+44 20 8123 2220
info@marketpublishers.com

Intrusion Detection and Prevention Systems Market – Global Industry Size, Share, Trends, Opportunity, and Forecast. Segmented by Components (Solutions, Services), by Type (Network-Based, Wireless-based, Network behavior analysis, Host-based), by Organization Size (Small and Medium-sized Enterprises (SMEs), Large Enterprise), by Deployment Model (Cloud, On-premises) and by Industry Verticals (Banking, Financial Services and Insurance (BFSI), Government and Defense, Healthcare, Information Technology (IT) and Telecom, Retail and eCommerce, Manufacturing, Others), By Region, By Company and By Geography, Forecast & Opportunities, 2018-2028.

https://marketpublishers.com/r/IAAB50DD45ACEN.html
Date: October 2023
Pages: 181
Price: US$ 4,900.00 (Single User License)
ID: IAAB50DD45ACEN

Abstracts

The Global Intrusion Detection and Prevention Systems Market, valued at USD 6 billion in 2022, is experiencing significant growth, with a projected CAGR of 11.9% during the forecast period. This growth is primarily driven by the ever-evolving landscape of cybersecurity threats.

In today's digital age, IDPS solutions have become indispensable for organizations of all sizes. They are essential in safeguarding networks, data, and critical assets from a wide range of malicious activities, including cyberattacks, data breaches, and unauthorized access. These systems are meticulously designed to detect and respond to security incidents in real-time, providing proactive defense mechanisms against both known and

+44 20 8123 2220
info@marketpublishers.com

emerging threats.

Several factors contribute to the increasing demand for advanced IDPS solutions. These include the stringent requirements of regulatory compliance, the rapid expansion of cloud computing services, and the necessity to secure remote work environments. As organizations prioritize cybersecurity as a fundamental component of their business strategies, the Global IDPS Market is poised for continuous growth. It offers innovative solutions that address the ever-evolving challenges posed by the digital age, ensuring the security and integrity of critical digital assets.

Key Market Drivers

Rising Cybersecurity Threats

The escalating and ever-evolving landscape of cybersecurity threats is a primary driver behind the rapid growth of the global Intrusion Detection and Prevention Systems (IDPS) market. In recent years, cyberattacks have become increasingly sophisticated, frequent, and damaging, targeting organizations across all sectors, from government agencies to private enterprises. These attacks range from ransomware and data breaches to advanced persistent threats (APTs) and zero-day vulnerabilities. As cybercriminals continuously develop new tactics and attack vectors, the need for robust IDPS solutions has never been more critical. IDPS systems serve as a frontline defense, constantly monitoring network traffic and systems for suspicious activities and patterns indicative of cyber threats. By swiftly detecting and mitigating intrusions and vulnerabilities, IDPS solutions play a pivotal role in preventing data breaches, service disruptions, and financial losses. Organizations are increasingly recognizing the importance of proactive cybersecurity measures to safeguard their digital assets, intellectual property, and customer data. As a result, they are investing heavily in advanced IDPS technologies to fortify their security postures and stay one step ahead of cyber adversaries. This rising awareness of the pervasive and evolving nature of cybersecurity threats is propelling the global IDPS market forward, driving innovation in threat detection and mitigation strategies and fueling the demand for cutting-edge IDPS solutions to protect critical infrastructures and maintain business continuity in an increasingly interconnected and digital world.

Stringent Regulatory Requirements

The stringent regulatory requirements imposed on businesses across industries are a driving force behind the growth of the global Intrusion Detection and Prevention

+44 20 8123 2220
info@marketpublishers.com

Systems (IDPS) market. Governments and industry regulatory bodies worldwide have recognized the critical importance of cybersecurity in protecting sensitive data and critical infrastructure. Consequently, they have introduced a myriad of stringent compliance standards and data protection regulations, such as GDPR, HIPAA, and PCI DSS, mandating that organizations implement robust security measures to safeguard their digital assets and customer information. Compliance with these regulations necessitates the deployment of advanced IDPS solutions capable of proactively identifying and mitigating cyber threats in real-time. IDPS systems play a pivotal role in helping organizations achieve regulatory compliance by continuously monitoring network traffic, detecting potential intrusions or data breaches, and facilitating incident response. Furthermore, they provide detailed logs and reports that can be essential for demonstrating adherence to regulatory requirements during audits and investigations. As businesses face increasingly complex and evolving regulatory landscapes, the demand for comprehensive IDPS solutions continues to rise, making them indispensable tools in ensuring legal and regulatory compliance. In this context, the global IDPS market is set to expand as organizations prioritize meeting regulatory standards and mitigating the potential financial and reputational risks associated with non-compliance in an era of escalating cyber threats and regulatory scrutiny.

