+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, By Competition Forecast & Opportunities, 2018-2028

https://marketpublishers.com/r/ECC522578B59EN.html
Date: October 2023
Pages: 172
Price: US$ 4,500.00 (Single User License)
ID: ECC522578B59EN

Abstracts

The Global Extended Detection and Response Market was valued at USD 1.82 Billion in 2022 and is growing at a CAGR of 22.56% during the forecast period. The Global Extended Detection and Response (XDR) Market is experiencing remarkable growth and transformation, driven by the relentless evolution of cyber threats and the increasing complexity of modern digital environments. XDR represents a pivotal shift in the cybersecurity landscape, offering organizations a comprehensive and proactive approach to threat detection, response, and containment. As businesses worldwide grapple with the escalating sophistication of cyberattacks, the demand for XDR solutions is rapidly expanding, shaping a dynamic and highly competitive market with promising prospects. One of the primary catalysts behind the growth of the XDR market is the sheer volume and complexity of cyber threats facing organizations today. Traditional security solutions are often siloed and struggle to keep pace with the ever-evolving threat landscape. XDR addresses this challenge by integrating data from multiple security tools, including endpoint detection and response (EDR), network detection and response (NDR), and cloud security, into a unified platform. This integrated approach enables organizations to correlate and analyze data across their

+357 96 030922
info@marketpublishers.com

entire digital ecosystem, providing a holistic view of potential threats. The rise of remote work and cloud adoption has further accelerated the demand for XDR solutions. With employees accessing corporate networks from various locations and devices, the attack surface has expanded, making it imperative for organizations to have real-time threat visibility and response capabilities. XDR's ability to monitor and protect endpoints, networks, and cloud environments makes it well-suited for modern, distributed work environments. Moreover, compliance and regulatory requirements are compelling organizations to invest in robust cybersecurity solutions like XDR. Regulations such as GDPR, HIPAA, and CCPA mandate stringent data protection measures and reporting. XDR not only helps detect and respond to security incidents but also provides valuable audit trails and reporting capabilities, simplifying compliance efforts. The continuous innovation and integration of artificial intelligence (AI) and machine learning (ML) technologies within XDR solutions have significantly enhanced their effectiveness. These technologies enable XDR platforms to detect anomalies, identify advanced threats, and automate response actions with greater accuracy and speed. As threats become more sophisticated, AI and ML are crucial in staying one step ahead of cybercriminals. The XDR market is characterized by intense competition, with established cybersecurity vendors and startups vying for market share. Vendors are investing heavily in research and development to deliver advanced XDR solutions that can adapt to evolving threats. Additionally, partnerships and acquisitions are common strategies to broaden the capabilities of XDR platforms and offer customers a more comprehensive security stack. In conclusion, the Global Extended Detection and Response (XDR) Market are thriving due to the escalating cyber threat landscape, the adoption of remote work and cloud technologies, regulatory compliance demands, and the integration of AI and ML technologies. XDR's holistic, integrated approach to cybersecurity is well-aligned with the needs of modern organizations seeking proactive threat detection and response. As businesses worldwide recognize the critical importance of robust cybersecurity measures, the XDR market is poised for continued growth and innovation.

Key Market Drivers

Escalating Cyber Threat Landscape

The continually escalating cyber threat landscape stands as a primary driving factor behind the rapid growth of the Global Extended Detection and Response (XDR) market. In an increasingly digital and interconnected world, the scope and sophistication of cyberattacks have reached unprecedented levels. Cybercriminals employ an array of tactics, from malware and ransomware to phishing and zero-day exploits, to target

+357 96 030922
info@marketpublishers.com

organizations of all sizes and sectors. As a result, the demand for robust and comprehensive cybersecurity solutions like XDR has never been higher.

Sophistication of Threats: Cyber threats are evolving at an alarming rate. Attackers are becoming more adept at evading traditional security measures, making it imperative for organizations to adopt advanced solutions like XDR. Sophisticated threats often employ multi-vector techniques, targeting endpoints, networks, and cloud environments simultaneously. XDR's ability to monitor and correlate data across these various attack vectors provides organizations with a holistic view of the threat landscape.

