

Zero Trust Security - Market Share Analysis, Industry Trends & Statistics, Growth Forecasts 2019 - 2029

Market Report | 2024-02-17 | 159 pages | Mordor Intelligence

AVAILABLE LICENSES:

- Single User License \$4750.00
- Team License (1-7 Users) \$5250.00
- Site License \$6500.00
- Corporate License \$8750.00

Report description:

The Zero Trust Security Market size is estimated at USD 33.07 billion in 2024, and is expected to reach USD 72.01 billion by 2029, growing at a CAGR of 16.84% during the forecast period (2024-2029).

Key Highlights

-A developing cybersecurity strategy called zero trust security has attracted a lot of attention and acceptance in recent years. The zero trust approach is predicated on the maxim 'never trust, always verify,' which makes assumptions that threats might originate from internal and external sources. The need for zero-trust security solutions has increased as enterprises increasingly acknowledge the need to secure their networks, apps, and data in an environment with a more complex and dynamic threat landscape.

-Organizations are concentrating more on implementing strong security measures like Zero Trust due to the increased number and sophistication of cyber threats, including data breaches, ransomware attacks, and insider threats. The popularity of remote work was accelerated by the COVID-19 pandemic, increasing the attack surface. Zero trust is a crucial strategy for protecting distributed and remote workforces.

-Organizations have had to review their security postures due to the move toward cloud computing. Zero trust facilitates secure access to cloud-based apps and data, which fits well with cloud-first plans. Organizations must develop robust data protection mechanisms to comply with strict data privacy laws like GDPR and CCPA, making zero trust a compliance enabler. Businesses use the zero trust framework in various sectors more widely as a fundamental security strategy. The conventional perimeter-based paradigm is being abandoned. Big technology corporations are buying zero trust security businesses to improve security services.

-Organizations are incorporating zero trust concepts into their DevOps pipelines as they adopt DevOps strategies to ensure security is a part of the development process. A significant increase has been observed in the secure remote access-focused zero trust network access (ZTNA) sector. This is particularly pertinent given the prevalence of remote work and the requirement for

Scotts International. EU Vat number: PL 6772247784

tel. 0048 603 394 346 e-mail: support@scotts-international.com

www.scotts-international.com

safe access to company resources. A thorough zero trust strategy's implementation can be challenging and time-consuming. Identity and access management, network security, and analytics are a few components that organizations need to plan and integrate.

-Zero trust is crucial for security, but businesses must strike a balance between strict security measures and a smooth, effective user experience. Finding the ideal balance is difficult. Many businesses continue to use outdated architectures and systems that make it difficult to implement zero-trust principles. Migrating away from these systems can take time and effort. The compromise of user credentials and insider threats remain major security worries. Phishing and other social engineering assaults are still common attack methods.

-The constantly changing threat landscape and the demand for thorough security measures have led to a major increase in the global zero-trust security market. However, enterprises have a big problem because of outdated operating systems, infrastructure, and applications. The wider market adoption needs to be improved by the resistance of these antiquated components to adopt the zero trust concept.

-The COVID-19 pandemic had a positive impact, providing a contactless payment mode, including online and in-person transactions. This has included the digital infrastructure extensively, exposing the financial system to cybersecurity vulnerabilities, which created considerable demand for fool-proof security models like zero trust security. For instance, according to RBI, approximately 71 billion digital payments were made throughout India in fiscal year 2022. This was a significant increase over the preceding three years.

Zero Trust Security Market Trends

BFSI Sector to be the Largest End User

- The International Monetary Fund (IMF) reveals that financial and technological interconnections within the banking, financial services, and insurance (BFSI) sector facilitate the rapid spread of cyberattacks, causing widespread disruption and loss of critical information throughout the entire financial ecosystem. Cybersecurity is a significant threat to financial stability, especially among the developing economies.

- A recent IMF survey of 51 countries states that most financial supervisors in emerging markets still need to introduce cybersecurity regulations or build resources to enforce them. The survey highlights that 56% of the central bank authorities need a national cyber strategy, 42% lack a dedicated cybersecurity or risk-management regulation, 68% lack a specialized risk unit, and 64% do not mandate testing and exercising cyber security measures.

- According to IBM's 'Cost of a Data Breach 2022' report, 2022 witnessed a surge in data breaches. The average data breach cost reached USD 4.35 million in the same year, marking a 2.6% increment from 2021. The report also states that 83% of organizations, including banks, reported more than one data breach in 2022.

- Cloud deployments are gaining rapid popularity in the global banking and financial sector as banks and financial institutions migrate their platforms to the cloud. With the rise of hybrid cloud, businesses increasingly appreciate the advantages of diversifying their services across multiple cloud providers. A multi-cloud approach and rapid increase of internet services enable more and more consumers to use the internet and mobile applications for transactions.