Growth in Cloud Computing

The proliferation of cloud computing has emerged as a significant catalyst for the growth of the global Intrusion Detection and Prevention Systems (IDPS) market. As organizations increasingly migrate their IT infrastructure and data to cloud environments, they face unique security challenges that necessitate robust IDPS solutions. Cloud computing's scalability and flexibility bring about expanded attack surfaces, making it imperative to have effective intrusion detection and prevention measures in place. IDPS solutions tailored for cloud environments offer real-time monitoring and protection against threats targeting cloud-hosted applications and data. They can detect unauthorized access, anomalous behaviors, and suspicious activities within cloud-based systems, providing timely alerts and automated responses to security incidents. Furthermore, the integration of IDPS with cloud-native security platforms bolsters cloud security postures by offering centralized visibility and control over cloud assets. As businesses across various industries continue to embrace cloud services to enhance agility and scalability, the demand for cloud-compatible IDPS solutions is poised to grow. The symbiotic relationship between cloud computing and IDPS not only fortifies cloud security but also contributes significantly to the evolution and expansion of the global IDPS market as organizations prioritize safeguarding their cloud-based assets and data in an increasingly digital and interconnected world.

+44 20 8123 2220
info@marketpublishers.com

Integration with Security Ecosystem

The integration of Intrusion Detection and Prevention Systems (IDPS) with the broader security ecosystem is a pivotal driver in the growth of the global IDPS market. In today's complex cybersecurity landscape, organizations recognize that a multi-layered security approach is essential to effectively combat evolving threats. IDPS solutions are now seamlessly integrated with complementary security technologies such as Security Information and Event Management (SIEM) systems and Security Orchestration, Automation, and Response (SOAR) platforms. This integration empowers organizations with a holistic and real-time view of their security posture. When a potential threat is detected by the IDPS, it can trigger automated responses within the security ecosystem, such as isolating affected devices, blocking suspicious traffic, or alerting security teams for further investigation. This orchestration and automation significantly reduce response times, enhance incident management, and mitigate the impact of security breaches. Furthermore, the synergy between IDPS and other security tools allows organizations to correlate data across various sources, improving threat detection accuracy. This integrated approach not only strengthens an organization's security defenses but also streamlines operations, making it a strategic imperative for businesses looking to stay ahead of cyber threats. As the threat landscape continues to evolve, the seamless integration of IDPS within the broader security ecosystem will be a driving force in fortifying cybersecurity postures and driving the growth of the global IDPS market.

Key Market Challenges

Complex Network Integration

The Global Intrusion Detection and Prevention Systems (IDPS) Market faces a substantial challenge in the intricate integration of these systems into complex network infrastructures. Organizations typically operate diverse IT environments, comprising legacy systems, cloud-based services, and a multitude of interconnected devices. Integrating IDPS solutions seamlessly across these diverse components while maintaining consistent threat detection and response capabilities can be demanding. The challenge lies in ensuring that the IDPS can effectively monitor and analyze network traffic, detect anomalies, and mitigate threats across a highly dynamic and heterogeneous network landscape. Addressing this challenge requires comprehensive network assessment, robust API integrations, and advanced orchestration platforms that facilitate the unified operation of IDPS solutions within complex IT ecosystems.

+44 20 8123 2220
info@marketpublishers.com

Evolving Threat Landscape

The constantly evolving threat landscape is a significant challenge for the Global IDPS Market. Cyber adversaries are becoming increasingly sophisticated, deploying new tactics and techniques to bypass traditional security measures. From polymorphic malware to zero-day vulnerabilities, organizations face a barrage of advanced threats that can easily evade detection by conventional IDPS solutions. This challenge emphasizes the need for IDPS systems to continuously evolve and adapt to emerging threats. It necessitates advanced threat intelligence, machine learning, and behavioral analysis capabilities to detect and respond to previously unseen attack patterns. Organizations must also invest in ongoing training and skill development for their security teams to stay ahead of the evolving threat landscape.