Zero-Day Vulnerabilities: Zero-day vulnerabilities are security flaws unknown to the vendor or security community, making them extremely difficult to defend against. XDR solutions equipped with advanced threat detection capabilities, including anomaly detection and behavior analytics, are crucial in identifying and mitigating zero-day threats before they cause damage.

Ransomware Attacks: Ransomware attacks, where cybercriminals encrypt an organization's data and demand a ransom for its release, have surged in recent years. XDR's real-time monitoring and rapid incident response capabilities help organizations detect and contain ransomware attacks before data is encrypted, preventing costly data breaches.

Digital Transformation and Cloud Adoption:

Digital Transformation and Cloud Adoption are two pivotal factors propelling the global Extended Detection and Response (XDR) market into a new era of cybersecurity. In an increasingly interconnected and digitalized world, organizations are grappling with a growing array of cyber threats and vulnerabilities. To effectively combat these challenges, they are turning to XDR solutions that provide comprehensive and proactive threat detection and response capabilities. This paradigm shift is being catalyzed by the twin forces of Digital Transformation and Cloud Adoption.

Digital Transformation represents the fundamental reimagining of business processes, products, and services through the integration of digital technologies. As organizations strive to remain competitive and relevant in today's fast-paced landscape, they are embracing technologies such as IoT, AI, machine learning, and big data analytics. While these innovations bring immense benefits, they also expand the attack surface for cybercriminals. Digital Transformation initiatives necessitate a proactive cybersecurity posture, which is precisely what XDR offers.

+357 96 030922
info@marketpublishers.com

XDR, as a holistic security approach, goes beyond traditional endpoint detection and response (EDR) and encompasses network, email, and cloud security, offering a unified view of an organization's entire digital environment. With Digital Transformation, companies are increasingly reliant on cloud infrastructure and applications to enhance agility and scalability. Cloud Adoption is not only revolutionizing IT infrastructure but also challenging conventional security models. As data and workloads migrate to the cloud, organizations require security solutions that can seamlessly adapt to this new paradigm. XDR fits the bill by providing cloud-native capabilities, ensuring that organizations can maintain a consistent security posture across on-premises and cloud environments. Furthermore, Digital Transformation is ushering in a new era of remote and hybrid work models. Employees are accessing corporate resources from a multitude of devices and locations, making the traditional network perimeter obsolete. This distributed workforce requires robust security measures that can identify threats across various entry points. XDR, with its ability to correlate data from multiple sources and detect anomalies and suspicious activities, is perfectly suited to protect these expanded attack surfaces. In the context of Digital Transformation, data has emerged as the lifeblood of modern organizations. The proliferation of data generates a wealth of information that cybercriminals seek to exploit. XDR leverages advanced analytics and machine learning to process and analyze this data in real-time, identifying potential threats and vulnerabilities before they escalate into full-blown security incidents. Moreover, XDR's automated response capabilities are indispensable in the Digital Transformation era, as they allow organizations to respond rapidly to threats and minimize potential damage. As organizations increasingly adopt cloud services and migrate sensitive data to cloud environments, the need for robust cloud security becomes paramount. XDR seamlessly integrates with cloud platforms, offering end-to-end visibility and control over cloud-based assets. This ensures that organizations can harness the benefits of the cloud while mitigating security risks associated with data exposure and breaches.

In conclusion, the convergence of Digital Transformation and Cloud Adoption is revolutionizing the cybersecurity landscape. Extended Detection and Response (XDR) solutions have emerged as a critical enabler of this transformation, providing organizations with the capabilities needed to defend against evolving cyber threats in an era of digital innovation. XDR's holistic approach, cloud-native capabilities, and adaptability make it the go-to choice for organizations looking to secure their digital assets and navigate the complex cybersecurity challenges of today's interconnected world. As Digital Transformation and Cloud Adoption continue to reshape business models and IT infrastructure, XDR will remain at the forefront of the cybersecurity

+357 96 030922
info@marketpublishers.com

arsenal, safeguarding organizations and enabling them to thrive in the digital age.

Regulatory Compliance and Data Privacy:

Regulatory Compliance and Data Privacy concerns have emerged as compelling catalysts propelling the global Extended Detection and Response (XDR) market to new heights. In an era marked by increasingly stringent data protection regulations and a growing awareness of the importance of safeguarding sensitive information, organizations are turning to XDR solutions to not only fortify their cybersecurity defenses but also ensure they remain in compliance with legal mandates and industry standards.

