terminals)
 - 5.2.4. By Organization Size (Small and Medium Enterprises, and Large Enterprises)
 - 5.2.5. By End-User Industry (BFSI, IT and Telecom, Manufacturing, Healthcare, Retail, Other)
 - 5.2.6. By Region
- 5.3. By Company (2023)
- 5.4. Market Map

6. NORTH AMERICA ENDPOINT DETECTION AND RESPONSE (EDR) 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 Type

6.2.3. By Solution Type

6.2.4. By Organization Size

6.2.5. By End-User Industry

6.2.6. By Country

6.3. North America: Country Analysis

6.3.1. United States Endpoint Detection and Response (EDR) 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 Type

6.3.1.2.3. By Solution Type

6.3.1.2.4. By Organization Size

6.3.1.2.5. By End-User Industry

6.3.2. Canada Endpoint Detection and Response (EDR) 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 Type

6.3.2.2.3. By Solution Type

6.3.2.2.4. By Organization Size

6.3.2.2.5. By End-User Industry

6.3.3. Mexico Endpoint Detection and Response (EDR) 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 Type

6.3.3.2.3. By Solution Type

6.3.3.2.4. By Organization Size

6.3.3.2.5. By End-User Industry

7. ASIA-PACIFIC ENDPOINT DETECTION AND RESPONSE (EDR) 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 Type

7.2.3. By Solution Type

7.2.4. By Organization Size

7.2.5. By End-User Industry

7.2.6. By Country

7.3. Asia-Pacific: Country Analysis

7.3.1. China Endpoint Detection and Response (EDR) 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 Type

7.3.1.2.3. By Solution Type

7.3.1.2.4. By Organization Size

7.3.1.2.5. By End-User Industry

7.3.2. India Endpoint Detection and Response (EDR) 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 Type

7.3.2.2.3. By Solution Type

7.3.2.2.4. By Organization Size

7.3.2.2.5. By End-User Industry

7.3.3. Japan Endpoint Detection and Response (EDR) 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 Type
- 7.3.3.2.3. By Solution Type
- 7.3.3.2.4. By Organization Size
- 7.3.3.2.5. By End-User Industry
- 7.3.4. South Korea Endpoint Detection and Response (EDR) 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 Type
 - 7.3.4.2.3. By Solution Type
 - 7.3.4.2.4. By Organization Size
 - 7.3.4.2.5. By End-User Industry
- 7.3.5. Indonesia Endpoint Detection and Response (EDR) 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 Type
 - 7.3.5.2.3. By Solution Type
 - 7.3.5.2.4. By Organization Size
 - 7.3.5.2.5. By End-User Industry

8. EUROPE ENDPOINT DETECTION AND RESPONSE (EDR) 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 Type
 - 8.2.3. By Solution Type
 - 8.2.4. By Organization Size
 - 8.2.5. By End-User Industry
 - 8.2.6. By Country
- 8.3. Europe: Country Analysis
 - 8.3.1. Germany Endpoint Detection and Response (EDR) 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 Type
- 8.3.1.2.3. By Solution Type
- 8.3.1.2.4. By Organization Size
- 8.3.1.2.5. By End-User Industry
- 8.3.2. United Kingdom Endpoint Detection and Response (EDR) 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 Type
 - 8.3.2.2.3. By Solution Type
 - 8.3.2.2.4. By Organization Size
 - 8.3.2.2.5. By End-User Industry
- 8.3.3. France Endpoint Detection and Response (EDR) 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 Type
 - 8.3.3.2.3. By Solution Type
 - 8.3.3.2.4. By Organization Size
 - 8.3.3.2.5. By End-User Industry
- 8.3.4. Russia Endpoint Detection and Response (EDR) 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 Type
 - 8.3.4.2.3. By Solution Type
 - 8.3.4.2.4. By Organization Size
 - 8.3.4.2.5. By End-User Industry
- 8.3.5. Spain Endpoint Detection and Response (EDR) 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 Type
 - 8.3.5.2.3. By Solution Type

