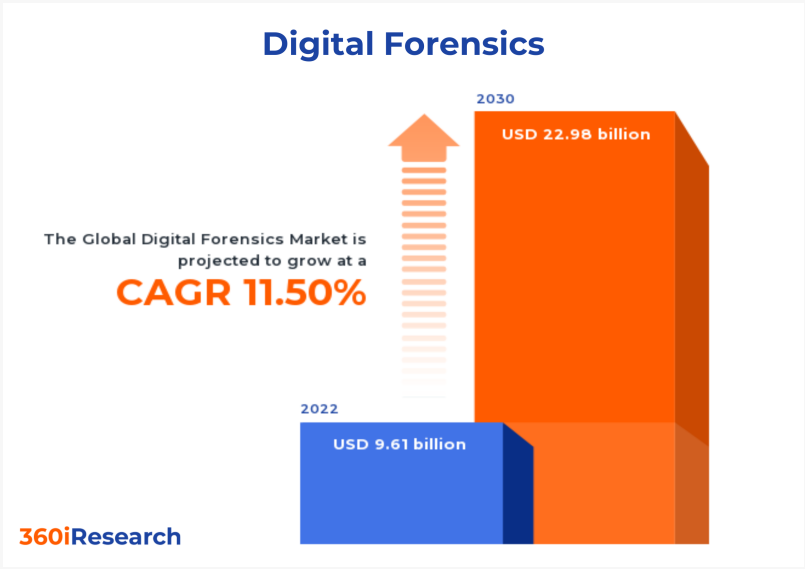
Digital Forensics Market worth $22.98 billion by 2030, growing at a CAGR of 11.50% - Exclusive Report by 360iResearch

The Global Digital Forensics Market to grow from USD 9.61 billion in 2022 to USD 22.98 billion by 2030, at a CAGR of 11.50%.



Digital Forensics Market - Exclusive Report by 360iResearch

PUNE, MAHARASHTRA, INDIA , November 15, 2023 / EINPresswire.com/ -- The "Digital Forensics Market by Type (Cloud Forensics, Database Forensics, Mobile Device Forensics), Component (Hardware, Services, Software), Deployment, Application, Vertical - Global Forecast 2023-2030" report has been added to 360iResearch.com's offering.

The Global Digital Forensics Market to grow from USD 9.61 billion in 2022 to USD 22.98 billion by 2030, at a CAGR of 11.50%.

Request a Free Sample Report @ https://www.360iresearch.com/library/intelligence/digital-forensics?utm_source=einpresswire&utm_medium=referral&utm_campaign=sample

Digital forensics encapsulates an array of professional services that revolve around investigating and recovering data in digital devices. Digital forensics includes systematic inspection of computer systems, networks, software, and digital devices to discover and identify potential evidence of cyber crimes. The increasing incidence of cybercrime, data breaches, and digital misconduct activities worldwide has surged the need for e-discovery of data for legal and litigation support. The rising adoption of cloud systems within small & medium enterprises with the utilization of cloud forensics is also responsible for the market growth. However, the technical complexity of digital forensics and the need for specialized resources may limit the market adoption of digital forensics solutions. Limitations associated with data encryption of digital evidence also emerged as a concerning factor for the market growth. Moreover, The

advancements in digital forensics tools & AI & ML technologies are expected to create opportunities for market growth. The ongoing collaborations between digital forensics providers and corporate investigators are also anticipated to captivate advantageous prospects in the market.

Deployment: Rising cloud-based deployment of digital forensics tools
The growing need for remote accessibility and multifarious benefits, such as unlimited storage and scalability, has led to an increasing preference for cloud-based deployment of digital forensics tools. Despite the growing cloud trend, on-premises deployment has the ability to provide more control, strong data security, and low latency, thus proving useful for organizations handling sensitive data.

Component: Improvements in digital forensic software components
Hardware includes physical components, including computers, storage devices, and specialized equipment such as write-blockers that prevent modifications to a storage device while allowing access to data in the process of digital investigations. The software component refers to a suite of tools for file recovery, decryption, data carving, timeline analysis, and reporting of various digital investigation stages, from the initial collection phase to the eventual reporting of investigations. The services encompass the procedural and consultative operations in digital forensics investigations for in-field data collection, analysis, and preservation of digital evidence. Services related to digital forensics are essential for enhancing system security, preventing cybercrime, and enabling accurate data recovery from digital devices.

