+357 96 030922
info@marketpublishers.com

Zero Trust Security Market Forecasts to 2030 – Global Analysis By Solution (Identity and Access Management (IAM), Multi-factor Authentication (MFA), Network Security, Endpoint Security and Other Solutions), Authentication Type, Deployment Type, Application and By Geography

https://marketpublishers.com/r/Z172B6B6CE97EN.html
Date: February 2025
Pages: 150
Price: US$ 4,150.00 (Single User License)
ID: Z172B6B6CE97EN

Abstracts

According to Stratistics MRC, the Global Zero Trust Security Market is accounted for $39.7 billion in 2024 and is expected to reach $102.5 billion by 2030 growing at a CAGR of 17.1% during the forecast period. Zero Trust Security is a cybersecurity model that assumes no user, device, or system—whether inside or outside the network—can be trusted by default. It requires continuous verification of identity, access rights, and security status before granting access to any resource. This approach minimizes the risk of security breaches by enforcing strict access controls, monitoring, and segmenting the network. Zero Trust focuses on the principle of 'never trust, always verify' to protect sensitive data and systems.

According to a Microsoft report from 2023, accounts with MFA are 99.9% less likely of getting compromised than those depending only on passwords.

Market Dynamics:

Driver:

Growing remote work trends

Zero Trust Security, which assumes no trust by default, ensures continuous verification

+357 96 030922
info@marketpublishers.com

and strict access controls for all users, regardless of their location. This paradigm is crucial as businesses seek to safeguard sensitive data from cyber threats and unauthorized access. As remote workforces expand, the need for solutions that authenticate users, devices, and networks before granting access becomes more pressing. Furthermore, the rise in cloud computing, which often supports remote work, aligns with the Zero Trust model's focus on protecting cloud infrastructure. Ultimately, these factors are propelling the growth of the Zero Trust Security market, as organizations adapt to evolving security needs in a distributed work environment.

Restraint:

High implementation costs

Sophisticated cyber-attacks, such as advanced persistent threats and zero-day vulnerabilities, make it harder to maintain robust security controls. As cybercriminals adopt increasingly sophisticated techniques, traditional security measures often fail, which in turn accelerates the need for constant updates and innovations within Zero Trust frameworks. Additionally, organizations face difficulties in seamlessly integrating Zero Trust with existing IT infrastructures. The complexity of maintaining real-time threat detection and response capabilities adds pressure on Zero Trust adoption. Consequently, these hurdles slow down the widespread implementation and growth of Zero Trust Security solutions.

Opportunity:

Government and defense sectors

The Government and defense sectors are prompting the adoption of Zero Trust models to enhance security protocols. Zero Trust, with its focus on strict identity verification, ensures only authorized users can access vital systems, reducing insider threats. Governments worldwide are investing heavily in Zero Trust to comply with increasingly stringent cybersecurity regulations. The rise in cyberattacks targeting defense systems further accelerates the demand for robust Zero Trust solutions. Consequently, these sectors are a significant catalyst for the market's expansion, shaping cybersecurity strategies for national security and defense operations.

Threat:

Evolving cyber threat landscape

+357 96 030922
info@marketpublishers.com

Cybercriminals are leveraging advanced tactics, making traditional security models less effective and increasing the demand for adaptive Zero Trust solutions. However, as the landscape evolves, Zero Trust solutions need continuous updates to address new vulnerabilities, which can lead to delays in implementation. Budget constraints and a shortage of skilled cybersecurity professionals can hinder the adoption of Zero Trust models. Additionally, the integration of Zero Trust across diverse IT environments adds complexity and may cause resistance from organizations with legacy systems. Lastly, the growing threat of insider attacks and advanced persistent threats (APTs) challenges Zero Trust's ability to provide comprehensive protection across all levels of an organization.