Data Privacy and Compliance

Maintaining data privacy and compliance with stringent regulatory requirements is a pressing challenge within the Global IDPS Market. With data breaches and privacy violations becoming more frequent and costly, organizations are under increased pressure to safeguard sensitive information and adhere to data protection regulations such as GDPR, HIPAA, and CCPA. IDPS solutions play a crucial role in identifying and mitigating threats to data security. However, organizations must balance the benefits of threat detection with the need to protect user privacy and adhere to legal and regulatory frameworks. Ensuring that IDPS systems do not inadvertently violate privacy laws or expose sensitive data during threat analysis is a complex task. Overcoming this challenge requires the development of privacy-preserving IDPS technologies, robust data anonymization techniques, and adherence to stringent compliance practices.

Resource Constraints

Resource constraints, including budget limitations and a shortage of skilled cybersecurity professionals, pose a significant challenge in the Global IDPS Market. Many organizations, especially small and mid-sized enterprises, may face budgetary constraints that limit their ability to invest in advanced IDPS solutions and services. Additionally, the cybersecurity talent gap continues to widen, making it challenging for organizations to recruit and retain skilled professionals capable of managing and optimizing IDPS systems. This resource constraint hampers the effective deployment and operation of IDPS solutions, leaving organizations vulnerable to cyber threats. To address this challenge, organizations should explore cost-effective IDPS options, such

+44 20 8123 2220
info@marketpublishers.com

as managed security services, and invest in cybersecurity training and education programs to bridge the talent gap.

Key Market Trends

Advanced Threat Detection Capabilities

An influential trend shaping the Global Intrusion Detection and Prevention Systems (IDPS) Market is the focus on Advanced Threat Detection Capabilities. With the cybersecurity landscape constantly evolving and threats becoming more sophisticated, organizations are increasingly turning to IDPS solutions with advanced threat detection mechanisms. This trend is driven by the need to identify and respond to previously unknown and highly targeted cyber threats effectively. Modern IDPS solutions leverage artificial intelligence (AI), machine learning, and behavioral analysis to detect anomalies and potential breaches in real-time. They offer enhanced visibility into network traffic, rapid threat identification, and proactive threat mitigation. As cyberattacks continue to rise in complexity, the adoption of IDPS solutions with advanced threat detection capabilities becomes crucial for organizations looking to bolster their cybersecurity posture.

Zero Trust Architecture Integration

The integration of Zero Trust Architecture (ZTA) is a significant trend influencing the Global IDPS Market. With the traditional perimeter-based security model proving insufficient in the face of evolving threats, organizations are embracing ZTA principles that advocate a 'never trust, always verify' approach to network security. IDPS solutions play a pivotal role in ZTA by continuously monitoring and inspecting network traffic, irrespective of whether it originates from inside or outside the network perimeter. This trend is driven by the need to secure hybrid and remote work environments, where employees access corporate resources from various locations and devices. IDPS solutions aligned with ZTA enhance security by scrutinizing user behavior, device posture, and application access, thereby reducing the attack surface and minimizing the risk of breaches. As organizations shift towards ZTA to adapt to the changing threat landscape, the integration of IDPS solutions as a foundational element of this approach is expected to gain prominence.

Cloud-Native and SaaS-Based Solutions

The adoption of Cloud-Native and Software as a Service (SaaS)-Based IDPS solutions

+44 20 8123 2220
info@marketpublishers.com

is reshaping the Global IDPS Market. Organizations are increasingly migrating their IT infrastructures and applications to the cloud, leading to a growing demand for cloud-native security solutions, including IDPS. This trend is driven by the scalability, flexibility, and cost-efficiency offered by cloud-based IDPS deployments. Cloud-native IDPS solutions can seamlessly integrate with cloud environments, providing real-time threat detection and prevention without the need for on-premises hardware. Additionally, SaaS-based IDPS solutions offer ease of management, automatic updates, and simplified deployment, making them attractive to organizations seeking rapid implementation and reduced operational overhead. As the adoption of cloud computing continues to grow, the shift towards cloud-native and SaaS-based IDPS solutions is expected to accelerate, enabling organizations to secure their cloud workloads effectively.

