+357 96 030922
info@marketpublishers.com

Zero Trust Networks Market Forecasts to 2034 – Global Analysis By Component (Solutions and Services), Solution Type, Deployment Mode, Organization Size, Application, End User and By Geography

https://marketpublishers.com/r/Z6B3D7E2833EEN.html
Date: June 2026
Pages: 200
Price: US$ 4,150.00 (Single User License)
ID: Z6B3D7E2833EEN

Abstracts

According to Stratistics MRC, the Global Zero Trust Networks Market is accounted for $32.4 billion in 2026 and is expected to reach $98.3 billion by 2034 growing at a CAGR of 14.8% during the forecast period. Zero-trust networks refer to a cybersecurity architecture paradigm and associated technology platforms implementing the principle that no user, device, application, or network segment is inherently trusted, regardless of its physical or network location, requiring continuous verification of identity, device health, and contextual access legitimacy for every access request to enterprise resources. These platforms encompass zero trust network access solutions replacing traditional VPN architectures with identity-aware application access proxies, software-defined perimeter platforms establishing dynamically provisioned encrypted tunnels for verified entities, micro-segmentation systems dividing network environments into granular security zones preventing lateral movement, identity and access management platforms with continuous authentication and adaptive risk-based access policies, device trust and endpoint security posture assessment, and cloud access security broker solutions governing SaaS application access.

Market Dynamics:

Driver:

Remote work architecture and cloud migration security requirements

+357 96 030922
info@marketpublishers.com

The structural shift to hybrid and remote work, eliminating the defined corporate network perimeter that traditional castle-and-moat security architectures were designed to protect, combined with enterprise application migration to cloud and SaaS platforms operating outside the corporate network boundary, has rendered conventional perimeter-based network security architectures fundamentally insufficient for protecting modern distributed enterprise IT environments. Government cybersecurity mandates, including the US Executive Order on Cybersecurity requiring federal agency zero trust architecture adoption and CISA zero trust maturity model implementation guidance, are creating compliance-driven zero trust investment programs that are establishing procurement frameworks influencing private sector enterprise adoption across regulated industries.

Restraint:

Implementation complexity and user experience disruption

Comprehensive zero trust architecture implementation across large enterprise IT environments requiring identity integration, device enrollment, application onboarding, and policy configuration across hundreds of applications and thousands of users creates substantial implementation complexity that extends deployment timelines significantly beyond initial business case projections. Overly restrictive zero trust access policies creating authentication friction, excessive re-verification prompts, and legitimate access denial incidents generate workforce productivity complaints and executive pushback that can create program scope reduction pressure and partial rollback of deployed zero trust controls. The multi-vendor integration complexity of comprehensive zero trust architectures spanning identity, network, endpoint, and application security platforms requires specialized implementation expertise that is scarce in the cybersecurity talent market.

Opportunity:

Operational technology and industrial network zero trust expansion

Extension of zero trust architecture principles to operational technology networks managing industrial control systems, critical infrastructure, and manufacturing automation environments represents a large and rapidly growing addressable market as IT-OT network convergence expands cyber-attack surface exposure of previously air-gapped industrial systems. Zero-trust micro-segmentation and device identity verification solutions adapted for the deterministic communication patterns, legacy

+357 96 030922
info@marketpublishers.com

protocol constraints, and safety-critical availability requirements of industrial OT environments are commanding premium pricing from critical infrastructure operators facing mandatory OT cybersecurity compliance requirements. Government investment in critical infrastructure zero trust programs is creating institutional procurement channels for OT-specialized zero trust platform providers.

Threat:

Identity provider and zero trust platform concentration risk

The strategic dependence of enterprise zero trust architectures on identity platform providers, including Microsoft Azure Active Directory, Okta, and Ping Identity for the continuous authentication and policy enforcement intelligence that zero trust frameworks require creates platform concentration risks where identity provider security incidents, pricing increases, or service disruptions can simultaneously compromise or disable enterprise-wide zero trust access controls. Single identity provider dependency amplifying the blast radius of identity system compromises is recognized as a systemic zero trust architecture vulnerability that is difficult to address without complex multi-identity provider architectures that introduce their own management complexity and policy consistency challenges.

Covid-19 Impact:

The pandemic forced emergency remote access architecture deployment for millions of workers simultaneously, which exposed the scaling limitations and security inadequacies of traditional VPN-based network access, creating urgent enterprise recognition of zero-trust network access as the required architectural successor. Government pandemic cybersecurity emergency guidance explicitly recommending zero trust approaches for securing remote workforce access accelerated both enterprise and public sector zero trust adoption programs. Post-pandemic, permanent hybrid work embedding remote access as a permanent operational requirement has sustained structural enterprise investment in zero-trust network architecture transformation.

The services segment is expected to be the largest during the forecast period

The services segment is expected to account for the largest market share during the forecast period, due to the substantial professional services, managed zero trust operations, architecture advisory, implementation, and ongoing policy management services revenue generated by enterprise zero trust transformation programs. The

+357 96 030922
info@marketpublishers.com

architectural complexity of enterprise zero trust deployments spanning identity, network, endpoint, and application security domains requires extensive specialist implementation and ongoing managed services engagement that generates multi-year service revenue substantially exceeding software platform licensing across the enterprise security program lifecycle.