Application: Emerging applications for cybersecurity risk management
Data recovery has extensive applications in digital forensics to retrieve data from damaged, corrupted, or inaccessible storage media when it cannot be accessed normally. Data recovery is used in data loss scenarios due to mechanical damages, system malfunctions, accidental deletions, and cyber threats. Incident response utilizes an organized approach to managing and addressing the aftermath of a security breach or cyber attack. Incident response tools involve identifying and closing the security breach, mitigating the risks of future incidents, and communicating effectively about the issue to affected parties. Risk management tools involve identifying, assessing, and prioritizing risks to predict potential vulnerabilities and threats that compromise data integrity and security. Regulatory compliance ensures that companies are adhering to laws, policies, and regulations relevant to their business processes. e-Discovery is utilized to seek electronic data located, secured, and searched with the intention of using it as evidence in a legal case. E-Discovery also extends to data that is rarely accessible, such as backup data, which is often used as a necessary asset during legal proceedings.

Vertical: Emerging practices of digital forensic tools across law enforcement and education
Banking, finance & insurance utilize digital forensic tools to detect fraudulent transactions and protect client information. Digital forensics is crucial in the government, defense, and law enforcement sectors, offering meticulous investigation and surveillance facilities. Digital forensics aids in gathering intelligence, countering hacking attempts, and safeguarding defense-

related sensitive data. In the Healthcare sector, Digital forensics is vital to ensure patient privacy, as well as to maintain data integrity and abide by privacy laws for tracking and resolving suspicious activities. Digital forensics plays an essential role in securing sensitive infrastructure data and managing the cybersecurity of operations for reinforcing cybersecurity measures, preventing hacking attempts at energy plants, and supporting the security of smart grid systems. Digital forensics ensures the safety of student data and enforces digital ethics among students to identify unauthorized access to sensitive information, investigate cyberbullying cases, and promote a safe digital learning environment.

Type: Rising utilization of cloud forensics for enterprise data security
Network forensics covers tracking and inspecting network traffic, both local and WAN/large-scale web connections, focusing on data recovery. Mobile device forensics concentrates on recovering data from mobile devices that may provide pivotal information during investigations. Mobile device forensics involves both physical and logical data extraction from phones, tablets, personal digital assistants (PDAs), and other related devices. Database forensics is preferred for the holistic study and examination of databases and their related metadata to uncover a sequence of events or manipulate data in a security incident on the enterprise level. Cloud forensics has gained significant momentum due to rapid data migration from local servers to cloud platforms. Cloud forensics applies forensic investigation techniques to cloud environments, mainly focusing on data recovery following a security breach.

Regional Insights:
In the Americas, the digital forensics market is growing precipitously due to increasing cybercrimes and strict regulations for data protection. Major countries such as the United States, Canada, and Brazil have shown significant growth resulting from advancements in cyber legislation and extensive consumer awareness about the importance of data security. In Europe, data protection regulations are fostering growth in major countries such as Germany, Italy, and the United Kingdom for discovering and identifying potential evidence of cyber crimes. Increasing online transactions, government initiatives, and rising awareness about data security are contributing to significant market growth in the APAC region. The rising number of technology startups in the region has also contributed to the market growth.

FPNV Positioning Matrix:

The FPNV Positioning Matrix is essential for assessing the Digital Forensics Market. It provides a comprehensive evaluation of vendors by examining key metrics within Business Strategy and Product Satisfaction, allowing users to make informed decisions based on their specific needs. This advanced analysis then organizes these vendors into four distinct quadrants, which represent varying levels of success: Forefront (F), Pathfinder (P), Niche (N), or Vital(V).

Market Share Analysis:

The Market Share Analysis offers an insightful look at the current state of vendors in the Digital

Forensics Market. By comparing vendor contributions to overall revenue, customer base, and other key metrics, we can give companies a greater understanding of their performance and what they are up against when competing for market share. The analysis also sheds light on just how competitive any given sector is about accumulation, fragmentation dominance, and amalgamation traits over the base year period studied.

