

DevSecOps Market Forecasts to 2034 – Global Analysis By Component (Solutions, and Services), Deployment Mode (Cloud, On-Premises, and Hybrid), Organization Size, Security Type, Development Stage, Tool Type, End User, and By Geography

<https://marketpublishers.com/r/DE1AA30F6452EN.html>

Date: July 2026

Pages: 0

Price: US\$ 4,150.00 (Single User License)

ID: DE1AA30F6452EN

Abstracts

According to Statistics MRC, the Global DevSecOps Market is accounted for \$12.6 billion in 2026 and is expected to reach \$38.1 billion by 2034 growing at a CAGR of 14.8% during the forecast period. DevSecOps is a software development approach that integrates security practices into the DevOps pipeline, enabling continuous security testing, monitoring, and remediation throughout the application lifecycle. This market encompasses solutions including application security testing, infrastructure security, container security, cloud security, compliance and governance, secrets management, and vulnerability management, along with professional and managed services. As organizations accelerate digital transformation and adopt cloud-native architectures, integrating security into development workflows has become essential for reducing risk and accelerating time-to-market. The shift from traditional security models to DevSecOps is transforming how enterprises build and deploy software.

Market Dynamics:

Driver:

Increasing adoption of cloud-native and containerized applications

The rapid migration to cloud-native architectures and containerized applications is a primary driver for the DevSecOps market. As organizations adopt microservices, Kubernetes, and serverless computing, traditional security approaches are no longer

effective in protecting dynamic, ephemeral environments. DevSecOps enables automated security scanning, policy enforcement, and compliance validation throughout the development pipeline, ensuring security keeps pace with continuous deployment. The need to secure container images, orchestration platforms, and cloud infrastructure has made DevSecOps essential for modern application development. As cloud adoption accelerates across all industries, demand for integrated security solutions continues growing.

Restraint:

Cultural resistance and skills gap in security integration

Cultural resistance and the shortage of skilled DevSecOps professionals represent significant restraints for market growth. Traditional development, operations, and security teams often operate in silos with conflicting priorities and methodologies. Integrating security into DevOps workflows requires cultural transformation and collaboration, which many organizations struggle to achieve. The shortage of professionals with combined expertise in development, operations, and security creates implementation challenges. Teams accustomed to rapid deployment may perceive security integration as slowing delivery. These cultural and skills barriers slow adoption, particularly among organizations with legacy development practices and traditional security models.

Opportunity:

Integration of AI and automation in security testing

The integration of artificial intelligence and automation into DevSecOps presents substantial opportunities for market expansion. AI-powered security solutions automate vulnerability detection, prioritize remediation efforts, and reduce false positives, enabling faster, more accurate security testing. Automated remediation capabilities allow organizations to fix vulnerabilities without manual intervention, accelerating delivery while maintaining security. Predictive analytics identify potential security issues before they reach production. As AI technologies mature and automation capabilities expand, DevSecOps solutions become more intelligent and efficient, attracting organizations seeking to balance speed and security.

Threat:

Complexity of managing security across hybrid and multi-cloud environments

The increasing complexity of securing applications across hybrid and multi-cloud environments poses significant threats to DevSecOps adoption. Organizations operate applications across on-premises infrastructure, multiple public cloud providers, and edge environments, each with distinct security requirements and tools. Consistent security policy enforcement across diverse environments requires sophisticated orchestration and integration. The proliferation of security tools creates management complexity and potential gaps in coverage. Compliance requirements vary across jurisdictions and industries, adding operational burden. These complexities may lead organizations to delay full DevSecOps implementation, affecting market growth.

Covid-19 Impact:

The COVID-19 pandemic accelerated DevSecOps adoption as organizations rapidly shifted to remote work and digital channels, increasing software delivery velocity while expanding attack surfaces. The surge in remote development and cloud migration required security transformation. Organizations prioritized automated security testing to maintain protection without slowing deployment. However, some initiatives faced budget constraints during economic uncertainty. The need for rapid digital transformation during the crisis demonstrated the value of integrated security. Post-pandemic, DevSecOps has become a strategic priority, with the crisis serving as a catalyst for modernizing security approaches.

The Cloud Security segment is expected to be the largest during the forecast period

The Cloud Security segment is expected to account for the largest market share during the forecast period, driven by the widespread migration of applications and data to cloud environments. As organizations adopt public, private, and hybrid cloud models, securing cloud infrastructure, platforms, and applications has become critical. Cloud security solutions enable automated policy enforcement, threat detection, and compliance monitoring across cloud environments. The dynamic nature of cloud resources, with rapid provisioning and scaling, necessitates DevSecOps integration for continuous protection. Growing cloud adoption across enterprise segments and expanding cloud-native application development ensure this segment maintains dominant market position.