The agent-based ZTNA segment is expected to have the highest CAGR during the forecast period

Over the forecast period, the agent-based ZTNA segment is predicted to witness the highest growth rate, driven by the superior security posture and device health visibility that endpoint agent-based zero trust network access provides compared to agentless browser-based alternatives, making it the preferred deployment model for managed enterprise devices where endpoint agent installation is operationally feasible. Agent-based ZTNA platforms enabling continuous device posture assessment, user behavior analytics, and real-time access policy enforcement based on device health signals represent the highest-security zero trust access implementation that large enterprise and government sector organizations with stringent security requirements are prioritizing.

Region with largest share:

During the forecast period, the North America region is expected to hold the largest market share, due to the US federal government's zero trust mandate creating the largest single government zero trust procurement program globally, combined with the highest private sector cybersecurity investment and concentration of leading zero trust platform vendors. The United States financial services, healthcare, and technology sectors represent the highest-value enterprise zero trust adoption concentrations, driving continuous platform innovation.

Region with highest CAGR:

Over the forecast period, the Europe region is anticipated to exhibit the highest CAGR, due to the NIS2 Directive mandatory cybersecurity requirements for essential entities creating regulatory compliance-driven zero trust adoption across European critical infrastructure, financial services, and digital service provider sectors. European enterprise zero trust adoption is additionally driven by DORA financial sector operational resilience requirements and national cybersecurity agency zero trust guidance from ENISA, ANSSI, and BSI, creating consistent regulatory momentum across EU member

+357 96 030922
info@marketpublishers.com

state markets.

Key players in the market

Some of the key players in Zero Trust Networks Market include Zscaler Inc., Palo Alto Networks Inc., Cisco Systems Inc., Microsoft Corporation, Akamai Technologies Inc., Cloudflare Inc., Netskope Inc., Okta Inc., Fortinet Inc., Check Point Software Technologies Ltd., CrowdStrike Holdings Inc., Vmware Inc., Iboss Inc., Appgate Inc., Forcepoint LLC, Broadcom Inc., and Juniper Networks Inc..

Key Developments:

In March 2026, Zscaler Inc. launched an AI-powered zero trust platform with generative AI security policy configuration, automated anomaly detection, and autonomous threat containment for enterprise and government zero trust architecture programs.

In February 2026, Cloudflare Inc. introduced a zero-trust OT security platform extending ZTNA and micro-segmentation capabilities to industrial control networks with support for legacy Modbus, DNP3, and PROFINET operational technology protocols.

In January 2026, Palo Alto Networks Inc. released an AI-powered continuous identity verification platform integrating behavioral biometrics and device trust signals for adaptive zero-trust access policy enforcement without user authentication friction.

Components Covered:

- Solutions
- Services

Solution Types Covered:

- Agent-Based ZTNA
- Agentless ZTNA
- Universal ZTNA

+357 96 030922
info@marketpublishers.com

Micro-Segmentation

Software-Defined Perimeter

Deployment Modes Covered:

Cloud

On-Premises

Hybrid

Organization Sizes Covered:

Large Enterprises

Small & Medium Enterprises

Applications Covered:

Remote Workforce Access

Third-Party & BYOD Access

Private Application Access

Workload-to-Workload & API Access

Data Center & Cloud Workload Protection

End Users Covered:

BFSI

Government & Defense

+357 96 030922
info@marketpublishers.com

- IT & Telecom
- Healthcare
- Retail & E-Commerce
- Manufacturing
- Energy & Utilities
- Media & Entertainment

Regions Covered:

- North America
  - United States
  - Canada
  - Mexico
- Europe
  - United Kingdom
  - Germany
  - France
  - Italy
  - Spain
  - Netherlands
  - Belgium

+357 96 030922
info@marketpublishers.com

- Sweden
- Switzerland
- Poland
- Rest of Europe

Asia Pacific

- China
- Japan
- India
- South Korea
- Australia
- Indonesia
- Thailand
- Malaysia
- Singapore
- Vietnam
- Rest of Asia Pacific

South America

- Brazil
- Argentina

+357 96 030922
info@marketpublishers.com

- Colombia
- Chile
- Peru
- Rest of South America

- Rest of the World (RoW)
  - Middle East
    - Saudi Arabia
    - United Arab Emirates
    - Qatar
    - Israel
    - Rest of Middle East
  - Africa
    - South Africa
    - Egypt
    - Morocco
    - Rest of 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 2023, 2024, 2025, 2026, 2027, 2028, 2030, 2032 and 2034
- Market Trends (Drivers, Constraints, Opportunities, Threats, Challenges, Investment

+357 96 030922
info@marketpublishers.com

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

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

+357 96 030922
info@marketpublishers.com

+357 96 030922
info@marketpublishers.com

14 COMPANY PROFILES

+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 Rest of the World (RoW) 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 Networks Market Forecasts to 2034 – Global Analysis By Component (Solutions and Services), Solution Type, Deployment Mode, Organization Size, Application, End User and By Geography

Product link: https://marketpublishers.com/r/Z6B3D7E2833EEN.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/Z6B3D7E2833EEN.html