

Mobile Threat Defense Market worth \$6.97 billion by 2030, growing at a CAGR of 14.10% - Exclusive Report by 360iResearch

The Global Mobile Threat Defense Market to grow from USD 2.42 billion in 2022 to USD 6.97 billion by 2030, at a CAGR of 14.10%.

PUNE, MAHARASHTRA, INDIA ,
December 8, 2023 /EINPresswire.com/
-- The "[Mobile Threat Defense Market](#) by Offering (Services, Software), Operating System (Android, IOS, Windows), Deployment, End-user - Global Forecast 2023-2030" report has been added to 360iResearch.com's offering.

The Global Mobile Threat Defense Market to grow from USD 2.42 billion in 2022 to USD 6.97 billion by 2030, at a CAGR of 14.10%.

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

The mobile threat defense includes solutions and services to protect personal and corporate mobile devices from threats such as malware, data breaches, and phishing attacks. It supports an array of business applications while also protecting confidential information on end-users' devices. Increasing incidences of cyber-attacks, the proliferation of smartphones and tablets, businesses' growing dependence on digitization, and the rising adoption of BYOD (Bring Your Own Device) policies in organizations are accelerating the use of mobile threat defense solutions. However, the high cost of implementing robust mobile threat defense solutions and the lack of skilled cybersecurity professionals may hinder the end-use sectors' use of mobile threat defense solutions. Moreover, the advent of AI and machine learning technologies in cybersecurity is expected to create numerous opportunities for mobile threat defense solutions by the end-use sectors globally.



Operating System: Significant penetration in Android-based operating system

Android is the most utilized operating system, boasting many devices. In terms of mobile threat defense, Android's open-source nature makes it a popular choice for security researchers and white-hat hackers. iOS is known for its stringent security protocols, closed-source code, and proprietary software. This makes it less susceptible to cyber threats and limits third-party researchers' security research. Companies heavily invest in strengthening their mobile security, signing multiple agreements with cyber defense companies to guard against sophisticated threats. Windows is known for substantial system updates that patch vulnerabilities regularly.

Offering: Proliferating use of MTD software across end-use sectors

Mobile Threat Defense (MTD) services refer to professional assistance organizations hire to protect their mobile devices and infrastructure from security threats. Businesses with limited internal resources or time constraints often prefer these services as they offer personalized defense strategies tailored to the organization's unique needs. Their offerings focus on customized outreach, including threat intelligence services, device risk scoring, and mobile phishing protection. Organizations with an in-house cybersecurity team choose MTD software offerings and require extra measures to protect their operations against mobile threats. They rely less on external services and need comprehensive software products to manage their security concerns in-house.

Deployment: Increasing deployment of cloud-based mobile threat defense (MTD)

Cloud-based Mobile Threat Defense (MTD) solutions have been growing in popularity due to their scalability, still-robust defense capabilities, and lower upfront costs. Enterprises with remote teams or those needing flexible data access can benefit from a cloud-based MTD. On-premise MTD solutions entice major corporations and government institutions that prioritize data autonomy and close control over their cybersecurity infrastructure. These offer the utmost data security, as they are less exposed to third-party vulnerabilities. Cloud-based systems are suitable for corporations with flexible working environments and those looking for cost-effective solutions. They ensure seamless integration, instant updates, and scalability. On-premise MTD solutions are preferred by entities requiring total control over their data, such as those in regulated industries or handling sensitive information.

End-user: Expanding applications of IT & Telecom sector

The education sector has rapidly adopted digital tools, making it crucial to implement mobile threat defense. Academicians, students, and staff are increasingly relying on smartphones and tablets to access information. Protecting these devices against malicious applications, network threats and vulnerabilities is key to securing sensitive data including course material, research papers, and personal identification detail. The BFSI sector is exposed to risks, with mobile banking and finance apps being targeted by cyber-attacks. Mobile threat defense solutions help in securing mobile banking applications and channel management systems from malwares, phishing activities, and credential thefts, thus enhancing the security of sensitive financial information. Government organizations hold massive amounts of confidential data, making