Covid-19 Impact

The COVID-19 pandemic significantly accelerated the adoption of Zero Trust Security as businesses shifted to remote work models. With increased cybersecurity threats and vulnerabilities due to the rapid transition, organizations prioritized securing networks with a Zero Trust approach. The market saw a surge in demand for solutions that offer continuous authentication and access control, ensuring only authorized users and devices can access sensitive data. The shift to cloud-based services further boosted the market, as traditional security models became inadequate for decentralized operations.

The single-factor authentication segment is expected to be the largest during the forecast period

The single-factor authentication segment is estimated to have a lucrative growth by emphasizing identity verification as a key component of access control. Although it is a basic form of authentication, it serves as a foundational layer in Zero Trust models, ensuring that users are properly authenticated before gaining access to sensitive resources. SFA is essential for organizations transitioning to Zero Trust architectures, offering a starting point for secure access management. However, its limitations push companies toward adopting more advanced methods, such as multi-factor authentication (MFA), to enhance security. As a result, the need for comprehensive access controls in Zero Trust strategies fuels demand for authentication solutions, contributing to the market's growth.

The healthcare segment is expected to have the highest CAGR during the forecast period

+357 96 030922
info@marketpublishers.com

The healthcare segment is anticipated to witness the highest CAGR growth during the forecast period, due to the increasing need to protect sensitive patient data. With the rise in cyberattacks targeting healthcare organizations, implementing Zero Trust frameworks ensures that all users, devices, and applications are continuously verified, even within the network. Zero Trust security models, by default, minimize the attack surface, reducing the potential entry points for malicious actors. Furthermore, the healthcare industry's shift toward digital health records, telemedicine, and IoT devices increases the need for a comprehensive security approach. As regulatory requirements around patient data privacy tighten, healthcare providers are increasingly adopting Zero Trust to ensure compliance and safeguard critical information.

Region with largest share:

Asia Pacific is expected to hold the largest market share during the forecast period due to increasing cybersecurity threats and the region's fast-paced digital transformation. Organizations across industries, including BFSI, healthcare, and IT, are adopting Zero Trust models to mitigate risks associated with cloud adoption and remote work. Governments in countries like China, India, and Australia are introducing stringent data protection regulations, further driving demand for advanced security solutions. Key players are expanding their presence and forming strategic partnerships to cater to the region's growing need for robust security frameworks. The market is expected to witness sustained growth, fueled by investments in AI-driven security technologies and a focus on securing critical infrastructure.

Region with highest CAGR:

North America is expected to have the highest CAGR over the forecast period, owing to the increasing adoption of cloud computing and the rising prevalence of cyber threats. Organizations across various sectors are embracing Zero Trust principles to ensure robust security frameworks, driven by regulatory compliance requirements and the need to safeguard sensitive data. The region's advanced IT infrastructure and high adoption of innovative technologies contribute to its market leadership. Key players are investing heavily in R&D and partnerships to enhance their offerings and address evolving cybersecurity challenges. The rapid digital transformation and hybrid work models further amplify the demand for Zero Trust Security solutions in North America.

Key players in the market

Some of the key players profiled in the Zero Trust Security Market include Cisco

+357 96 030922
info@marketpublishers.com

Systems, Inc., Palo Alto Networks, Inc., Zscaler, Inc., Okta, Inc., Forcepoint, LLC, SonicWall, Inc., Check Point Software Technologies Ltd., Microsoft Corporation, CrowdStrike Holdings, Inc., Fortinet, Inc., VMware, Inc., IBM Corporation, Illumio, Inc., CyberArk Software Ltd., Tanium Inc. and Proofpoint, Inc.

Key Developments:

In December 2024, Cisco partnered with AppOmni to enhance SaaS security by integrating AppOmni's Zero Trust Posture Management (ZTPM) solution with Cisco's Security Service Edge (SSE). This collaboration aims to provide comprehensive zero trust principles at the application layer for SaaS applications, improving visibility and security across complex installations.