The global landscape of regulatory compliance has undergone a seismic shift in recent years, with frameworks like the European Union's General Data Protection Regulation (GDPR) and the California Consumer Privacy Act (CCPA) setting the stage for a worldwide focus on data privacy and security. These regulations impose strict requirements on organizations, mandating the protection of personal data and the prompt disclosure of data breaches. Non-compliance can result in substantial fines and reputational damage. Consequently, organizations are seeking comprehensive security solutions like XDR to not only detect and respond to threats but also to maintain adherence to these regulations.

XDR's appeal in the realm of regulatory compliance lies in its ability to offer a holistic view of an organization's security posture. It amalgamates data from multiple sources, including endpoints, networks, and cloud environments, providing a centralized platform for monitoring and investigating potential security incidents. This capability proves invaluable when organizations need to demonstrate compliance by quickly identifying and reporting data breaches, as XDR can provide the necessary forensic evidence to pinpoint the source and scope of the breach.

Moreover, the proactive threat detection and response capabilities of XDR are instrumental in complying with regulations that require organizations to have robust security measures in place. By identifying and mitigating threats in real-time, XDR helps organizations preemptively thwart potential breaches, a critical aspect of regulatory compliance. Furthermore, the automated incident response features of XDR enable organizations to take swift and appropriate action when a security incident occurs, which is often a stipulation of data protection regulations.

Data privacy is also a pivotal driver for the adoption of XDR. Organizations are

+357 96 030922
info@marketpublishers.com

increasingly aware of the reputational and financial risks associated with data breaches and the mishandling of sensitive information. The exposure of personal data not only harms customer trust but can also lead to legal liabilities. XDR's capabilities in continuously monitoring an organization's digital environment, identifying suspicious activities, and facilitating rapid incident response provide a robust defense against data breaches. Its ability to uncover and mitigate insider threats, a common vector for data leaks, further reinforces data privacy efforts.

Furthermore, as data breaches become more sophisticated and widespread, organizations must go beyond traditional security measures to protect sensitive information. XDR's advanced analytics, machine learning, and behavioral analysis capabilities empower organizations to detect emerging threats and anomalies that may indicate data breaches in their early stages, preventing them from escalating into major incidents.

In conclusion, Regulatory Compliance and Data Privacy concerns have become twin engines propelling the adoption of Extended Detection and Response (XDR) solutions. In an era of stringent data protection regulations and heightened awareness of the importance of safeguarding sensitive information, organizations recognize that XDR not only enhances their cybersecurity posture but also helps them navigate the complex landscape of regulatory compliance. By offering real-time threat detection, centralized monitoring, automated incident response, and robust data protection capabilities, XDR emerges as an indispensable tool for organizations striving to meet the demands of an evolving regulatory landscape and safeguard the privacy of their customers' data. As regulatory frameworks continue to evolve and data privacy remains a paramount concern, XDR's role in securing organizations and preserving their reputation will continue to grow in significance.

Key Market Challenges

Integration and Interoperability Complexities:

The Global Extended Detection and Response (XDR) market has witnessed remarkable growth in recent years, driven by the increasing need for advanced cybersecurity solutions to combat ever-evolving cyber threats. However, one of the significant challenges faced by organizations in this market is the complexity associated with integration and interoperability. Integration complexities arise from the diverse and often fragmented landscape of cybersecurity tools and solutions. Organizations typically employ a range of security products, each serving a specific purpose, such as endpoint

