Network Forensics Market Soars Owing to Need for Efficient Identification and Response to Security Breaches

Rising cyber threats and need for proactive threat detection drive growth in the Network Forensics Market, ensuring network security.

AUSTIN, TEXAS, UNITED STATES, March 5, 2024 /EINPresswire.com/ -- According to the latest SNS Insider report, the Network Forensics Market, valued at USD 2.89 Billion in 2022, is poised to reach USD 8.87 Billion by 2030. This remarkable growth, with a projected CAGR of 15.05% from 2023 to 2030, signifies the escalating importance of network security in today's interconnected landscape.

NETWORK FORENSICS MARKET SIZE AND SHARE 2023-2030

USD **2.89 BN** IN 2022

CAGR OF 15.05%

USD **8.87 BN** BY 2030

copyright ® snsinsider.com

Network Forensics Market Report

Network forensics, a pivotal process in cybersecurity, empowers companies to protect data, identify vulnerabilities, and investigate security threats. It involves the capture, recording, and analysis of network data to uncover the sources of cyber threats. As the volume of data traffic surges globally, the demand for network security solutions, particularly network forensics, witnesses a corresponding rise. The primary objective is evidence collection, with a focus on analyzing network traffic data from various sources and equipment. Network forensics aids in detecting attacks, analyzing attacker behavior, and identifying intrusion patterns, thereby enhancing overall cybersecurity measures.

> " Stringent regulatory compliance, increasing incidents of cyberattacks, and demand for real-time monitoring solutions fuel the Network Forensics Market's expansion."
>
> *SNS Insider Research*

Get a Report Sample of Network Forensics Market @ https://www.snsinsider.com/sample-request/2105

Some of the Major Key Players Studied in this Report are:

- IBM
- FireEye
- RSA Security
- Netscout Systems
- Cisco Systems
- Symantec
- Viavi Solutions
- LogRhythm
- Niksun
- Fortinet
- Proofpoint
- Other Players

Network Forensics Market Analysis

The Network Forensics Market is propelled by the surge in global network traffic and system complexities, with the internet population reaching 4.9 billion in 2021. Asia, boasting 51.8% of internet users, drives the market further. The escalating need to secure networks from advanced attacks and curb network crimes fuels the demand for network forensics solutions. As organizations globally increase investments in security solutions, network forensics emerges as a leading solution. This market addresses the challenges posed by heavy data traffic and intricate systems, offering the capability to capture, record, and analyze network traffic for investigation and incident response. The market's growth is underpinned by the rising adoption of cloud-based network forensics technologies, particularly for remote detection of security anomalies. With a forecasted CAGR of 15.05% from 2023 to 2030, the Network Forensics Market is poised to reach USD 8.87 Billion by 2030, reflecting its critical role
in the evolving cybersecurity landscape.

Market Segmentation Analysis

In the network forensics market, the cloud-based segment emerges as the dominant force, projecting the highest CAGR. The surge is attributed to the widespread adoption of cloud-based network forensics technologies for remote detection of security anomalies and incidents. As cloud computing gains popularity globally, government and private organizations shift services to the cloud, fueling the demand for cloud network forensics solutions. On the application front, the SMEs segment is on the rise, driven by growing adoption for large-scale data examination.

Key Regional Developments

North America is set to dominate the global network forensics market, thanks to prominent players in the region and increasing investments in network forensics infrastructure by various

industries. Meanwhile, the Asia Pacific region experiences a dynamic shift due to rising network complexities, changing threat landscapes, and the rapid adoption of new technologies. China, Singapore, India, and other Asia Pacific countries contribute significantly to this growth, making it the fastest-growing region during the forecast period.

Key Growth Drivers of the Network Forensics Market

The Network Forensics Market is propelled by several key growth drivers that underscore the critical importance of cybersecurity in today's interconnected digital landscape.

 Rising Cybersecurity Threats: With the proliferation of cyber attacks, including malware, ransomware, phishing, and data breaches, organizations face unprecedented security challenges. Network forensics solutions provide essential capabilities to detect, investigate, and mitigate cyber threats by analyzing network traffic, identifying suspicious activities, and uncovering the root causes of security incidents.