Zero-Day Vulnerability Protection

Zero-Day Vulnerability Protection is a critical trend in the Global IDPS Market, focusing on mitigating vulnerabilities and reducing the risk of zero-day attacks. Zero-day vulnerabilities are software flaws that are exploited by attackers before vendors can release patches or updates. Organizations are increasingly seeking IDPS solutions that can proactively identify and defend against such vulnerabilities. This trend is driven by the potentially devastating impact of zero-day attacks, which can lead to data breaches, financial losses, and reputational damage. Modern IDPS solutions employ techniques like vulnerability scanning, threat intelligence feeds, and behavior analysis to detect and block zero-day exploits in real-time. By prioritizing zero-day vulnerability protection, organizations aim to strengthen their security posture and reduce the window of vulnerability when new threats emerge. As cyber threats continue to target undiscovered vulnerabilities, the emphasis on zero-day protection remains a key trend in the IDPS market.

Segmental Insights

Component Insights

The 'Solutions' segment emerged as the dominant force in the Global Intrusion Detection and Prevention Systems (IDPS) Market, and it is poised to maintain its dominance throughout the forecast period. Solutions in the IDPS market include hardware and software components that directly contribute to threat detection and prevention. This dominance is attributed to the increasing emphasis on cybersecurity across industries, driving organizations to invest significantly in robust IDPS solutions to safeguard their networks and sensitive data. As cyber threats become more

sophisticated and prevalent, the demand for comprehensive IDPS solutions equipped with advanced threat detection mechanisms, behavioral analysis, and real-time monitoring capabilities is on the rise. Organizations are keen on bolstering their cybersecurity posture, and this trend is expected to persist, driving the continued dominance of the 'Solutions' segment in the Global IDPS Market. Additionally, as the threat landscape evolves, IDPS solution providers are innovating and enhancing their offerings to address emerging cybersecurity challenges, further solidifying the Solutions segment's position as the cornerstone of the IDPS market.

Deployment Model Insights

The 'On-premises' deployment model segment asserted its dominance in the Global Intrusion Detection and Prevention Systems (IDPS) Market, and this trend is anticipated to persist throughout the forecast period. The on-premises deployment model involves the installation and operation of IDPS solutions within an organization's own physical infrastructure, offering complete control over security measures and data. This dominance is primarily driven by industries and enterprises with stringent data security and compliance requirements, such as government agencies, financial institutions, and healthcare providers. These organizations prefer on-premises IDPS solutions to maintain data sovereignty and meet regulatory standards effectively. Furthermore, they prioritize the ability to customize and fine-tune security measures to align with their specific needs. While cloud-based IDPS solutions have gained traction, particularly among smaller businesses seeking scalability and flexibility, the need for robust, localized security infrastructure continues to fuel the dominance of the on-premises deployment model. As data breaches and cyber threats persist, organizations are committed to safeguarding their critical assets, making the on-premises deployment model a pivotal component of their cybersecurity strategies and ensuring its continued dominance in the Global IDPS Market.

Organization Size Insights

The 'Large Enterprise' segment emerged as the dominant force in the Global Intrusion Detection and Prevention Systems (IDPS) Market, and this dominance is projected to persist throughout the forecast period. Large enterprises, characterized by their expansive networks, complex IT infrastructures, and substantial data assets, have a heightened need for robust cybersecurity solutions. They typically encounter a higher volume of cyber threats and attacks due to their larger attack surface, making them proactive in implementing comprehensive IDPS systems. Furthermore, large enterprises often handle sensitive customer data and proprietary information,

necessitating stringent security measures to safeguard their assets and maintain regulatory compliance. Their substantial financial resources and dedicated IT security teams enable them to invest in and manage sophisticated IDPS solutions effectively. While small and medium-sized enterprises (SMEs) also recognize the importance of cybersecurity, budget constraints and resource limitations sometimes lead them to opt for more cost-effective or cloud-based IDPS solutions. In contrast, large enterprises prioritize comprehensive, on-premises IDPS systems to ensure robust protection against evolving threats. Given the continuous evolution of cyber threats and the persistent need for advanced security measures, the large enterprise segment is expected to maintain its dominance in the Global IDPS Market.

