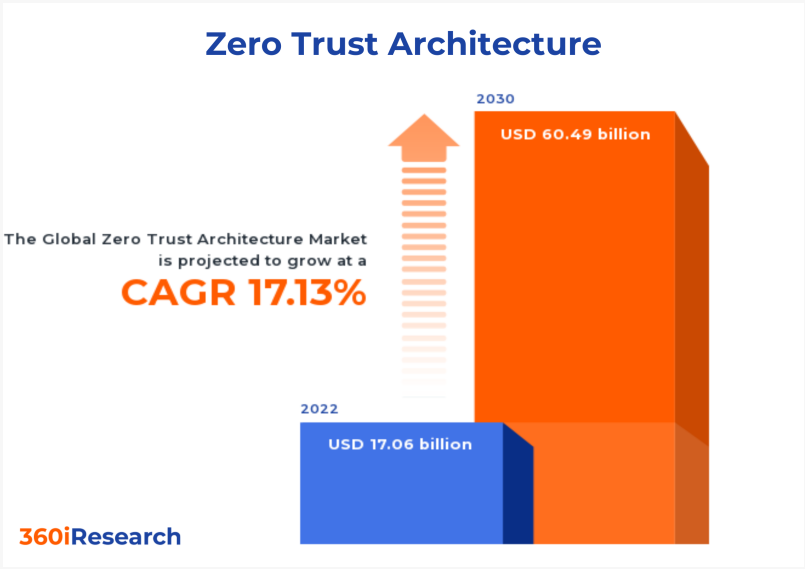
Zero Trust Architecture Market worth $60.49 billion by 2030- Exclusive Report by 360iResearch

The Global Zero Trust Architecture Market to grow from USD 17.06 billion in 2022 to USD 60.49 billion by 2030, at a CAGR of 17.13%.



Zero Trust Architecture Market - Exclusive Report by 360iResearch

PUNE, MAHARASHTRA, INDIA , December 7, 2023 /EINPresswire.com/ -- The "Zero Trust Architecture Market by Offering (Services, Solution), Deployment Mode (Cloud, On-Premises), Organization Size, Vertical - Global Forecast 2023-2030" report has been added to 360iResearch.com's offering.

The Global Zero Trust Architecture Market to grow from USD 17.06 billion in 2022 to USD 60.49 billion by 2030, at a CAGR of 17.13%.

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

Zero trust architecture represents a model for a more secure, modern approach to information systems and data security. This cyber-security strategy operates under the core principle of "never trust, always verify." Zero trust architecture is designed to combat the constant security threats in today's digital age by eradicating the concept of trust from an organization's network infrastructure. Zero trust architecture offers a diverse range of benefits for an organization. It provides enhanced security against data breaches by incorporating multi-factor authentication, micro-segmentation, and least-privilege controls. It improves compliance with regulations and standards by lowering the attack surface and limiting lateral movement within the network. The escalating cyber-attacks, increasing cloud-based solutions adoption, stringent data protection regulations, and the rapid digitization of industries increase the need for zero-trust architecture. However, the high cost of implementation and interoperability issues may hinder the market

growth. Moreover, integrating advanced technologies such as machine learning and blockchain can create a surge of new opportunities in this market.

Organization Size: Proliferating use of zero trust architecture in large enterprises
Cybercriminals constantly target large enterprises due to the abundance of valuable information. By adopting ZTA, they aim to create multi-layered defenses, decreasing the chances of large-scale breaches. Contrary to large enterprises, small and medium-sized enterprises (SMEs) often overlook their cybersecurity needs predominantly due to limited resources. However, the rising prevalence of cyber-attacks has made it essential for SMEs to explore affordable yet effective security solutions, such as ZTA. Large enterprises with extensive budgets and complex networks prefer providers offering advanced features and robust protection. However, the cost-sensitive nature of SMEs makes them lean towards providers capable of delivering budget-friendly and scalable solutions. Furthermore, in terms of recent launches, while large enterprise-focused products hinge on providing comprehensive security for intricate and extensive networks, SME-focused solutions stress affordability, scalability, and ease of use.

Vertical: Evolving use of zero trust architecture in banking, financial services, and insurance (BFSI) sector
The increasing instances of financial fraud and cyber threats have highlighted the importance of zero trust architecture in the banking, financial services, and insurance (BFSI) sector. This architecture offers enhanced data security to these institutions, minimizing the financial and reputational risks associated with security breaches. The energy and utilities sector has always been vulnerable to cyber threats due to their over-dependency on legacy systems. Adopting zero trust architecture helps companies ensure an unbreakable secure environment by providing a comprehensively segmented infrastructure. Government and defense sectors have a crucial need to protect their sensitive information. Hence, the adoption of zero trust architecture is escalating in this domain. This framework adds a security layer through its 'never trust and always verify' approach. The healthcare sector is increasingly adopting zero trust architecture to safeguard patients' sensitive data. This architectural model ensures the minimum privilege policy, allowing users access based on their needs and roles. IT & ITES providers are increasingly adopting zero trust architecture with a rise in the frequency and sophistication of cyber-attacks to safeguard their assets. Online transactions have become a cornerstone for the retail and e-commerce industry, which has amplified the need for advanced virtual protection, such as zero trust architecture. The sector benefits explicitly from the model's principle of least privilege (PoLP), which minimizes possible attack touchpoints.

