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

Market Report | 2025-04-28 | 137 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 Container Security Market size is estimated at USD 3.24 billion in 2025, and is expected to reach USD 8.14 billion by 2030, at a CAGR of 20.27% during the forecast period (2025-2030).

The container security market is expanding, driven by enterprises increasingly adopting microservices and digital transformation initiatives, coupled with a rise in security threats. Additionally, the market is driven by the universal adoption of containerized applications across enterprises, a notable surge in cloud computing solutions spanning diverse industry verticals, and a growing inclination towards serverless technologies.

Key Highlights
- The increasing adoption of hybrid cloud technology and heightened concerns over vulnerabilities in container architecture are key drivers propelling the growth of the container security market. As organizations increasingly adopt cloud-native technologies and multi-cloud or hybrid strategies, managing security becomes more complex. With the deployment of containers across varied cloud environments, companies seek security solutions that ensure visibility across multiple clouds and maintain uniform security controls.
- As cloud adoption has surged, containerization has gained significant traction. In an era where multi-cloud infrastructures dominate, deploying self-sufficient applications anywhere proves invaluable. Moreover, containerization streamlines deployment and management by packaging applications with the necessary dependencies. However, with the growth in containerization across businesses, the vulnerabilities associated with container architecture drive the demand for container security solutions.
- As container architecture gains traction, the importance of container security has surged. For example, in 2023, Sysdig, Inc., a software firm specializing in security for containers, Kubernetes, and the cloud, reported that 16% of its global enterprise clientele operate up to 100 containers within their infrastructure. Further, nearly 39% of enterprises leveraging container technology

manage up to 250 containers and 61% of customers run more than 250 containers.
- Companies often engage multiple cloud providers, leading to challenges in synchronizing security, performance, and compliance across these platforms. These varied cloud management demands specialized expertise and involves time-intensive manual configurations. To address these challenges, vendors like IBM and VMware have rolled out solutions that centralize multi-cloud management, streamlining operations across diverse platforms.
- With the looming recession in European countries and the United States, a decline in demand for container security solutions is expected. Economic pressures will likely lead companies to tighten their budgets, resulting in more stringent IT expenditures. Consequently, businesses may become more selective in their cybersecurity investments, prioritizing essential solutions that offer a high return on investment (ROI). For instance, according to the latest Gross Domestic Product (GDP) release by the German Federal Statistical Office, the country's economy went through a recession in 2023 when real GDP declined by 0.2%. Further, according to the European Commission, following a recession in 2023, economic activity in Germany is anticipated to stagnate in 2024.

Container Security Market Trends

Cloud-based is Expected to Hold a Strong Market Share

- Cloud-based deployment of container security solutions is gaining significant traction in businesses worldwide. This model brings notable benefits: enhanced scalability, greater flexibility, and reduced costs. Organizations can swiftly adjust their security measures in response to evolving needs without making hefty investments in infrastructure. Such adaptability is invaluable for enterprises in dynamic settings, where workloads and security demands can shift swiftly.
- The rise of cloud-based deployment is further fueled by the growing integration of container security with cloud service providers. Leading cloud platforms, including Amazon Web Services (AWS), Microsoft Azure, and Google Cloud Platform, are incorporating built-in container security features into their offerings. These integrated solutions ensure robust security for containerized applications on their platforms, simplifying the adoption and implementation of container security measures for organizations.
- Hybrid clouds, which combine private and public infrastructures, heighten potential security vulnerabilities across these environments. As organizations increasingly manage containerized applications in hybrid settings, the demand for robust container security solutions capable of safeguarding diverse infrastructures has surged.
- Hybrid cloud solutions merge the flexibility of public cloud services with the robust security of private infrastructures, enabling businesses to streamline operations while safeguarding sensitive data. Public cloud services have emerged as cloud computing has cemented its role in contemporary business practices. A survey conducted by Flexera Software in 2024 indicates that 73% of global businesses favor hybrid cloud services, underscoring the model's growing popularity and cost-effectiveness. This pay-as-you-go model empowers companies to adjust resources dynamically, appealing to organizations across the spectrum.
- Additionally, cloud-based container security solutions are often easier to deploy and manage than their on-premises counterparts. This allows organizations to focus on their core business operations while ensuring their containerized environments are well-protected. The growing adoption of cloud-native applications drives the demand for cloud-based container security solutions.

North America is Expected to Hold a Significant Market Share

- As containerized applications rapidly gain traction across diverse industries, the U.S. market is witnessing a pronounced transition from traditional IT setups to containerized environments, which offer enhanced flexibility and expedited deployment.