8.3.5.2.4. By Organization Size

8.3.5.2.5. By End-User Industry

9. SOUTH AMERICA ENDPOINT DETECTION AND RESPONSE (EDR) 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 Type

9.2.3. By Solution Type

9.2.4. By Organization Size

9.2.5. By End-User Industry

9.2.6. By Country

9.3. South America: Country Analysis

9.3.1. Brazil Endpoint Detection and Response (EDR) 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 Type

9.3.1.2.3. By Solution Type

9.3.1.2.4. By Organization Size

9.3.1.2.5. By End-User Industry

9.3.2. Argentina Endpoint Detection and Response (EDR) 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 Type

9.3.2.2.3. By Solution Type

9.3.2.2.4. By Organization Size

9.3.2.2.5. By End-User Industry

10. MIDDLE EAST & AFRICA ENDPOINT DETECTION AND RESPONSE (EDR) 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 Type
 - 10.2.3. By Solution Type
 - 10.2.4. By Organization Size
 - 10.2.5. By End-User Industry
 - 10.2.6. By Country
- 10.3. Middle East & Africa: Country Analysis
 - 10.3.1. Saudi Arabia Endpoint Detection and Response (EDR) 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 Type
 - 10.3.1.2.3. By Solution Type
 - 10.3.1.2.4. By Organization Size
 - 10.3.1.2.5. By End-User Industry
 - 10.3.2. South Africa Endpoint Detection and Response (EDR) 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 Type
 - 10.3.2.2.3. By Solution Type
 - 10.3.2.2.4. By Organization Size
 - 10.3.2.2.5. By End-User Industry
 - 10.3.3. UAE Endpoint Detection and Response (EDR) 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 Type
 - 10.3.3.2.3. By Solution Type
 - 10.3.3.2.4. By Organization Size
 - 10.3.3.2.5. By End-User Industry
 - 10.3.4. Israel Endpoint Detection and Response (EDR) Market Outlook
 - 10.3.4.1. Market Size & Forecast
 - 10.3.4.1.1. By Value

10.3.4.2. Market Share & Forecast

10.3.4.2.1. By Component

10.3.4.2.2. By Deployment Type

10.3.4.2.3. By Solution Type

10.3.4.2.4. By Organization Size

10.3.4.2.5. By End-User Industry

10.3.5. Egypt Endpoint Detection and Response (EDR) Market Outlook

10.3.5.1. Market Size & Forecast

10.3.5.1.1. By Value

10.3.5.2. Market Share & Forecast

10.3.5.2.1. By Component

10.3.5.2.2. By Deployment Type

10.3.5.2.3. By Solution Type

10.3.5.2.4. By Organization Size

10.3.5.2.5. By End-User Industry

11. MARKET DYNAMICS

11.1. Drivers

11.2. Challenge

12. MARKET TRENDS & DEVELOPMENTS

13. COMPANY PROFILES

13.1. Cisco Systems Inc.

13.1.1. Business Overview

13.1.2. Key Revenue and Financials

13.1.3. Recent Developments

13.1.4. Key Personnel

13.1.5. Key Product/Services

13.2. CrowdStrike, Inc.

13.2.1. Business Overview

13.2.2. Key Revenue and Financials

13.2.3. Recent Developments

13.2.4. Key Personnel

13.2.5. Key Product/Services

13.3. Broadcom Inc.

13.3.1. Business Overview

- 13.3.2. Key Revenue and Financials
- 13.3.3. Recent Developments
- 13.3.4. Key Personnel
- 13.3.5. Key Product/Services
- 13.4. Cybereason Inc.
 - 13.4.1. Business Overview
 - 13.4.2. Key Revenue and Financials
 - 13.4.3. Recent Developments
 - 13.4.4. Key Personnel
 - 13.4.5. Key Product/Services
- 13.5. Deep Instinct Ltd.
 - 13.5.1. Business Overview
 - 13.5.2. Key Revenue and Financials
 - 13.5.3. Recent Developments
 - 13.5.4. Key Personnel
 - 13.5.5. Key Product/Services
- 13.6. Fortra, LLC
 - 13.6.1. Business Overview
 - 13.6.2. Key Revenue and Financials
 - 13.6.3. Recent Developments
 - 13.6.4. Key Personnel
 - 13.6.5. Key Product/Services
- 13.7. FireEye, Inc.
 - 13.7.1. Business Overview
 - 13.7.2. Key Revenue and Financials
 - 13.7.3. Recent Developments
 - 13.7.4. Key Personnel
 - 13.7.5. Key Product/Services
- 13.8. OpenText Corporation
 - 13.8.1. Business Overview
 - 13.8.2. Key Revenue and Financials
 - 13.8.3. Recent Developments
 - 13.8.4. Key Personnel
 - 13.8.5. Key Product/Services
- 13.9. McAfee, LLC
 - 13.9.1. Business Overview
 - 13.9.2. Key Revenue and Financials
 - 13.9.3. Recent Developments
 - 13.9.4. Key Personnel

13.9.5. Key Product/Services

14. STRATEGIC RECOMMENDATIONS

15. ABOUT US & DISCLAIMER

I would like to order

Product name: Endpoint Detection and Response (EDR) Market – Global Industry Size, Share, Trends, Opportunity, and Forecast Segmented By Component (Solutions and Services), By Deployment Type (Cloud-based and On-premise), By Solution Type (Workstations, Mobile Devices, Servers, and Point of Sale Terminals), By Organization Size (Small and Medium Enterprises, and Large Enterprises), By End-User Industry (BFSI, IT and Telecom, Manufacturing, Healthcare, Retail, Other), By Region & Competition, 2019-2029F

Product link: <https://marketpublishers.com/r/E7DE75098158EN.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/E7DE75098158EN.html>

To pay by Wire Transfer, please, fill in your contact details in the form below:

First name:
Last name:
Email:
Company:
Address:
City:
Zip code:
Country:
Tel:
Fax:
Your message:

****All fields are required**

Customer signature _____

Please, note that by ordering from marketpublishers.com you are agreeing to our Terms & Conditions at <https://marketpublishers.com/docs/terms.html>

To place an order via fax simply print this form, fill in the information below and fax the completed form to +44 20 7900 3970