them prime targets for cyber-attacks. Mobile threat defense solutions are pivotal in safeguarding sensitive information, ensuring seamless public service distribution and enhancing adherence to data privacy & security regulations. For the healthcare industry, patient confidentiality and data protection are paramount. Mobile threat defense systems ensure secure access to patients' medical records, hospital management systems, and other sensitive applications on mobile devices, thus guarding against identity theft, privacy breaches, and other cyber threats. The IT and Telecom industry needs robust mobile threat defense mechanisms. It ensures the secure transmission of voice and data services, preventing intrusion attempts, denial-of-service attacks, or other network-based threats. In a manufacturing environment, mobile threat defense can protect shop floor devices from malware attacks and ensure uninterrupted, secure operations. These solutions also safeguard intellectual property and other proprietary information, essential for maintaining a competitive edge in the market. The retail industry is highly vulnerable to data privacy threats and mobile threat defense tools provide robust protection against threats on mobile point-of-sale systems, e-commerce apps, and customer data, ultimately securing transactions and customer trust. Mobile threat defense in transportation and logistics ensures the safety of critical logistics applications and location data. It enhances fleet management, reduces risks to delivery timelines and protects shipment information from cyber threats.

Regional Insights:

The mobile threat defense market is evolving in the Americas owing to the proliferation of mobile devices in businesses and homes, necessitating stricter mobile defense strategies. Ongoing investment in research and development has resulted in the registration of various patents aimed at enhancing mobile threat defense technologies in the Americas. Significant growth in mobile device usage, rising cybersecurity awareness levels, and emphasis on digital infrastructure are driving the use of mobile threat defense solutions in the APAC region. In EMEA, regulatory frameworks, active cybersecurity initiatives, and a rise in mobile and internet users have led to a surge in investments to manage mobile threats more effectively. Besides, improvements and advancements in mobile threat defense solutions are anticipated to propel the use of mobile threat defense solutions worldwide.

FPNV Positioning Matrix:

The FPNV Positioning Matrix is essential for assessing the Mobile Threat Defense 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 Mobile Threat Defense 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 Mobile Threat Defense Market, highlighting leading vendors and their innovative profiles. These include AO Kaspersky Lab, Barracuda Networks, Inc., BlackBerry Ltd., Broadcom, Inc., Check Point Software Technologies Ltd., Cisco Systems, Inc, Citrix Systems, Inc., Esper.io, Inc., Fortinet, Inc., Guardsquare NV, Ivanti Software, Inc., Lookout, Inc., Open Text Corporation, PRADEO SECURIT SYSTEMS, SAP SE, Thoma Bravo, LLC, Upstream Security Ltd., VMware, Inc., Zimperium, Inc., and Zoho Corporation Pvt. Ltd..

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

Market Segmentation & Coverage:

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

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

Based on Operating System, market is studied across Android, IOS, and Windows. The IOS is projected to witness significant market share during forecast period.

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

Based on End-user, market is studied across BFSI, Education, Government, Healthcare, IT & Telecom, Manufacturing, Retail, and Transportation & Logistics. The IT & Telecom 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 43.72% in 2022, followed by Europe, Middle East & Africa.

Key Topics Covered:

1. Preface
2. Research Methodology
3. Executive Summary
4. Market Overview
5. Market Insights
6. Mobile Threat Defense Market, by Offering
7. Mobile Threat Defense Market, by Operating System
8. Mobile Threat Defense Market, by Deployment
9. Mobile Threat Defense Market, by End-user
10. Americas Mobile Threat Defense Market
11. Asia-Pacific Mobile Threat Defense Market
12. Europe, Middle East & Africa Mobile Threat Defense Market
13. Competitive Landscape
14. Competitive Portfolio
15. Appendix

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 Mobile Threat Defense Market?
2. Which are the products/segments/applications/areas to invest in over the forecast period in the Mobile Threat Defense Market?
3. What is the competitive strategic window for opportunities in the Mobile Threat Defense Market?
4. What are the technology trends and regulatory frameworks in the Mobile Threat Defense Market?
5. What is the market share of the leading vendors in the Mobile Threat Defense Market?

6. What modes and strategic moves are considered suitable for entering the Mobile Threat Defense Market?

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

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

This press release can be viewed online at: <https://www.einpresswire.com/article/673763225>

EIN Presswire's priority is source transparency. We do not allow opaque clients, and our editors try to be careful about weeding out false and misleading content. As a user, if you see something we have missed, please do bring it to our attention. Your help is welcome. EIN Presswire, Everyone's Internet News Presswire™, tries to define some of the boundaries that are reasonable in today's world. Please see our Editorial Guidelines for more information.

© 1995-2023 Newsmatics Inc. All Right Reserved.