In November 2024, Cisco continues to advance its Zero Trust offerings by integrating various solutions such as Duo Security, Identity Services Engine (ISE), and Secure Workload into a cohesive framework. These solutions are designed to enforce strict access controls based on user identity and context, essential for maintaining security in a hybrid work environment.

Solutions Covered:

- Identity and Access Management (IAM)
- Multi-factor Authentication (MFA)
- Network Security
- Endpoint Security
- Security Information and Event Management (SIEM)
- Data Loss Prevention (DLP)
- Encryption
- Next-Generation Firewalls (NGFW)
- Cloud Security

+357 96 030922
info@marketpublishers.com

Security Analytics

Other Solutions

Authentication Types Covered:

Single-Factor Authentication

Multi-Factor Authentication

Deployment Types Covered:

On-premises

Cloud-based

Hybrid

Applications Covered:

Banking, Financial Services, and Insurance

Healthcare

IT & Telecom

Retail

Government and Defense

Manufacturing

Energy and Utilities

Education

+357 96 030922
info@marketpublishers.com

- Other Applications

Regions Covered:

- North America
  - US
  - Canada
  - Mexico
- Europe
  - Germany
  - UK
  - Italy
  - France
  - Spain
  - Rest of Europe
- Asia Pacific
  - Japan
  - China
  - India
  - Australia
  - New Zealand

+357 96 030922
info@marketpublishers.com

South Korea

Rest of Asia Pacific

South America

Argentina

Brazil

Chile

Rest of South America

Middle East & Africa

Saudi Arabia

UAE

Qatar

South Africa

Rest of Middle East & Africa

What our report offers:
- Market share assessments for the regional and country-level segments
- Strategic recommendations for the new entrants
- Covers Market data for the years 2022, 2023, 2024, 2026, and 2030
- Market Trends (Drivers, Constraints, Opportunities, Threats, Challenges, Investment Opportunities, and recommendations)
- Strategic recommendations in key business segments based on the market estimations
- Competitive landscaping mapping the key common trends
- Company profiling with detailed strategies, financials, and recent developments
- Supply chain trends mapping the latest technological advancements

+357 96 030922
info@marketpublishers.com

Free Customization Offerings:

All the customers of this report will be entitled to receive one of the following free customization options:

- Company Profiling
  - Comprehensive profiling of additional market players (up to 3)
  - SWOT Analysis of key players (up to 3)
- Regional Segmentation
  - Market estimations, Forecasts and CAGR of any prominent country as per the client's interest (Note: Depends on feasibility check)
- Competitive Benchmarking
  - Benchmarking of key players based on product portfolio, geographical presence, and strategic alliances

+357 96 030922
info@marketpublishers.com

Contents

+357 96 030922
info@marketpublishers.com

+357 96 030922
info@marketpublishers.com

9 GLOBAL ZERO TRUST SECURITY MARKET, BY GEOGRAPHY

10 KEY DEVELOPMENTS

+357 96 030922
info@marketpublishers.com

11 COMPANY PROFILING

+357 96 030922
info@marketpublishers.com

List Of Tables

LIST OF TABLES

+357 96 030922
info@marketpublishers.com

Note: Tables for North America, Europe, APAC, South America, and Middle East & Africa Regions are also represented in the same manner as above.

+357 96 030922
info@marketpublishers.com

I would like to order

Product name: Zero Trust Security Market Forecasts to 2030 – Global Analysis By Solution (Identity and Access Management (IAM), Multi-factor Authentication (MFA), Network Security, Endpoint Security and Other Solutions), Authentication Type, Deployment Type, Application and By Geography

Product link: https://marketpublishers.com/r/Z172B6B6CE97EN.html

Price: US$ 4,150.00 (Single User License / Electronic Delivery)

If you want to order Corporate License or Hard Copy, please, contact our Customer Service:
info@marketpublishers.com

Payment

To pay by Credit Card (Visa, MasterCard, American Express, PayPal), please, click button on product page https://marketpublishers.com/r/Z172B6B6CE97EN.html