Zero Trust Security: Redefining the Perimeter of Network Security | Says Evolve Business Intelligence

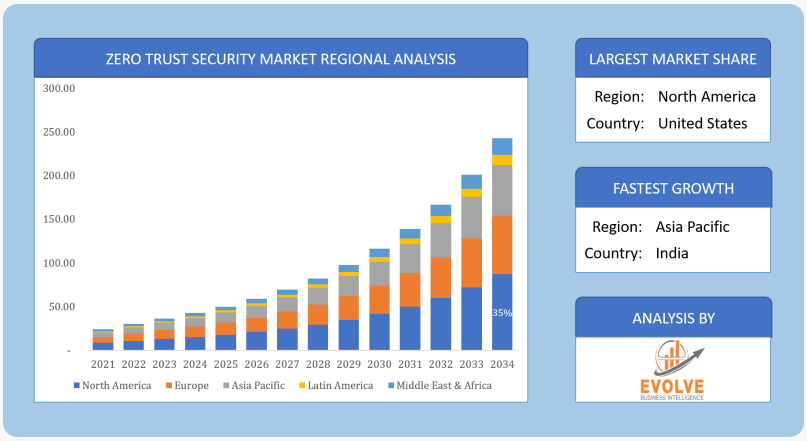
The Zero Trust Security Market, valued at USD 36.5 billion in 2023, is expected to grow at a compound annual growth rate (CAGR) of 18.21% from 2023 to 2033

INDIA, October 21, 2024 /EINPresswire.com/ -- The Zero Trust Security Market is experiencing rapid growth, driven by the increasing need for robust cybersecurity measures in an era of escalating cyber threats. Growing Incidents of Cyber Attacks are a primary driver, as organizations face sophisticated breaches and data theft. Shift to Remote Work has heightened the demand for secure access to corporate resources, necessitating zero-trust solutions. Regulatory Compliance Requirements are also pushing businesses to adopt stringent security frameworks to protect sensitive information. Advancements in Technologies such as AI and machine learning enhance the capabilities of zero trust security, providing more effective threat detection and response. Additionally, Increasing Adoption of Cloud Services requires organizations to implement zero-trust principles to secure their distributed environments and protect against unauthorized access.

Zero Trust Security Market Segment Analysis

For More Information: https://evolvebi.com/report/zero-trust-security-market-analysis/

Unlocking Growth Potential



Zero Trust Security Market Regional Analysis

The increasing implementation of Multi-Factor Authentication (MFA) is a significant driver in the Zero Trust Security market. As cyber threats become more sophisticated, relying solely on traditional passwords is no longer sufficient to secure sensitive information. MFA adds an extra layer of security by requiring multiple forms of verification, such as something the user knows (password), something the user has (security token), and something the user is (biometric verification). This approach significantly reduces the risk of unauthorized access, even if one factor is compromised. The rise in remote work and the adoption of cloud services further necessitate the use of MFA to protect against phishing attacks, credential theft, and other security breaches. Consequently, organizations are increasingly integrating MFA into their zero-trust security frameworks to enhance their overall cybersecurity posture and ensure secure access to critical resources.

The Future of Zero Trust Security Market

The surging demand for cloud-based zero-trust security solutions among SMEs presents significant opportunities in the zero-trust security market. As small and medium-sized enterprises increasingly adopt cloud services to enhance scalability and reduce IT costs, they require robust security measures to protect their distributed environments. Cloud-based zero-trust solutions offer flexible, scalable, and cost-effective security, making them ideal for SMEs with limited resources. This growing adoption creates a substantial market for providers to develop and offer tailored zero-trust security solutions that address the unique needs of SMEs, driving market growth.

For sample report pages - https://evolvebi.com/report/zero-trust-security-market-analysis/

North America to main its dominance by 2034

North America is expected to maintain its dominance in the Zero Trust Security market by 2034, driven by several key factors. The region's strong emphasis on advanced cybersecurity measures and significant investments in technology infrastructure contribute to this leadership. The high prevalence of cyber threats and stringent regulatory requirements compel organizations to adopt comprehensive zero-trust security frameworks. Additionally, the rapid digital transformation, including the widespread adoption of cloud services and remote work, further accelerates the demand for zero-trust solutions. The presence of leading cybersecurity firms and continuous innovation in security technologies also bolster North America's dominant position in the market.

Get access to the report - https://evolvebi.com/report/zero-trust-security-market-analysis/

Strategic Market Segments
“The cloud segment is expected to grow faster throughout the forecast period.
By deployment type, the market is segmented as (On-Premises, Cloud). The cloud sub-segment leads due to the growing shift towards cloud-based services and infrastructure. Organizations are increasingly adopting cloud solutions for their flexibility, scalability, and cost-effectiveness. The rise in remote work and digital transformation initiatives further drive the demand for cloud-based zero trust security solutions, which offer seamless integration and robust protection for distributed environments.”

“The Data Security segment is expected to grow faster throughout the forecast period.
By solution type, the market is segmented as (Network Security, Data Security, Endpoint Security, API Security, Security Analytics, and Others). The Data Security segment is anticipated to capture the largest market share, driven by the rising volume of sensitive data generated and stored by businesses and organizations. This trend, coupled with the increasing frequency of data breaches and cyber attacks, has resulted in a heightened emphasis on securing data.”

“The Multi-factor Authentication segment is expected to grow faster throughout the forecast period.
By authentication type, the market is segmented as (Single-factor Authentication, Multi-factor Authentication). MFA is the dominant sub-segment due to its enhanced security over single-factor authentication. By requiring multiple forms of verification, MFA significantly reduces the risk of unauthorized access, making it a crucial component of zero-trust security frameworks. The increasing frequency of credential-based attacks and regulatory requirements for stronger authentication mechanisms further drive the adoption of MFA.”

“The IT and ITES segment is expected to grow faster throughout the forecast period.
By vertical industry, the market is segmented as (IT and ITES, Financial and Insurance, Healthcare and Social Assistance, Retail Trade, Utilities, and Others). The IT and ITES (Information Technology and IT-enabled services) sector is the largest sub-segment because these industries are highly targeted by cyber threats and require advanced security measures to protect sensitive data and maintain service integrity. The rapid adoption of new technologies and the critical need for continuous operation in these sectors make zero trust security essential for mitigating risks and ensuring business continuity.”

Industry Leaders/ Market Dominators
Palo Alto Networks, Inc., Symantec Corporation, Okta Inc., Cisco Systems Inc., Akamai Technologies Inc., Microsoft, IBM, Sophos Group, Centrify Corporation, Cyxtera Technologies

Key Matrix for Latest Report Update
- Base Year: 2023
- Estimated Year: 2024

- CAGR: 2024 to 2034

About EvolveBI
Evolve Business Intelligence is a market research, business intelligence, and advisory firm providing innovative solutions to challenging pain points of a business. Our market research reports include data useful to micro, small, medium, and large-scale enterprises. We provide solutions ranging from mere data collection to business advisory.
Evolve Business Intelligence is built on account of technology advancement providing highly accurate data through our in-house AI-modelled data analysis and forecast tool – EvolveBI. This tool tracks real-time data including, quarter performance, annual performance, and recent developments from fortune's global 2000 companies.

Swapnil Patel
Evolve Business Intelligence
+91 63539 63987
email us here
Visit us on social media:
LinkedIn
