

Zero Trust Security Market to Surpass USD 82.97 billion by 2030 owing to Evolving Cyber Threats

Zero Trust Security Market size was valued at USD 24.12 billion in 2022 and is expected to grow to USD 82.97 billion By 2030 and grow at a CAGR of 16.7%

AUSTIN, TEXAS, UNITED STATES, January 25, 2024 /EINPresswire.com/ -- The SNS Insider report indicates that the [Zero Trust Security Market](#) was valued at USD 24.12 billion in 2022, and it is projected to achieve a market size of USD 82.97 billion by 2030, with a compound annual growth rate (CAGR) of 16.7 % expected over the forecast period from 2023 to 2030.

Zero-trust security is an emerging cybersecurity tactic that has attracted a lot of interest and approval. Based on the principle of 'never trust, always verify,' this approach assumes threats might originate from both internal and external sources. The need for zero-trust security solutions has surged as enterprises recognize the necessity to secure their networks, apps, and data amidst a complex and dynamic threat landscape. Organizations are prioritizing robust security measures like Zero Trust due to the escalating number and sophistication of cyber threats, including data breaches, ransomware attacks, and insider threats.

Get Full PDF Sample Copy of Report (Including TOC, List of Tables & Figures, Chart):@ <https://www.snsinsider.com/sample-request/2951>

Prominent Players:

- Check Point
- Akamai
- Microsoft
- Palo Alto Networks
- Illumio
- OKTA



- IBM
- Cyxtera Technologies
- ZScaler
- Forcepoint
- Google
- Trend Micro
- Cisco
- Broadcom
- Trellix
- RSA
- Centrify
- Sophos
- Cloudflare
- Qnext Corporation
- SonicWall
- VMware
- ON2IT
- Fortinet
- Varonis
- Pulse Secure

Market Analysis:

Organizations are searching for more complex security solutions, such zero-trust security, as a result of the growing threat of sophisticated cyberattacks. With attackers continually evolving their tactics, robust defenses against self-propagating malware and ransomware have become imperative. The rapid adoption of cloud technology and digital transformation is expanding the attack surface, necessitating the adoption of a “never trust, always verify” approach. Stringent regulatory compliance demands are compelling businesses to embrace Zero Trust to ensure data protection and mitigate potential breaches. Additionally, the diminishing effectiveness of traditional perimeter security in a mobile and interconnected world is driving the shift toward zero-trust security.

Segment Analysis:

In the realm of authentication types, multi-factor authentication (MFA) is experiencing explosive growth in the zero-trust security market. MFA is widely acknowledged for playing a crucial role in system security by limiting resource access to just authorised users. The endpoint security segment is projected to occupy the largest market share, benefiting from improved patch management, insider threat prevention, web content filtering, and streamlined cybersecurity.

The Zero Trust Security Market is segmented into five types on the basis of By Security Type, By Organization Size, By Deployment, By Authentication, and By Application.

By Security Type

- Network Security
- Data Security
- Endpoint Security
- Cloud Security
- Others

By Organization Size

- SMEs
- Large Enterprise

By Deployment

- On-premises
- Cloud

By Authentication

- Single-factor authentication
- Multi-factor authentication

By Application

- IT & Telecom
- BFSI
- Healthcare
- Retail
- Others

Key Regional Development:

The zero-trust security market in North America is witnessing rapid growth due to high cybersecurity awareness, comprehensive protection priorities, and the presence of major market players like Cisco, Palo Alto Networks, and Okta. Zero trust adoption is fueled by stringent regulatory requirements, including the CCPA and GDPR, for compliance. The early embrace of cloud computing in North America further fuels the need for robust security measures.

Key Takeaways for Zero Trust Security Market:

- Accelerated Growth: The market is poised for substantial growth, driven by the escalating

sophistication of cyber threats and the inadequacy of traditional security measures.

- Regional Emphasis: North America is at the forefront of zero-trust security adoption, emphasizing the need for comprehensive protection and compliance.
- Segment Dominance: Multi-factor authentication and endpoint security are pivotal segments, addressing critical security concerns and offering a multifaceted approach against unauthorized access.

Recent Developments:

- Microsoft and Samsung joined forces in July 2023 to enhance mobile device security, utilizing Microsoft Intune and Samsung Galaxy devices for hardware-backed device attestation.
- Zscaler and the Centre for Internet Security (CIS) established a strategic alliance in May 2023, leveraging the CIS CyberMarket to enhance cybersecurity for government entities.

Buy This Exclusive Report: @ <https://www.snsinsider.com/checkout/2951>

Zero Trust Security Market: Challenges and Opportunities

Challenges:

- Legacy System Integration: Implementing Zero Trust security may pose challenges in integrating with existing legacy systems, requiring careful planning to ensure a seamless transition without disruptions.
- User Adoption and Education: Overcoming resistance and ensuring user adoption of Zero Trust principles can be challenging, requiring effective communication and education on the benefits and changes in security practices.
- Continuous Monitoring Complexity: The continuous monitoring of user activities and devices across the network introduces challenges related to the complexity of managing and analyzing large volumes of security data.
- Strategic Shift in Security Culture: Adopting a Zero Trust approach involves a cultural shift in how organizations perceive and implement security, presenting challenges in aligning security practices with the new paradigm.

Opportunities:

- Advanced Authentication Solutions: Opportunities arise from the development and adoption of advanced authentication methods, such as biometrics and multifactor authentication, to strengthen access controls in a Zero Trust environment.
- Cloud-Based Security Solutions: Opportunities exist in leveraging cloud-based security solutions to facilitate the implementation of Zero Trust principles, providing scalability and flexibility in securing diverse environments.
- Integration with AI and Automation: Opportunities arise from integrating artificial intelligence and automation in Zero Trust security to enhance threat detection, response times, and overall

security posture.

- Industry-Specific Zero Trust Solutions: Providing industry-specific Zero Trust security solutions offers opportunities to tailor security measures to the unique needs and regulatory requirements of different sectors.

Successfully navigating these challenges and capitalizing on opportunities in the Zero Trust Security market requires a strategic approach, investment in advanced technologies, and a commitment to continuous education and communication on the evolving security landscape.

Table of Contents:

1. Introduction

1.1 Market Definition

1.2 Scope

1.3 Research Assumptions

2. Research Methodology

3. Market Dynamics

3.1 Drivers

3.2 Restraints

3.3 Opportunities

3.4 Challenges

4. Impact Analysis

4.1 Impact of the Ukraine- Russia war

4.2 Impact of ongoing Recession

4.2.1 Introduction

4.2.2 Impact on major economies

4.2.2.1 US

4.2.2.2 Canada

4.2.2.3 Germany

4.2.2.4 France

4.2.2.5 United Kingdom

4.2.2.6 China

4.2.2.7 Japan

4.2.2.8 South Korea

4.2.2.9 Rest of the World

5. Value Chain Analysis

6. Porter's 5 forces model

7. PEST Analysis

.....

13. Competitive Landscape

13.1 Competitive Benchmarking

13.2 Company Share Analysis

13.3 Recent Developments

- 13.3.1 Industry News
- 13.3.2 Company News
- 13.3.3 Mergers & Acquisitions
- 14. Use Case and Best Practices
- 15. Conclusion

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.

Akash Anand
SNS Insider | Strategy and Stats
+1 415-230-0044

[email us here](#)

Visit us on social media:

[Facebook](#)

[Twitter](#)

[LinkedIn](#)

[Instagram](#)

[YouTube](#)

This press release can be viewed online at: <https://www.einpresswire.com/article/683782208>

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.

© 1995-2024 Newsmatics Inc. All Right Reserved.