Zero Trust Security - Market Share Analysis, Industry Trends & Statistics, Growth Forecasts (2025 - 2030)

Market Report | 2025-04-28 | 152 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 38.37 billion in 2025, and is expected to reach USD 86.57 billion by 2030, at a CAGR of 17.67% during the forecast period (2025-2030).

Organizations have had to review their security postures due to the move toward cloud computing. Zero Trust facilities 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.

Key Highlights
- To successfully adopt zero-trust security, businesses are increasingly developing alliances with cybersecurity vendors and managed security service providers (MSSPs). These collaborations contribute knowledge and resources to handle the challenges of protecting the wider security perimeter. The growing use of cloud computing, which provides flexibility, scalability, and cost-efficiency, has completely changed how businesses function. Sensitive information and essential applications are no longer restricted to on-premises data centers, which also expanded the security perimeter.
- Businesses frequently use numerous cloud providers, which results in scattered data and applications. The enlarged security perimeter is more difficult to secure with this multi-cloud strategy. Under a shared responsibility approach, cloud service providers (CSPs) secure the infrastructure while customers are in charge of protecting their data and applications. This shared duty emphasizes the necessity of an all-encompassing security plan. Employees and third-party partners use a variety of locations and devices to access cloud services. So, there is a need for continuous monitoring and safe access controls.
- Adapting to the changing security perimeter, where data and users are dispersed across numerous locations and devices, is

essential for the future of cybersecurity. Zero-trust security offers a scalable architecture to keep ahead of new threats and address current issues. The global zero-trust security market has been anticipated to experience sustained growth as enterprises continue to reevaluate their security policies in response to these shifts, with innovative solutions continuously reshaping the cybersecurity landscape.
- Adopting zero-trust security requires a longer transition period for organizations with legacy systems. The deployment of thorough security measures may be delayed as a result. It takes time, money, and labor to upgrade or replace historical systems so they align with the zero-trust approach. As a result, some businesses may be discouraged from adopting zero-trust efforts. Legacy components may develop security flaws as organizations progressively use zero-trust security for their contemporary systems and applications, thereby offsetting the advantages of zero trust elsewhere in the network.
- Zero Trust Security has become much more crucial in the post-COVID-19 environment. Remote work, the cloud, emerging threats, and compliance obligations highlight the necessity for a flexible, proactive security approach. Organizations that adopt zero trust are better equipped to deal with the challenges of the post-pandemic scenario and protect their most essential assets in a constantly evolving digital environment.

Zero Trust Security Market Trends

Small and Medium Enterprises to Witness Major Growth

- SMEs play a central role in the economic landscape, helping to strengthen financial inclusion and supplying goods and services to poor and underserved markets. These enterprises are critical drivers of innovation and offer high growth potential. For instance, according to the European Commission, approximately 24.4 million small and medium-sized enterprises (SMEs) were estimated to be in the European Union in 2023, as SMEs form the backbone of the European economy.
- Even following a hybrid model, most small businesses have yet to prepare for flexibility within future work environments and employee policies. Growth in working from home, hybrid modalities, and family-focused employee structures aid quick transition to more secure strategies. To ensure sustainability, MSMEs should identify market opportunities and consumer demands.
- The cloud-based environment ensures long-term sustainability and resilience, driving the demand for various cybersecurity strategies for SMEs. A robust and secure work environment is guaranteed with zero-trust security, and an attempt to access an organization's network architecture can only succeed once trust is validated. When a user accesses an application, the user and device are confirmed, and trust is continuously monitored. This helps secure the organization's applications and environments from any user, device, and location, which is vital for SME's future growth.
- Many established and emerging cybersecurity players offer zero-trust network access (ZTNA) services for small and medium enterprises to cater to the rising demands. The cloud-delivered service extends the company's zero-trust solutions to cloud-native businesses and enterprises, embracing cloud adoption and giving SMEs improved productivity, better security, greater visibility, and a significantly reduced attack surface.

Asia Pacific Expected to Register Significant Growth

- Asia's technological abilities have increased over the past decade, with many businesses concentrating on the digital shift as one of their key goals throughout the pandemic. While the revolutions of digital transformation were set in motion much earlier, the pandemic accelerated their speed. It particularly impacted how organizations approach their IT ecosystem and security.
- Asia-Pacific is anticipated to dominate the global manufacturing industry, recording the highest inter-annual growth rate, especially in China. This country has achieved significant growth in its production rates compared to its pre-pandemic pace.
- China keeps prioritizing digitalization and improving its cybersecurity posture. ZAT solutions safeguard its digital operations and

help comply with regulatory standards. Chinese businesses are increasingly realizing the value of ZAT solutions, making the Chinese market a key driver of adoption in the Asia-Pacific region.
- In August 2023, Singtel, Asia's leading telecommunications technology group, announced a strategic partnership to offer Zscaler's security solutions in Asia, a first for the region. Through this partnership, Singtel's MSSE offers businesses impacted by insufficient in-house resources or skill sets an all-in-one digital security solution that helps to protect their digital assets against cyber threats.
- Enterprises in the APAC region will now have seamless access to Zscaler's Zero Trust Exchange, a cloud-based platform, through Singtel's Managed Security Service Edge (MSSE) suite of services, which includes pre-sales to post-sales support from dedicated cybersecurity experts as well as resources such as build implementation, platform consultation, maintenance, and round-the-clock threat mitigation. As the rate of enterprise digitalization continues to accelerate at an unprecedented pace, so does the risk of cyber threats.

Zero Trust Security Market Overview

The zero trust security market is fragmented with the presence of global and regional players such as Cisco Systems Inc., Palo Alto Networks Inc., IBM Corporation Inc., Broadcom Inc. (Symantec Corporation), and Microsoft Corporation. Moderate to high product differentiation, growing levels of product penetration, and high levels of competition characterize the market. Generally, the solutions are offered as a package solution, making the consolidated offering look like a part of the product's service.

- In September 2023, Broadcom acquired Vmware. With its potential VMware acquisition, Broadcom can meld Symantec's security portfolio with VMware's SD-WAN capabilities. By integrating Symantec, VMware SD-WAN, and some of Carbon Black's security capabilities, Broadcom could enter the single-vendor secure access service edge (SASE) industry and boost its overall SASE industry share and revenue if executed well. Broadcom's current Symantec SASE and security service edge (SSE) portfolio includes components such as secure web gateway (SWG), data loss prevention (DLP), cloud access security brokers (CASB), zero-trust network access (ZTNA), SSL inspection, and web isolation.
- In July 2023, Accenture teamed with Palo Alto Networks to bolster Zero Trust Security. In order to enable enterprises to improve their cybersecurity posture and speed up the implementation of business transformation initiatives, they have joined forces to deliver jointly secure access service edge solutions using a SASE solution. Palo Alto Networks and Accenture provide a comprehensive managed SASE solution that tackles organizations' challenges. Enterprises worldwide can accelerate their business transformation by combining the strength of the largest global systems integrator with the SASE solution, benefiting from improved network performance and a consistent security policy and implementation.

Additional Benefits:

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

Table of Contents:

Zero Trust Security - Market Share Analysis, Industry Trends & Statistics, Growth Forecasts (2025 - 2030)

Market Report | 2025-04-28 | 152 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	2025-05-07
		Signature