The Hybrid segment is expected to have the highest CAGR during the forecast period

Over the forecast period, the Hybrid segment is predicted to witness the highest growth rate, fueled by organizations maintaining mixed infrastructure across on-premises and cloud environments. Hybrid deployments enable organizations to balance security and compliance requirements with the benefits of public cloud scalability. This approach accommodates legacy applications requiring on-premises infrastructure alongside modern cloud-native applications. Hybrid DevSecOps solutions provide consistent security policies and workflows across diverse environments. As many enterprises adopt hybrid strategies as transitional steps to full cloud adoption, demand for hybrid DevSecOps solutions grows at exceptionally high rates.

Region with largest share:

During the forecast period, the North America region is expected to hold the largest market share, supported by early technology adoption, significant security investment, and the presence of major DevSecOps vendors. The region's strong technology sector and cybersecurity awareness create favorable conditions for DevSecOps adoption. Regulatory requirements including HIPAA, PCI DSS, and SOX mandate security integration in software development, driving demand. Large enterprises across financial services, technology, and healthcare sectors invest heavily in DevSecOps. With strong innovation ecosystems and regulatory drivers, North America maintains its dominant market position.

Region with highest CAGR:

Over the forecast period, the Asia Pacific region is anticipated to exhibit the highest CAGR, driven by rapid digital transformation, expanding cloud adoption, and increasing security awareness. Countries including China, India, Australia, and Singapore are experiencing growing investment in DevSecOps as organizations modernize development practices. Government cybersecurity initiatives and data protection regulations promote security integration. The region's large technology workforce and growing startup ecosystem create substantial addressable market. As digital transformation accelerates and security becomes a competitive priority, Asia Pacific delivers the fastest DevSecOps market growth globally.

Key players in the market

Some of the key players in DevSecOps Market include Microsoft Corporation, IBM Corporation, GitLab Inc., Atlassian Corporation, Palo Alto Networks, Inc., Check Point Software Technologies Ltd., Broadcom Inc., Cisco Systems, Inc., Synopsys, Inc.,

OpenText Corporation, JFrog Ltd., Veracode, Inc., Sonatype, Inc., Snyk Limited, Akamai Technologies, Inc., CloudBees, Inc., Qualys, Inc., and Rapid7, Inc.

Key Developments:

In June 2026, Microsoft introduced the new GitHub app for agentic development alongside a preview of 'Foundry IQ' enterprise AI security updates, establishing a unified control plane to govern, audit, and secure AI-generated and reviewed code.

In June 2026, GitLab was positioned as a Leader in the 2026 Gartner Magic Quadrant for DevSecOps Platforms for the fourth consecutive year, backed by a newly instituted 99.9% monthly availability SLA commitment for its Ultimate tier cloud customers.

In March 2026, Palo Alto Networks' open-source Infrastructure as Code (IaC) scanning tool, Checkov, received structural database updates to handle policy-as-code enforcement for complex multi-cloud deployments across Terraform and Kubernetes, neutralizing misconfigurations before deployment.

Components Covered:

Solutions

Services

Deployment Modes Covered:

Cloud

On-Premises

Hybrid

Organization Sizes Covered:

Large Enterprises

Small and Medium Enterprises (SMEs)

Security Types Covered:

Application Security

Cloud Security

Container Security

Network Security

Endpoint Security

Data Security

Identity and Access Management

Development Stages Covered:

Planning and Design

Code Development

Build and Integration

Testing

Deployment

Operations and Monitoring

Tool Types Covered:

Static Application Security Testing (SAST)

Dynamic Application Security Testing (DAST)

Interactive Application Security Testing (IAST)

Software Composition Analysis (SCA)

Runtime Application Self-Protection (RASP)

Container Security Tools

Infrastructure as Code Security Tools

CI/CD Security Tools

End Users Covered:

BFSI

IT and Telecommunications

Government and Defense

Healthcare

Retail and E-commerce

Manufacturing

Energy and Utilities

Media and Entertainment

Education

Other End Users

Regions Covered:

North America

United States

Canada

Mexico

Europe

United Kingdom

Germany

France

Italy

Spain

Netherlands

Belgium

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

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 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