Leading this shift, AWS's Amazon Elastic Kubernetes Service (EKS) empowers businesses to oversee their containerized workloads, seamlessly integrating with a suite of other AWS offerings. Meanwhile, Microsoft Azure and Google Cloud Platform are leveraging Kubernetes, providing analogous services that simplify application scaling and management, amplifying the demand for robust security measures.

- Tech giants like AWS and Azure invest heavily in Kubernetes and container services. This investment is underscored by an escalating demand for integrated security driven by mounting concerns over vulnerabilities in containerized applications. For instance, in April 2024, Microsoft unveiled a significant update addressing 150 vulnerabilities. They highlighted a critical vulnerability, tracked as CVE-2024-29990, which poses a severe risk. This flaw permits unauthenticated hackers to command Azure Kubernetes clusters, enabling them to pilfer credentials and compromise resources beyond the protective measures of Azure's Kubernetes Service Confidential Containers (AKSCC).
- In Canada, the container security market is witnessing consistent growth. This trend is largely driven by the surge in cloud-native application deployments and a growing preference among businesses for hybrid and multi-cloud strategies. As Canadian enterprises harness container technology for improved scalability, there's a parallel uptick in the demand for robust security solutions to address potential vulnerabilities.
- Moreover, Canadian enterprises' adoption of DevOps and Continuous Integration/Continuous Delivery (CI/CD) pipelines is further fueling the growth of container security. Recognizing these pipelines' importance, companies prioritize their security to thwart vulnerabilities from infiltrating production environments. This emphasis has led to heightened investments in security solutions specifically designed for containerized applications.

Container Security Industry Overview

The container security market is highly competitive, with many established players offering comprehensive container security solutions and the emergence of startups offering innovative solutions to mitigate security challenges associated with containers.

Vendors' competitive strategy is to gain a foothold in the market through innovation, mergers, and acquisitions. Major vendors' capability of investing in research and development is higher, thus intensifying the competition in the container security market.

Some of the major players in the market are Google LLC (Alphabet Inc.), Trend Micro Incorporated, Qualys, Inc., Red Hat, Inc. (IBM Corporation), and Palo Alto Networks, Inc., among others.

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 INSIGHTS
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 Substitute Products
4.2.5 Intensity of Competitive Rivalry
4.3 Assessment of Macroeconomic Factors on the Market
4.4 Industry Value Chain Analysis

5 MARKET DYNAMICS
5.1 Market Drivers
5.1.1 Rising Adoption of the Hybrid Cloud Technology Applications
5.1.2 Growing Vulnerability Concern across the Container Architecture
5.2 Market Restraints
5.2.1 Complexity in Managing the Cloud Environments
5.2.2 Inadequate Budgets in SMEs and Lack of Technical Expertise
5.3 Technology Snapshot

6 MARKET SEGMENTATION
6.1 By Organisation Size
6.1.1 Large Enterprises
6.1.2 Small & Medium Enterprises
6.2 By Deployment
6.2.1 Cloud-based
6.2.2 On-premise
6.3 By End-user Industry
6.3.1 IT & ITES
6.3.2 BFSI
6.3.3 Retail
6.3.4 Healthcare
6.3.5 Industrial
6.3.6 Other End-user Industries
6.4 By Geography
6.4.1 North America
6.4.1.1 United States
6.4.1.2 Canada
6.4.2 Europe
6.4.2.1 United Kingdom
6.4.2.2 Germany
6.4.3 Asia
6.4.3.1 China
6.4.3.2 Japan
6.4.3.3 Australia and New Zealand
6.4.4 Latin America
6.4.5 Middle East and Africa

7 COMPETITIVE LANDSCAPE

7.1 Company Profiles
7.1.1 Google LLC (Alphabet Inc.)
7.1.2 Trend Micro Incorporated
7.1.3 Qualys, Inc.
7.1.4 Red Hat, Inc. (IBM Corporation)
7.1.5 Palo Alto Networks, Inc.
7.1.6 Aqua Security Software Ltd.
7.1.7 Rapid7, Inc.
7.1.8 Mirantis, Inc.
7.1.9 SUSE S.A.
7.1.10 Thales Group
7.1.11 Fidelis Cybersecurity, Ltd

8 INVESTMENT ANALYSIS

9 FUTURE OUTLOOK OF THE MARKET

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

Market Report | 2025-04-28 | 137 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	2026-03-07
		Signature	