Regional Insights

In 2022, North America emerged as the dominant region in the Global Intrusion Detection and Prevention Systems (IDPS) Market, and it is anticipated to maintain its leadership throughout the forecast period. Several factors contribute to North America's dominance in this market. Firstly, North America is home to a plethora of technology giants, cybersecurity firms, and cutting-edge startups, making it a hotbed for innovation and development in the field of cybersecurity. The region's extensive research and development activities continually yield advanced IDPS solutions, driving adoption. Secondly, North America faces a significant and persistent threat landscape, with a high frequency of cyberattacks on government institutions, businesses, and critical infrastructure. This heightened threat perception has led organizations to prioritize cybersecurity investments, including robust IDPS solutions. Additionally, stringent regulatory frameworks, such as the Health Insurance Portability and Accountability Act (HIPAA) and the Payment Card Industry Data Security Standard (PCI DSS), mandate stringent security measures, fueling the demand for IDPS solutions in healthcare and financial sectors. Furthermore, North America's thriving e-commerce industry and cloud adoption contribute to the need for robust cybersecurity measures, further propelling the IDPS market. Lastly, the region's strong digital economy, the presence of major financial institutions, and its role as a global business hub make it particularly attractive to cybercriminals, underscoring the necessity for comprehensive intrusion detection and prevention systems. As North American organizations continue to face evolving cyber threats, the region is poised to maintain its dominance in the Global IDPS Market, serving as a significant driver of innovation and adoption in the cybersecurity landscape.

Key Market Players

Nortek Security & Control LLC

+44 20 8123 2220
info@marketpublishers.com

Tyco International Ltd.

Bosch Security Systems

Allegion PLC

UTC Fire & Security.

Honeywell International, Inc.

Detection.com

Godrej & Boyce Manufacturing Company Limited

AssaAbloy Group

Control4 Corporation

Report Scope:

In this report, the Global Intrusion Detection and Prevention Systems Market has been segmented into the following categories, in addition to the industry trends which have also been detailed below:

Global Intrusion Detection and Prevention Systems Market, By Components:

Solutions

Services

Global Intrusion Detection and Prevention Systems Market, By Type:

Network-Based

Wireless-based

Network behavior analysis

+44 20 8123 2220
info@marketpublishers.com

Host-based

Global Intrusion Detection and Prevention Systems Market, By Organization Size:

Small and Medium-sized Enterprises (SMEs)

Large Enterprise

Global Intrusion Detection and Prevention Systems Market, By Deployment Model:

Cloud

On-premises

Global Intrusion Detection and Prevention Systems Market, By Industry Verticals:

Banking

Financial Services and Insurance (BFSI)

Government and Defense

Healthcare

Information Technology (IT) and Telecom

Retail and eCommerce

Manufacturing

Others

Global Intrusion Detection and Prevention Systems Market, By Region:

North America

+44 20 8123 2220
info@marketpublishers.com

- Europe
- South America
- Middle East & Africa
- Asia Pacific

Competitive Landscape

Company Profiles: Detailed analysis of the major companies present in the Global Intrusion Detection and Prevention Systems Market.

Available Customizations:

Global Intrusion Detection and Prevention Systems 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).

+44 20 8123 2220
info@marketpublishers.com

Contents

+44 20 8123 2220
info@marketpublishers.com

+44 20 8123 2220
info@marketpublishers.com

9. EUROPE INTRUSION DETECTION AND PREVENTION SYSTEMS MARKET OUTLOOK

+44 20 8123 2220
info@marketpublishers.com

+44 20 8123 2220
info@marketpublishers.com

11. MIDDLE EAST & AFRICA INTRUSION DETECTION AND PREVENTION SYSTEMS MARKET OUTLOOK

+44 20 8123 2220
info@marketpublishers.com

12. ASIA PACIFIC INTRUSION DETECTION AND PREVENTION SYSTEMS MARKET OUTLOOK

+44 20 8123 2220
info@marketpublishers.com

+44 20 8123 2220
info@marketpublishers.com

+44 20 8123 2220
info@marketpublishers.com

+44 20 8123 2220
info@marketpublishers.com

+44 20 8123 2220
info@marketpublishers.com

I would like to order

Product name: Intrusion Detection and Prevention Systems Market – Global Industry Size, Share, Trends, Opportunity, and Forecast. Segmented by Components (Solutions, Services), by Type (Network-Based, Wireless-based, Network behavior analysis, Host-based), by Organization Size (Small and Medium-sized Enterprises (SMEs), Large Enterprise), by Deployment Model (Cloud, On-premises) and by Industry Verticals (Banking, Financial Services and Insurance (BFSI), Government and Defense, Healthcare, Information Technology (IT) and Telecom, Retail and eCommerce, Manufacturing, Others), By Region, By Company and By Geography, Forecast & Opportunities, 2018-2028.

Product link: https://marketpublishers.com/r/IAAB50DD45ACEN.html

Price: US$ 4,900.00 (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/IAAB50DD45ACEN.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

Custumer signature _____

+44 20 8123 2220
info@marketpublishers.com

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