+357 96 030922
info@marketpublishers.com

protection, network security, and threat intelligence. These tools often come from different vendors and may not inherently work seamlessly together. When implementing an XDR solution, organizations must integrate these disparate systems, which can be a daunting task. Ensuring that data flows smoothly between these tools, while also maintaining compatibility and avoiding conflicts, is a significant challenge. Interoperability complexities exacerbate the integration challenge. XDR solutions aim to provide holistic threat detection and response capabilities by aggregating data from various sources, including endpoints, networks, and cloud environments. Achieving interoperability among these diverse data sources requires standardized protocols, data formats, and a deep understanding of the intricacies of each system. Compatibility issues can lead to data inconsistencies, delays in threat detection, and hindered incident response, ultimately weakening the effectiveness of the XDR solution. Furthermore, ensuring the interoperability and integration of XDR with existing security infrastructure, such as Security Information and Event Management (SIEM) systems, adds another layer of complexity. Organizations must bridge the gap between legacy tools and modern XDR solutions, often requiring custom development and ongoing maintenance. In conclusion, while Extended Detection and Response (XDR) solutions offer promising capabilities for enhancing cybersecurity posture, they also introduce significant integration and interoperability complexities. Organizations must invest in skilled personnel and resources to navigate these challenges successfully. The ability to seamlessly integrate and interoperate with existing and future security technologies will be a crucial factor in maximizing the benefits of XDR and staying ahead of the evolving threat landscape in the global cybersecurity market.

Cybersecurity Skills Gap

The Global Extended Detection and Response (XDR) market has emerged as a critical player in the ongoing battle against cyber threats, offering comprehensive solutions for threat detection and response. However, a formidable challenge faced by this market is the persistent cybersecurity skills gap. The cybersecurity landscape is constantly evolving, with cybercriminals developing increasingly sophisticated attack methods. To effectively implement and manage XDR solutions, organizations require highly skilled cybersecurity professionals who possess the expertise to configure, monitor, and respond to threats effectively. Unfortunately, the demand for such professionals far exceeds the current supply, resulting in a significant skills gap. One aspect of the skills gap challenge is the shortage of qualified personnel with expertise in XDR technologies specifically. XDR encompasses a wide range of security disciplines, including endpoint security, network monitoring, cloud security, and threat intelligence. Finding individuals who can proficiently work across these domains and understand the intricacies of XDR

+357 96 030922
info@marketpublishers.com

is a daunting task. Furthermore, the rapid pace of technological advancement and the continuous emergence of new cyber threats demand ongoing skill development and training. Cybersecurity professionals must stay updated on the latest threat vectors, vulnerabilities, and defensive strategies. However, traditional educational programs and training initiatives struggle to keep up with the ever-changing nature of the cybersecurity landscape. The consequences of the cybersecurity skills gap are profound. Organizations may struggle to fully leverage the capabilities of their XDR solutions, leaving them vulnerable to emerging threats. Moreover, the competition for skilled cybersecurity professionals drives up labor costs, putting additional pressure on organizations' budgets. To address the skills gap in the Global XDR market, proactive measures are essential. This includes investing in robust training and development programs, fostering collaboration between academia and industry, and encouraging more individuals to pursue careers in cybersecurity. Additionally, organizations may explore partnerships with managed security service providers (MSSPs) to access the expertise they lack in-house. In conclusion, the cybersecurity skills gap represents a significant challenge in the Global Extended Detection and Response (XDR) market. Addressing this gap is crucial for organizations seeking to harness the full potential of XDR solutions and effectively protect themselves against evolving cyber threats.

Customization and Adaptability

Customization and adaptability represent significant challenges in the Global Extended Detection and Response (HR SaaS) market. While HR SaaS solutions offer standardized features and functionalities to streamline HR processes, organizations often need the flexibility to tailor these systems to their specific needs and adapt them to changing business requirements. One of the key challenges in HR SaaS is striking the right balance between standardization and customization. HR processes can vary widely between organizations due to differences in industry, size, culture, and regulatory requirements. Organizations need the ability to customize their HR SaaS solutions to align with their unique workflows and business rules. This customization may involve configuring data fields, creating custom reports, or adapting workflows to match the organization's specific HR practices. Striking the right balance between standardization and customization is crucial to ensure that HR SaaS solutions remain user-friendly, maintainable, and upgradeable. Moreover, adaptability is vital in a dynamic business environment. Organizations often undergo changes such as mergers, acquisitions, reorganizations, and shifts in HR strategies. HR SaaS systems must be able to adapt to these changes swiftly and cost-effectively. The challenge lies in ensuring that customization efforts do not hinder the system's ability to accommodate evolving needs. This requires careful planning and a robust architecture that can accommodate updates