- Large enterprises dominate the BFSI industry, one of the most important sectors of the global economy. Several large retail banking, commercial banking, and investment banking organizations are taking a zero-trust approach to cybersecurity to help secure the ubiquitous nature of modern enterprises and meet the challenges caused by evolving business models. As per The State of Zero Security 2022, the implementation of zero trust security by organizations in the BFSI sector is expected to increase significantly.

North America is Expected to Hold Significant Market Share

Scotts International. EU Vat number: PL 6772247784

tel. 0048 603 394 346 e-mail: support@scotts-international.com

www.scotts-international.com

- The United States is a developed economy with a significant inclination towards implementing and accepting advanced technology, development in network automation, and the surge in cloud-based services, thereby contributing to the zero trust security market. Moreover, the growing digitization among end-user industries, coupled with the presence of prominent market vendors Cisco Systems, Inc., IBM Corporation, VMware Inc., Palo Alto Networks, and Akamai Technologies, contribute to the market's growth.
- Cyber attackers with a typical target go after end-point devices, cloud-based applications, networks, and other IT infrastructure components. The primary motive behind such attacks is to steal critical information. These attacks can result in business disruptions, financial loss, intellectual property theft, and critical and sensitive customer information loss. The US federal government is making a big push toward zero trust. In January 2023, the Office of Management and Budget released a memorandum that mandates a federal zero trust architecture (ZTA) strategy, directing agencies to meet specific cyber security measures and objectives by the end of the fiscal year 2024. This initiative reinforces the government's defenses against increasingly sophisticated and persistent threat campaigns.
- Further, the rapid adoption of new technology in the country and growing focus on security is pushing the demand for security-as-a-service forward. Industries, such as banking, healthcare, and government organizations, which hold databases of sensitive information, are preferred targets for hackers owing to the huge amount of information contained. Credit card data and social security numbers of individuals are the targeted information attacked by the hackers. To safeguard such critical data, there is a need for robust cloud intrusion protection and security solutions, along with suitable network security solutions. This is analyzed to boost the demand for zero-trust solutions in the coming years.
- The United States marked the increase of ransomware and phishing attacks targeted at organizations that involved less manual effort and were highly automated in 2021. According to Emsisoft's year-end report published in January 2023, Schools sustained almost the same number of cyberattacks in 2022 as in 2021, despite the US government's efforts to thwart the threat. Market vendors in the country are indulging in partnership activities to provide customers with an efficient and robust secure access service edge offering to secure and accelerate their digital transformation projects. For instance, in July 2023, Netskope, a Secure Access Service Edge (SASE) provider, announced a new collaboration with Wipro Limited to deliver Managed Zero Trust Network Access (ZTNA) and robust cloud-native Managed Secure Access Service Edge (SASE) services to Wipro's extensive global enterprise client portfolio.
- Overall, the zero trust market in North America is analyzed to witness substantial growth in coming years, primarily governed by the increasing cloud migration in end-user industries, coupled with the growing presence of cloud service and Zero Trust market vendors. In addition, the continuous launch of new solutions with enhanced features and growing partnership activities among market vendors will drive the growth of the market in the coming years. Moreover, there is huge growth potential from other industry segments in the Region, such as manufacturing, energy, and utilities, as they have already migrated to digital-transformed methods of operations and are now beginning to get a better understanding.

Zero Trust Security Industry Overview

The zero trust security market features a competitive landscape with global and regional players such as Cisco Systems Inc., Palo Alto Networks Inc., VMware Inc., Broadcom Inc., and Microsoft Corporation vying for market share. Despite significant barriers to entry, some new entrants have managed to gain a foothold in this space.

This market is characterized by a moderate to high degree of product differentiation, a growing level of product adoption, and intense competition. Typically, solutions are bundled together, creating a consolidated offering that appears integral to the overall service or product.

Many users opt for annual contracts to reduce costs, and there is a growing trend of companies seeking services that offer faster

Scotts International. EU Vat number: PL 6772247784

tel. 0048 603 394 346 e-mail: support@scotts-international.com

www.scotts-international.com

security updates. This has fueled a rising demand for cloud-based services, which enable real-time updates and are favored by service-based industries.

For instance, in July 2023, Microsoft Entra made significant strides in the Security Service Edge (SSE) arena, introducing two innovative products: Microsoft Entra Internet Access and Microsoft Entra Private Access. These cloud-based services are known for their agility, easy management, and cost-effectiveness when compared to traditional on-premises systems. They adhere to Zero Trust principles, verifying each user's identity and employing risk-based contextual information to grant access only to the necessary applications, resources, and destinations, ensuring optimal security without compromising productivity.