Contents

1 EXECUTIVE SUMMARY

- 1.1 Market Snapshot and Key Highlights
- 1.2 Growth Drivers, Challenges, and Opportunities
- 1.3 Competitive Landscape Overview
- 1.4 Strategic Insights and Recommendations

2 RESEARCH FRAMEWORK

- 2.1 Study Objectives and Scope
- 2.2 Stakeholder Analysis
- 2.3 Research Assumptions and Limitations
- 2.4 Research Methodology
 - 2.4.1 Data Collection (Primary and Secondary)
 - 2.4.2 Data Modeling and Estimation Techniques
 - 2.4.3 Data Validation and Triangulation
 - 2.4.4 Analytical and Forecasting Approach

3 MARKET DYNAMICS AND TREND ANALYSIS

- 3.1 Market Definition and Structure
- 3.2 Key Market Drivers
- 3.3 Market Restraints and Challenges
- 3.4 Growth Opportunities and Investment Hotspots
- 3.5 Industry Threats and Risk Assessment
- 3.6 Technology and Innovation Landscape
- 3.7 Emerging and High-Growth Markets
- 3.8 Regulatory and Policy Environment
- 3.9 Impact of COVID-19 and Recovery Outlook

4 COMPETITIVE AND STRATEGIC ASSESSMENT

- 4.1 Porter's Five Forces Analysis
 - 4.1.1 Supplier Bargaining Power
 - 4.1.2 Buyer Bargaining Power
 - 4.1.3 Threat of Substitutes
 - 4.1.4 Threat of New Entrants

- 4.1.5 Competitive Rivalry
- 4.2 Market Share Analysis of Key Players
- 4.3 Product Benchmarking and Performance Comparison

5 GLOBAL DEVSECOPS MARKET, BY COMPONENT

- 5.1 Solutions
 - 5.1.1 Application Security Testing
 - 5.1.2 Infrastructure Security
 - 5.1.3 Container Security
 - 5.1.4 Cloud Security
 - 5.1.5 Compliance and Governance
 - 5.1.6 Secrets Management
 - 5.1.7 Vulnerability Management
 - 5.1.8 Other Solutions
- 5.2 Services
 - 5.2.1 Professional Services
 - 5.2.2 Managed Services

6 GLOBAL DEVSECOPS MARKET, BY DEPLOYMENT MODE

- 6.1 Cloud
- 6.2 On-Premises
- 6.3 Hybrid

7 GLOBAL DEVSECOPS MARKET, BY ORGANIZATION SIZE

- 7.1 Large Enterprises
- 7.2 Small and Medium Enterprises (SMEs)

8 GLOBAL DEVSECOPS MARKET, BY SECURITY TYPE

- 8.1 Application Security
- 8.2 Cloud Security
- 8.3 Container Security
- 8.4 Network Security
- 8.5 Endpoint Security
- 8.6 Data Security
- 8.7 Identity and Access Management

9 GLOBAL DEVSECOPS MARKET, BY DEVELOPMENT STAGE

- 9.1 Planning and Design
- 9.2 Code Development
- 9.3 Build and Integration
- 9.4 Testing
- 9.5 Deployment
- 9.6 Operations and Monitoring

10 GLOBAL DEVSECOPS MARKET, BY TOOL TYPE

- 10.1 Static Application Security Testing (SAST)
- 10.2 Dynamic Application Security Testing (DAST)
- 10.3 Interactive Application Security Testing (IAST)
- 10.4 Software Composition Analysis (SCA)
- 10.5 Runtime Application Self-Protection (RASP)
- 10.6 Container Security Tools
- 10.7 Infrastructure as Code Security Tools
- 10.8 CI/CD Security Tools

11 GLOBAL DEVSECOPS MARKET, BY END USER

- 11.1 BFSI
- 11.2 IT and Telecommunications
- 11.3 Government and Defense
- 11.4 Healthcare
- 11.5 Retail and E-commerce
- 11.6 Manufacturing
- 11.7 Energy and Utilities
- 11.8 Media and Entertainment
- 11.9 Education
- 11.10 Other End Users