Deployment Mode: Burgeoning adoption of cloud deployment due to its flexibility and cost-effectiveness
The cloud deployment mode of zero trust architecture enables businesses to adopt this security architecture in a virtual environment. This mode is preferred by organizations that want to reduce their investment in physical infrastructure. Cloud deployment allows for scalability, cost-effectiveness, and expedited deployment. On-premises is the traditional mode of deploying zero trust architecture wherein security controls are located within the organizational perimeter. It is

preferred by entities dealing with highly sensitive or confidential data, such as in government, financial, and healthcare services, due to its enhanced control and security. Cloud deployment offers flexibility, cost-effectiveness, and swift deployment, and trust in third-party services is essential. Contrastingly, on-premises deployment enables maximum control over security details, inducing trust, especially in sectors where data sensitivity is a primary concern.

Offering: Increasing utilization of solutions as they provide essential tools to secure organizational infrastructure
Services within zero trust architecture primarily focus on offering continuous support to businesses for effectively managing and maintaining their security infrastructure. These services can be bifurcated into professional and managed Services. Professional services include consulting, training, support, and implementation, while managed services concern outsourced security management. Solutions within zero trust architecture aimed at providing businesses with essential tools and technology to secure their infrastructure. The primary categories include network security, data security, endpoint security, and security analytics. Each solution is vital depending upon an organization's specific needs and vulnerabilities.

Regional Insights:
The Zero Trust Architecture (ZTA) market is evolving in the Americas owing to the increasing number of cyber attacks and the growing need for data security solutions. Rapid digital transformation and advancements in technology coupled with stringent data protection regulations are accelerating the use of Zero Trust Architecture (ZTA) solutions in the APAC region. The EU is one of the most proactive regions in implementing ZTA in response to growing threats such as phishing and ransomware attacks. The surge in investment in cybersecurity due to the increasing rate of cyber-attacks and ambitious digital transformation strategies is increasing demand for robust ZTA in the EMEA region. Besides, increasing emphasis on advancing zero trust architecture to ensure data security and compliance is anticipated to encourage the growth of the Zero Trust Architecture (ZTA) market worldwide.

FPNV Positioning Matrix:

The FPNV Positioning Matrix is essential for assessing the Zero Trust Architecture 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 Zero Trust Architecture 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 Zero Trust Architecture Market, highlighting leading vendors and their innovative profiles. These include Akamai Technologies, Inc., Appgate, Inc., Axis Cyber Security Ltd., Broadcom, Inc., Check Point Software Technologies Ltd., Cisco Systems, Inc., Cloud Software Group, Inc., Cloudflare Inc., CrowdStrike Holdings, Inc., Cyxtera Technologies, Inc., Czech company, FireEye, Inc., Forcepoint LLC, Fortinet, Inc., International Business Machines Corporation, Microsoft Corporation, Musarubra US LLC, Netskope, Inc., Okta, Inc., Palo Alto Networks, Inc., Perimeter 81 Ltd., Proofpoint, Inc., Twingate Inc., Versa Networks, Inc., VMware, Inc., and Zscaler, Inc..

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

Market Segmentation & Coverage:

This research report categorizes the Zero Trust Architecture 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 Solution. The Solution is projected to witness significant market share during forecast period.

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

Based on Organization Size, market is studied across Large Enterprises and Small and Medium-Sized Enterprises (SMEs). The Small and Medium-Sized Enterprises (SMEs) is projected to witness significant market share during forecast period.

Based on Vertical, market is studied across Banking, Financial Services, and Insurance (BFS|), Energy and Utilities, Government and Defense, Healthcare, IT & ITeS, and Retail and e-commerce. The Banking, Financial Services, and Insurance (BFS|) 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 38.25% 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 Zero Trust Architecture Market?
2. Which are the products/segments/applications/areas to invest in over the forecast period in the Zero Trust Architecture Market?
3. What is the competitive strategic window for opportunities in the Zero Trust Architecture Market?
4. What are the technology trends and regulatory frameworks in the Zero Trust Architecture

Market?
5. What is the market share of the leading vendors in the Zero Trust Architecture Market?
6. What modes and strategic moves are considered suitable for entering the Zero Trust Architecture Market?

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

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