+357 96 030922
info@marketpublishers.com

Microsegmentation Market – Global Industry Size, Share, Trends, Opportunity, and Forecast, Segmented By Component (Solution v/s Service), By Security Type (Network Security, Database Security, End User Industry Security), By Deployment Mode (On-Premise v/s Cloud), By Organization Size (Large Enterprises v/s SMEs), By End User Industry (BFSI, IT & Telecommunication, Government & Defense, Healthcare, Manufacturing, Retail, Energy & Utilities, Others), By Region & Competition, 2021-2031F

https://marketpublishers.com/r/M1F10CC88932EN.html
Date: May 2026
Pages: 185
Price: US$ 4,500.00 (Single User License)
ID: M1F10CC88932EN

Abstracts

The Global microsegmentation market is expected to expand from USD 2.32 billion in 2025 to USD 8.18 billion by 2031, reflecting a compound annual growth rate of 23.37%. This network security approach isolates workloads into distinct segments, allowing organizations to manage and observe internal traffic through highly specific access rules. Market growth is accelerating largely due to the rising number of lateral movement cyberattacks and the broad integration of zero trust frameworks within enterprise networks. Additionally, the need to protect intricate multicloud infrastructures and meet strict data privacy compliance standards continues to drive the adoption of these security measures.

In 2025, an ISC2 report revealed that 28 percent of cybersecurity experts viewed network segmentation and isolation as an urgent skill gap for building effective security frameworks. While highly beneficial, the market's expansion is hindered by the difficulties of deploying these solutions within legacy environments. Aging IT systems

frequently lack the structural compatibility necessary to support precise policy controls, rendering the integration process exceptionally demanding and increasing the likelihood of operational downtime.

Market Driver

The growing danger of ransomware and lateral movement attacks serves as a primary catalyst for the global microsegmentation market's growth. Cybercriminals frequently breach outer defenses to move laterally across internal systems and compromise sensitive information. Microsegmentation mitigates this risk by establishing rigid internal perimeters that separate workloads and block illicit access. A February 2026 Dragos report, the '2026 OT Cybersecurity Report', noted that 119 different ransomware syndicates affected 3,300 industrial companies in 2025. This continuous threat of lateral infiltration compels businesses to apply precise rules that stop breaches where they start, making the prevention of widespread operational failures a major factor in adopting these safeguards.

Additionally, the rapid shift toward zero trust network frameworks is a major force behind market demand. Today's businesses are moving past legacy trust models, requiring constant authentication for all access attempts, with microsegmentation acting as the core mechanism for enforcing these rules. As noted in DXC Technology's October 2025 'The Trust Report From Risk Management to Strategic Resilience in Cybersecurity', 83 percent of companies implementing zero trust experienced a drop in security breaches. This risk reduction delivers clear operational and financial benefits to organizations utilizing segmented networks. Further underscoring this broader market value, a 2025 Akamai survey found that 60 percent of security executives secured reduced cyber insurance rates following enhancements to their network segmentation.

Market Challenge

The difficulty of deploying microsegmentation within legacy frameworks acts as a significant obstacle to global market growth. Aging infrastructures were typically built on flat network designs and inherent trust assumptions, making them incompatible with the strict demands of granular policy application. Bringing microsegmentation into these older systems requires an exhaustive analysis of current data traffic flows. Because legacy setups frequently struggle to accommodate modern security protocols, this rigorous integration process elevates the chances of system outages, causing many companies to hold back on deployments to prevent workflow interruptions and excessive resource consumption.

The friction involved in merging modern solutions with antiquated systems ultimately restricts the pace of microsegmentation adoption. A 2025 report from the SANS Institute revealed that 22 percent of companies faced operational technology cyber incidents, with 40 percent of those events leading to operational downtime. Such operational fragility makes business leaders even more hesitant to modify their deeply entrenched legacy architectures. Since microsegmentation relies on comprehensive monitoring of internal network activity, the foundational constraints of older hardware lead to prolonged installation phases, ultimately stalling the market's overall expansion.

Market Trends

The use of machine learning and artificial intelligence to automate policy creation is fundamentally revolutionizing the deployment of internal network security. Relying on manual configurations often leads to human error and slows down implementation within intricate systems, whereas contemporary platforms examine network traffic to instantly formulate accurate access controls. An April 2026 article by Zero Networks, '6 Processes to Automate When Implementing Microsegmentation', noted that 88 percent of cybersecurity executives considered automated policy generation a crucial feature when choosing a platform. By easing the operational burden for security personnel, this intelligent automation is driving faster acceptance across the market.

Simultaneously, the emergence of microsegmentation solutions tailored for cloud-native and containerized setups is reshaping the industry landscape. Traditional perimeter defenses struggle to monitor short-lived container environments characterized by constantly shifting workloads. To solve this, modern cloud-native segmentation binds security rules to specific workload identities instead of fixed IP addresses, allowing protective boundaries to travel alongside the applications. A February 2026 piece by 24x7 Server Management, 'Cloud Native Networking and Service Mesh Trends to Watch in 2026', highlighted that more than 90 percent of enterprises currently utilize Kubernetes in live production. The necessity of securing these orchestration frameworks is fundamentally motivating corporate investments toward specialized container segmentation technologies.

Key Market Players

- Cisco Systems, Inc.
- VMware, Inc.

Palo Alto Networks, Inc.

Illumio, Inc.

Akamai Technologies, Inc.

Fortinet, Inc.

Check Point Software Technologies Ltd.

Juniper Networks, Inc.

Trend Micro Incorporated

Sophos Ltd

Report Scope

In this report, the Global Microsegmentation Market has been segmented into the following categories, in addition to the industry trends which have also been detailed below:

Microsegmentation Market, By Component

Solution

Service

Microsegmentation Market, By Security Type

Network Security

Database Security

End User Industry Security

Microsegmentation Market, By Deployment Mode

- On-Premise
- Cloud

Microsegmentation Market, By Organization Size

- Large Enterprises
- SMEs

Microsegmentation Market, By End User Industry

- BFSI
- IT & Telecommunication
- Government & Defense
- Healthcare
- Manufacturing
- Retail
- Energy & Utilities
- Others

Microsegmentation Market, By Region

- North America
  - United States
  - Canada
  - Mexico

Europe

- France
- United Kingdom
- Italy
- Germany
- Spain

Asia Pacific

- China
- India
- Japan
- Australia
- South Korea

South America

- Brazil
- Argentina
- Colombia

Middle East & Africa

- South Africa
- Saudi Arabia
- UAE

Competitive Landscape

Company Profiles: Detailed analysis of the major companies present in the Global Microsegmentation Market.

Available Customizations:

Global Microsegmentation Market report with the given market data, TechSci Research offers customizations according to a company's specific needs. The following customization options are available for the report:

Company Information

Detailed analysis and profiling of additional market players (up to five).

+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

+357 96 030922
info@marketpublishers.com

+357 96 030922
info@marketpublishers.com

+357 96 030922
info@marketpublishers.com

I would like to order

Product name: Microsegmentation Market – Global Industry Size, Share, Trends, Opportunity, and Forecast, Segmented By Component (Solution v/s Service), By Security Type (Network Security, Database Security, End User Industry Security), By Deployment Mode (On-Premise v/s Cloud), By Organization Size (Large Enterprises v/s SMEs), By End User Industry (BFSI, IT & Telecommunication, Government & Defense, Healthcare, Manufacturing, Retail, Energy & Utilities, Others), By Region & Competition, 2021-2031F

Product link: https://marketpublishers.com/r/M1F10CC88932EN.html

Price: US$ 4,500.00 (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/M1F10CC88932EN.html