12 GLOBAL DEVSECOPS MARKET, BY GEOGRAPHY

- 12.1 North America
 - 12.1.1 United States
 - 12.1.2 Canada

- 12.1.3 Mexico
- 12.2 Europe
 - 12.2.1 United Kingdom
 - 12.2.2 Germany
 - 12.2.3 France
 - 12.2.4 Italy
 - 12.2.5 Spain
 - 12.2.6 Netherlands
 - 12.2.7 Belgium
 - 12.2.8 Sweden
 - 12.2.9 Switzerland
 - 12.2.10 Poland
 - 12.2.11 Rest of Europe
- 12.3 Asia Pacific
 - 12.3.1 China
 - 12.3.2 Japan
 - 12.3.3 India
 - 12.3.4 South Korea
 - 12.3.5 Australia
 - 12.3.6 Indonesia
 - 12.3.7 Thailand
 - 12.3.8 Malaysia
 - 12.3.9 Singapore
 - 12.3.10 Vietnam
 - 12.3.11 Rest of Asia Pacific
- 12.4 South America
 - 12.4.1 Brazil
 - 12.4.2 Argentina
 - 12.4.3 Colombia
 - 12.4.4 Chile
 - 12.4.5 Peru
 - 12.4.6 Rest of South America
- 12.5 Rest of the World (RoW)
 - 12.5.1 Middle East
 - 12.5.1.1 Saudi Arabia
 - 12.5.1.2 United Arab Emirates
 - 12.5.1.3 Qatar
 - 12.5.1.4 Israel
 - 12.5.1.5 Rest of Middle East

12.5.2 Africa

12.5.2.1 South Africa

12.5.2.2 Egypt

12.5.2.3 Morocco

12.5.2.4 Rest of Africa

13 STRATEGIC MARKET INTELLIGENCE

13.1 Industry Value Network and Supply Chain Assessment

13.2 White-Space and Opportunity Mapping

13.3 Product Evolution and Market Life Cycle Analysis

13.4 Channel, Distributor, and Go-to-Market Assessment

14 INDUSTRY DEVELOPMENTS AND STRATEGIC INITIATIVES

14.1 Mergers and Acquisitions

14.2 Partnerships, Alliances, and Joint Ventures

14.3 New Product Launches and Certifications

14.4 Capacity Expansion and Investments

14.5 Other Strategic Initiatives

15 COMPANY PROFILES

15.1 Microsoft Corporation

15.2 IBM Corporation

15.3 GitLab Inc.

15.4 Atlassian Corporation

15.5 Palo Alto Networks, Inc.

15.6 Check Point Software Technologies Ltd.

15.7 Broadcom Inc.

15.8 Cisco Systems, Inc.

15.9 Synopsys, Inc.

15.10 OpenText Corporation

15.11 JFrog Ltd.

15.12 Veracode, Inc.

15.13 Sonatype, Inc.

15.14 Snyk Limited

15.15 Akamai Technologies, Inc.

15.16 CloudBees, Inc.

15.17 Qualys, Inc.

15.18 Rapid7, Inc.

List Of Tables

LIST OF TABLES

Table 1 Global DevSecOps Market Outlook, By Region (2023–2034) (\$MN)
Table 2 Global DevSecOps Market Outlook, By Component (2023–2034) (\$MN)
Table 3 Global DevSecOps Market Outlook, By Solutions (2023–2034) (\$MN)
Table 4 Global DevSecOps Market Outlook, By Application Security Testing (2023–2034) (\$MN)
Table 5 Global DevSecOps Market Outlook, By Infrastructure Security (2023–2034) (\$MN)
Table 6 Global DevSecOps Market Outlook, By Container Security (2023–2034) (\$MN)
Table 7 Global DevSecOps Market Outlook, By Cloud Security (2023–2034) (\$MN)
Table 8 Global DevSecOps Market Outlook, By Compliance and Governance (2023–2034) (\$MN)
Table 9 Global DevSecOps Market Outlook, By Secrets Management (2023–2034) (\$MN)
Table 10 Global DevSecOps Market Outlook, By Vulnerability Management (2023–2034) (\$MN)
Table 11 Global DevSecOps Market Outlook, By Other Solutions (2023–2034) (\$MN)
Table 12 Global DevSecOps Market Outlook, By Services (2023–2034) (\$MN)
Table 13 Global DevSecOps Market Outlook, By Professional Services (2023–2034) (\$MN)
Table 14 Global DevSecOps Market Outlook, By Managed Services (2023–2034) (\$MN)
Table 15 Global DevSecOps Market Outlook, By Deployment Mode (2023–2034) (\$MN)
Table 16 Global DevSecOps Market Outlook, By Cloud (2023–2034) (\$MN)
Table 17 Global DevSecOps Market Outlook, By On-Premises (2023–2034) (\$MN)
Table 18 Global DevSecOps Market Outlook, By Hybrid (2023–2034) (\$MN)
Table 19 Global DevSecOps Market Outlook, By Organization Size (2023–2034) (\$MN)
Table 20 Global DevSecOps Market Outlook, By Large Enterprises (2023–2034) (\$MN)
Table 21 Global DevSecOps Market Outlook, By Small and Medium Enterprises (SMEs) (2023–2034) (\$MN)
Table 22 Global DevSecOps Market Outlook, By Security Type (2023–2034) (\$MN)
Table 23 Global DevSecOps Market Outlook, By Application Security (2023–2034) (\$MN)
Table 24 Global DevSecOps Market Outlook, By Cloud Security (2023–2034) (\$MN)
Table 25 Global DevSecOps Market Outlook, By Container Security (2023–2034) (\$MN)
Table 26 Global DevSecOps Market Outlook, By Network Security (2023–2034) (\$MN)
Table 27 Global DevSecOps Market Outlook, By Endpoint Security (2023–2034) (\$MN)