 Increasing Complexity of Network Environments: As networks become increasingly complex with the adoption of cloud computing, IoT devices, BYOD policies, and remote work arrangements, organizations struggle to maintain visibility and control over their digital assets. Network forensics tools offer advanced monitoring, analysis, and visualization capabilities to gain insights into network behavior, detect anomalies, and respond proactively to security incidents.

 Regulatory Compliance Requirements: Regulatory mandates and industry standards impose stringent requirements on organizations to protect sensitive data, prevent data breaches, and maintain compliance with data protection regulations such as GDPR, HIPAA, PCI DSS, and CCPA. Network forensics solutions help organizations demonstrate compliance by providing audit trails, incident response capabilities, and forensic evidence to support investigations and legal proceedings.

 Need for Real-Time Threat Detection and Response: In today's fast-paced threat landscape, organizations require real-time visibility into network traffic and rapid detection of security threats to mitigate risks and minimize the impact of cyberattacks. Network forensics solutions leverage advanced analytics, machine learning, and threat intelligence to identify suspicious behavior, correlate security events, and enable proactive threat hunting and incident response.

 Growing Adoption of Digital Transformation Technologies: The adoption of digital transformation technologies such as cloud computing, big data analytics, IoT, and AI/ML introduces new security challenges and attack vectors, increasing the complexity and scale of cybersecurity threats. Network forensics solutions play a crucial role in securing digital assets, protecting critical infrastructure, and safeguarding against emerging cyber threats in modern IT environments.

Emergence of Insider Threats: Insider threats, including negligent employees, malicious insiders, and compromised accounts, pose significant risks to organizational security and data integrity. Network forensics tools help organizations detect and investigate insider threats by monitoring user activity, analyzing network behavior, and detecting unauthorized access or data exfiltration attempts.

Overall, the Network Forensics Market is driven by the need for proactive threat detection, rapid incident response, regulatory compliance, and enhanced visibility into network traffic to safeguard digital assets, protect sensitive data, and mitigate cybersecurity risks in today's dynamic threat landscape. As organizations prioritize cybersecurity investments to address evolving threats and secure their digital infrastructure, the demand for network forensics solutions is expected to continue growing in the foreseeable future.

Key Takeaways

 The Network Forensics Market witnesses unprecedented growth, driven by the surge in cyber threats and the escalating need for robust security solutions.

 Cloud-based network forensics solutions and SMEs' increased adoption are pivotal factors shaping the market's trajectory.

 North America dominates the global market, while the Asia Pacific emerges as the fastest-growing region, fueled by technological advancements and changing threat landscapes.

Buy the Latest Version of this Report @ https://www.snsinsider.com/checkout/2105

Recent Developments

 In November 2021, NETSCOUT Systems partnered with AWS, enhancing security by expanding visibility for Amazon Web Services' customers.

 August 2021 saw Accenture Federal Services' acquisition of Novetta Solutions, bolstering its National Security portfolio.

 Viavi Solutions launched the XDR solution in August 2021, providing enterprises with analytics to defend against cloud- and identity-based threats.

Table of Contents- Major Key Points

1. Introduction

2. Research Methodology

About Us

SNS Insider is one of the leading market research and consulting agencies that dominates the market research industry globally. Our company's aim is to give clients the knowledge they require in order to function in changing circumstances. In order to give you current, accurate market data, consumer insights, and opinions so that you can make decisions with confidence, we employ a variety of techniques, including surveys, video talks, and focus groups around the world.

Our staff is dedicated to giving our clients reliable information, and with expertise working in the majority of industrial sectors, we're proud to be recognized as one of the world's top market research firms. We can quickly design and implement pertinent research programs, including surveys and focus groups, and we have the resources and competence to deal with clients in practically any company sector.

Akash Anand
SNS Insider | Strategy and Stats
+1 415-230-0044
email us here
Visit us on social media:
Facebook
Twitter
LinkedIn
Instagram
YouTube