+357 96 030922
info@marketpublishers.com

and changes without causing disruptions to day-to-day HR operations. Another aspect of customization and adaptability is localization. Global organizations with a presence in multiple regions may require HR SaaS solutions that can be localized to comply with local labor laws, languages, and cultural norms. Customizing and adapting HR SaaS platforms to cater to these diverse requirements can be complex, as it involves accommodating different regulatory frameworks and ensuring that the system remains coherent and user-friendly across various regions. Additionally, the rapid pace of technological advancements and the introduction of new HR practices and tools present ongoing challenges. HR SaaS solutions need to keep pace with emerging trends in HR, such as artificial intelligence, machine learning, and advanced analytics. They should offer the flexibility to integrate with or incorporate these innovations seamlessly. The challenge is to ensure that customization and adaptability efforts do not create a fragmented or overly complex HR tech stack. To address these challenges, organizations and HR SaaS providers should prioritize modular architecture, open APIs, and a user-friendly configuration interface. These features allow for easier customization and adaptability without sacrificing system stability or performance. Furthermore, organizations should establish clear change management processes and involve key stakeholders in customization and adaptation decisions to ensure alignment with business goals and strategies.

Key Market Trends

Convergence of Security Technologies:

A major trend in the XDR market is the convergence of various cybersecurity technologies into unified platforms. Organizations are moving away from deploying siloed security solutions, such as endpoint detection and response (EDR), network detection and response (NDR), and cloud security tools, in favor of integrated XDR solutions. These platforms provide a comprehensive and centralized approach to threat detection and response, offering a unified view of an organization's security posture across diverse environments. This convergence trend addresses the challenges of alert fatigue and disjointed security operations. XDR solutions gather and correlate data from multiple sources, including endpoints, networks, cloud services, and email, creating a holistic picture of potential threats. By aggregating and contextualizing data, XDR platforms enable more accurate threat detection and reduce false positives, allowing security teams to focus their efforts on genuine risks. Moreover, the integration of threat intelligence feeds and machine learning algorithms empowers XDR solutions to proactively identify emerging threats and provide actionable insights. The shift towards converged XDR platforms not only streamlines security operations but also enhances

+357 96 030922
info@marketpublishers.com

incident response capabilities. Centralized dashboards and automated response actions facilitate rapid threat mitigation, reducing the dwell time of attackers in an organization's network. This trend aligns with the broader industry goal of achieving better visibility and control over cybersecurity landscapes, and it simplifies the deployment and management of security technologies.

Zero Trust Security Framework:

Zero Trust has emerged as a dominant cybersecurity framework and is becoming increasingly integrated into XDR strategies. The Zero Trust approach challenges the traditional security paradigm by assuming that threats can exist both outside and inside an organization's network. Consequently, it requires continuous verification of users and devices, strict access control, and real-time monitoring of network traffic. XDR solutions are embracing the principles of Zero Trust by focusing on identity-centric security, micro-segmentation, and least-privilege access. These solutions help organizations establish a dynamic and adaptive security perimeter that adapts to changing threat landscapes. XDR platforms employ user and entity behavior analytics (UEBA) to monitor user and device behavior, identifying anomalies that may indicate insider threats or compromised accounts. Additionally, XDR integrates with identity and access management (IAM) solutions to enforce least-privilege access policies, limiting user permissions to the minimum necessary for their roles. With Zero Trust principles at its core, XDR enhances an organization's ability to prevent, detect, and respond to security incidents across the entire attack surface, regardless of where they originate.

Cloud-Native XDR Solutions:

The adoption of cloud computing continues to accelerate, and XDR solutions are evolving to meet the unique demands of cloud-native environments. Organizations are shifting their workloads and data to the cloud to leverage scalability, flexibility, and cost-efficiency. As a result, traditional on-premises security tools are becoming less effective in protecting cloud-based assets. Cloud-native XDR solutions are designed to seamlessly integrate with cloud environments, providing comprehensive security coverage for cloud workloads, applications, and infrastructure. These solutions offer centralized visibility and control over multi-cloud and hybrid cloud environments, addressing the challenges of maintaining consistent security policies and threat detection across diverse cloud platforms. Cloud-native XDR leverages native cloud integrations, APIs, and cloud-specific threat intelligence to detect and respond to threats in real-time. It also supports container security, serverless computing, and DevOps workflows, enabling organizations to secure their applications and services throughout