Table 28 Global DevSecOps Market Outlook, By Data Security (2023–2034) (\$MN)

Table 29 Global DevSecOps Market Outlook, By Identity and Access Management (2023–2034) (\$MN)

Table 30 Global DevSecOps Market Outlook, By Development Stage (2023–2034) (\$MN)

Table 31 Global DevSecOps Market Outlook, By Planning and Design (2023–2034) (\$MN)

Table 32 Global DevSecOps Market Outlook, By Code Development (2023–2034) (\$MN)

Table 33 Global DevSecOps Market Outlook, By Build and Integration (2023–2034) (\$MN)

Table 34 Global DevSecOps Market Outlook, By Testing (2023–2034) (\$MN)

Table 35 Global DevSecOps Market Outlook, By Deployment (2023–2034) (\$MN)

Table 36 Global DevSecOps Market Outlook, By Operations and Monitoring (2023–2034) (\$MN)

Table 37 Global DevSecOps Market Outlook, By Tool Type (2023–2034) (\$MN)

Table 38 Global DevSecOps Market Outlook, By Static Application Security Testing (SAST) (2023–2034) (\$MN)

Table 39 Global DevSecOps Market Outlook, By Dynamic Application Security Testing (DAST) (2023–2034) (\$MN)

Table 40 Global DevSecOps Market Outlook, By Interactive Application Security Testing (IAST) (2023–2034) (\$MN)

Table 41 Global DevSecOps Market Outlook, By Software Composition Analysis (SCA) (2023–2034) (\$MN)

Table 42 Global DevSecOps Market Outlook, By Runtime Application Self-Protection (RASP) (2023–2034) (\$MN)

Table 43 Global DevSecOps Market Outlook, By Container Security Tools (2023–2034) (\$MN)

Table 44 Global DevSecOps Market Outlook, By Infrastructure as Code Security Tools (2023–2034) (\$MN)

Table 45 Global DevSecOps Market Outlook, By CI/CD Security Tools (2023–2034) (\$MN)

Table 46 Global DevSecOps Market Outlook, By End User (2023–2034) (\$MN)

Table 47 Global DevSecOps Market Outlook, By BFSI (2023–2034) (\$MN)

Table 48 Global DevSecOps Market Outlook, By IT and Telecommunications (2023–2034) (\$MN)

Table 49 Global DevSecOps Market Outlook, By Government and Defense (2023–2034) (\$MN)

Table 50 Global DevSecOps Market Outlook, By Healthcare (2023–2034) (\$MN)

Table 51 Global DevSecOps Market Outlook, By Retail and E-commerce (2023–2034) (\$MN)

Table 52 Global DevSecOps Market Outlook, By Manufacturing (2023–2034) (\$MN)

Table 53 Global DevSecOps Market Outlook, By Energy and Utilities (2023–2034) (\$MN)

Table 54 Global DevSecOps Market Outlook, By Media and Entertainment (2023–2034) (\$MN)

Table 55 Global DevSecOps Market Outlook, By Education (2023–2034) (\$MN)

Table 56 Global DevSecOps Market Outlook, By Other End Users (2023–2034) (\$MN)

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.

I would like to order

Product name: DevSecOps Market Forecasts to 2034 – Global Analysis By Component (Solutions, and Services), Deployment Mode (Cloud, On-Premises, and Hybrid), Organization Size, Security Type, Development Stage, Tool Type, End User, and By Geography

Product link: <https://marketpublishers.com/r/DE1AA30F6452EN.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/DE1AA30F6452EN.html>