In June 2023, Cisco Systems expanded its security portfolio by unveiling a new Security Service Edge (SSE) solution called Cisco Secure Access. This solution facilitates an efficient hybrid work environment, simplifying access across different locations, devices, and applications. Cisco Secure Access offers frictionless access to all applications, fostering secure hybrid work settings. The solution streamlines security operations by consolidating multiple functions into a user-friendly solution that safeguards all traffic. This not only enhances efficiency and reduces costs but also adds flexibility to the IT environment.

Additional Benefits:

- The market estimate (ME) sheet in Excel format
- 3 months of analyst support

Table of Contents:

1 INTRODUCTION

- 1.1 Study Assumptions and Market Definition
- 1.2 Scope of the Study

2 RESEARCH METHODOLOGY

3 EXECUTIVE SUMMARY

4 MARKET INSIGHT

- 4.1 Market Overview
- 4.2 Industry Attractiveness - Porter's Five Forces Analysis
 - 4.2.1 Bargaining Power of Suppliers
 - 4.2.2 Bargaining Power of Buyers
 - 4.2.3 Threat of New Entrants
 - 4.2.4 Threat of Substitutes
 - 4.2.5 Intensity of Competitive Rivalry
- 4.3 Impact of COVID-19
- 4.4 Industry Value Chain Analysis
- 4.5 Technology Snapshot
 - 4.5.1 Zero Trust Networks
 - 4.5.2 Zero Trust Devices
 - 4.5.3 Zero Trust Data
 - 4.5.4 Zero Trust Identities
 - 4.5.5 Zero Trust Applications (Visibility and Analytics)

5 MARKET DYNAMICS

Scotts International. EU Vat number: PL 6772247784

tel. 0048 603 394 346 e-mail: support@scotts-international.com

www.scotts-international.com

5.1 Market Drivers

5.1.1 Increasing Number of Data Breaches

5.1.2 Security Perimeter of an Organization not Being Limited to Workplace

5.2 Market Restraints

5.2.1 Legacy Applications, Infrastructure, and Operating Systems Not Likely to Adopt Zero Trust Model

6 MARKET SEGMENTATION

6.1 By Deployment

6.1.1 On-premise

6.1.2 Cloud

6.2 By Organization Size

6.2.1 Small and medium Enterprises

6.2.2 Large Enterprises

6.3 By End-user Industry

6.3.1 IT and Telecom

6.3.2 BFSI

6.3.3 Manufacturing

6.3.4 Healthcare

6.3.5 Energy and Power

6.3.6 Retail

6.3.7 Government

6.3.8 Other End-user Industries

6.4 By Geography

6.4.1 North America

6.4.2 Europe

6.4.3 Asia Pacific

6.4.4 Rest of the World

7 COMPETITIVE LANDSCAPE

7.1 Company Profiles*

7.1.1 Cisco Systems Inc.

7.1.2 Palo Alto Networks, Inc.

7.1.3 Vmware, Inc.

7.1.4 Broadcom Inc. (Symantec Corporation)

7.1.5 Microsoft Corporation

7.1.6 IBM Corporation

7.1.7 Google LLC (Alphabet Inc.)

7.1.8 Check Point Software Technologies Ltd

7.1.9 BlackBerry Limited

7.1.10 Akamai Technologies Inc.

7.1.11 DELINEA (Centrify Corporation)

7.1.12 Okta Inc.

7.1.13 Fortinet, Inc.

7.1.14 Sophos Ltd.

7.1.15 Cyxtera Technologies Inc.

8 INVESTMENT ANALYSIS

Scotts International. EU Vat number: PL 6772247784

tel. 0048 603 394 346 e-mail: support@scotts-international.com

www.scotts-international.com

Zero Trust Security - Market Share Analysis, Industry Trends & Statistics, Growth Forecasts 2019 - 2029

Market Report | 2024-02-17 | 159 pages | Mordor Intelligence

To place an Order with Scotts International:

- ☐ - Print this form
- ☐ - Complete the relevant blank fields and sign
- ☐ - Send as a scanned email to support@scotts-international.com

ORDER FORM:

Select license	License	Price
	Single User License	\$4750.00
	Team License (1-7 Users)	\$5250.00
	Site License	\$6500.00
	Corporate License	\$8750.00
		VAT
		Total

*Please circle the relevant license option. For any questions please contact support@scotts-international.com or 0048 603 394 346.

** VAT will be added at 23% for Polish based companies, individuals and EU based companies who are unable to provide a valid EU Vat Numbers.

Email*		Phone*	
First Name*		Last Name*	
Job title*			
Company Name*		EU Vat / Tax ID / NIP number*	
Address*		City*	
Zip Code*		Country*	
		Date	2026-03-01
		Signature	

Scotts International. EU Vat number: PL 6772247784

tel. 0048 603 394 346 e-mail: support@scotts-international.com

www.scotts-international.com



Scotts International. EU Vat number: PL 6772247784

tel. 0048 603 394 346 e-mail: support@scotts-international.com
www.scotts-international.com