Key Company Profiles:

The report delves into recent significant developments in the Digital Forensics Market, highlighting leading vendors and their innovative profiles. These include BasisTech LLC, Blackhawk Intelligence Limited, Carahsoft Technology Corp., Cellebrite DI Ltd., Commvault Systems, Inc., Consilio LLC, CY4OR Legal Limited, Digital WarRoom, Elcomsoft s.r.o., Epiq Systems, Inc., Exterro, Inc., FRONTEO Inc., FTI Consulting, Inc., Google LLC, International Business Machines Corporation, Kroll, LLC., Magnet Forensics Inc., Microsoft Corporation, MSAB Systemation AB, Nuix Limited, OpenText Corporation, Oracle Corporation, Oxygen Forensics, Inc., Paraben Corporation, ProDiscover Forensics by DotC Technologies Pvt Ltd., Tata Consultancy Services Limited, Technology Concepts & Design Inc., Thomson Reuters Corporation, X-Ways Software Technology AG, and XLY SalvationDATA Technology INC..

Inquire Before Buying @ https://www.360iresearch.com/library/intelligence/digital-forensics?utm_source=einpresswire&utm_medium=referral&utm_campaign=inquire

Market Segmentation & Coverage:

This research report categorizes the Digital Forensics Market in order to forecast the revenues and analyze trends in each of following sub-markets:

Based on Type, market is studied across Cloud Forensics, Database Forensics, Mobile Device Forensics, and Network Forensics. The Cloud Forensics is projected to witness significant market share during forecast period.

Based on Component, market is studied across Hardware, Services, and Software. The Services is projected to witness significant market share during forecast period.

Based on Deployment, market is studied across Cloud-Based and On-Premises. The Cloud-Based is projected to witness significant market share during forecast period.

Based on Application, market is studied across Data Recovery, e-Discovery, Incident Response, Regulatory Compliance, and Risk Management. The e-Discovery is projected to witness significant market share during forecast period.

Based on Vertical, market is studied across Banking, Finance & Insurance, Education, Energy & Utilities, Government & Defense, Healthcare, IT & Telecom, and Law Enforcement. The Education

is projected to witness significant market share during forecast period.

Based on Region, market is studied across Americas, Asia-Pacific, and Europe, Middle East & Africa. The Americas is further studied across Argentina, Brazil, Canada, Mexico, and United States. The United States is further studied across California, Florida, Illinois, New York, Ohio, Pennsylvania, and Texas. The Asia-Pacific is further studied across Australia, China, India, Indonesia, Japan, Malaysia, Philippines, Singapore, South Korea, Taiwan, Thailand, and Vietnam. The Europe, Middle East & Africa is further studied across Denmark, Egypt, Finland, France, Germany, Israel, Italy, Netherlands, Nigeria, Norway, Poland, Qatar, Russia, Saudi Arabia, South Africa, Spain, Sweden, Switzerland, Turkey, United Arab Emirates, and United Kingdom. The Americas commanded largest market share of 39.04% in 2022, followed by Europe, Middle East & Africa.

Key Topics Covered:

The report provides insights on the following pointers:
1. Market Penetration: Provides comprehensive information on the market offered by the key players
2. Market Development: Provides in-depth information about lucrative emerging markets and analyzes penetration across mature segments of the markets
3. Market Diversification: Provides detailed information about new product launches, untapped geographies, recent developments, and investments
4. Competitive Assessment & Intelligence: Provides an exhaustive assessment of market shares, strategies, products, certification, regulatory approvals, patent landscape, and manufacturing capabilities of the leading players
5. Product Development & Innovation: Provides intelligent insights on future technologies, R&D

activities, and breakthrough product developments

The report answers questions such as:
1. What is the market size and forecast of the Digital Forensics Market?
2. Which are the products/segments/applications/areas to invest in over the forecast period in the Digital Forensics Market?
3. What is the competitive strategic window for opportunities in the Digital Forensics Market?
4. What are the technology trends and regulatory frameworks in the Digital Forensics Market?
5. What is the market share of the leading vendors in the Digital Forensics Market?
6. What modes and strategic moves are considered suitable for entering the Digital Forensics Market?

Read More @ https://www.360iresearch.com/library/intelligence/digital-forensics?utm_source=einpresswire&utm_medium=referral&utm_campaign=analyst

Mr. Ketan Rohom
360iResearch
+1 530-264-8485
ketan@360iresearch.com