+357 96 030922
info@marketpublishers.com

the development and deployment lifecycle. Furthermore, cloud-native XDR solutions are scalable and elastic, adapting to the dynamic nature of cloud environments and the fluctuating workloads that organizations encounter. This trend reflects the growing recognition that cloud security is an integral component of XDR strategies, as organizations increasingly rely on cloud resources to drive their digital transformation initiatives. In conclusion, the global Extended Detection and Response (XDR) market is witnessing significant transformations driven by the convergence of security technologies, the adoption of Zero Trust frameworks, and the development of cloud-native XDR solutions. These trends reflect the industry's response to the evolving threat landscape and the need for more holistic, adaptable, and scalable cybersecurity solutions. As organizations continue to grapple with advanced cyber threats, these trends will play a pivotal role in shaping the future of XDR and the broader cybersecurity landscape.

Segmental Insights

Solution Insights The solution segment dominated the global extended detection and response (XDR) market in 2022. This is expected to continue throughout the forecast period. The solution segment includes software and hardware products that are used to collect, analyze, and respond to security threats. XDR solutions typically include a variety of components, such as endpoint security, network security, and cloud security. The service segment is the second-largest segment in the global XDR market, with a revenue share of 39.8%. The service segment includes consulting, implementation, and managed services. Consulting services help organizations to assess their security needs and select the right XDR solution. Implementation services help organizations to deploy and configure the XDR solution. Managed services help organizations to operate and maintain the XDR solution. Here are some of the factors driving the growth of the solution segment in the global XDR market: The increasing sophistication of cyber threats, growing need for visibility into security threats across multiple attack vectors. Moreover, increasing adoption of cloud computing The increasing adoption of BYOD (bring your own device) policies.

Here are some of the factors driving the growth of the service segment in the global XDR market:

The complexity of XDR solutions

The need for expertise in deploying and configuring XDR solutions

+357 96 030922
info@marketpublishers.com

The need for ongoing support and maintenance of XDR solutions.

Regional Insights

North America is dominating the global extended detection and response (XDR) market, in 2022. This is due to the following factors:

The increasing number of cyberattacks in the region

The increasing awareness of the importance of cybersecurity

The presence of a large number of key players in the region.

Key Market Players

Bitdefender

BROADCOM

Cybereason

Cynet

Fidelis Cybersecurity

MCAFEE

Microsoft

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

+357 96 030922
info@marketpublishers.com

also been detailed below:

Global Extended Detection and Response Market, By Component:

Solution

Service

Global Extended Detection and Response Market, By Deployment Model:

Cloud Based

On-premise

Global Extended Detection and Response Market, By Enterprise Size:

Large Enterprises

SMEs

Global Extended Detection and Response Market, By Industry Vertical:

BFSI

Government

Manufacturing

Energy and Utilities

Healthcare

Retail and E Commerce

IT and Telecom

Global Extended Detection and Response Market, By Region:

North America

+357 96 030922
info@marketpublishers.com

- United States
- Canada
- Mexico

Europe

- France
- United Kingdom
- Italy
- Germany
- Spain

Asia-Pacific

- China
- India
- Japan
- Australia
- South Korea

South America

- Brazil
- Argentina
- Colombia

+357 96 030922
info@marketpublishers.com

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, Tech Sci 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).

+357 96 030922
info@marketpublishers.com

Contents

+357 96 030922
info@marketpublishers.com

OUTLOOK

7. ASIA-PACIFIC EXTENDED DETECTION AND RESPONSE MARKET OUTLOOK

+357 96 030922
info@marketpublishers.com

+357 96 030922
info@marketpublishers.com

8. EUROPE EXTENDED DETECTION AND RESPONSE MARKET OUTLOOK

+357 96 030922
info@marketpublishers.com

9. SOUTH AMERICA EXTENDED DETECTION AND RESPONSE MARKET OUTLOOK

+357 96 030922
info@marketpublishers.com

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

+357 96 030922
info@marketpublishers.com

+357 96 030922
info@marketpublishers.com

+357 96 030922
info@marketpublishers.com

+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, By Competition Forecast & Opportunities, 2018-2028

Product link: https://marketpublishers.com/r/ECC522578B59EN.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/ECC522578B59EN.html