

Application Security Market Size, Share, Trends and Forecast by Component, Type, Testing Type, Deployment Mode, Organization Size, Industry Vertical, and Region, 2026-2034

<https://marketpublishers.com/r/A7D7E03056B6EN.html>

Date: April 2026

Pages: 145

Price: US\$ 3,999.00 (Single User License)

ID: A7D7E03056B6EN

Abstracts

The global application security market size was valued at USD 11.9 Billion in 2025. Looking forward, IMARC Group estimates the market to reach USD 37.6 Billion by 2034, exhibiting a CAGR of 13.21% during 2026-2034. North America currently dominates the market, holding a significant market share of 40.5% in 2025. Because of its sophisticated technological infrastructure, broad adoption of digital transformation, and plenty of top cybersecurity companies, North America leads the market. Market expansion is also fueled by a high amount of cyberthreats, strict regulatory compliance requirements, and large industry investments in security solutions. Furthermore, the region's strong emphasis on innovation encourages ongoing advancements in application security technologies.

The market is experiencing growth as more businesses are embracing digital change and cybercriminals are targeting corporate applications like never before. This involves the use of cloud applications as well as the displacement of security practices across the software development lifecycle using DevSecOps. There are legal requirements like the CCPA and GDPR that mandate privacy and data security, which is driving the demand even more. In addition, the integration of machine learning (ML) and artificial intelligence (AI) in application security solutions enhances threat detection and response. Occupational trends like remote work as well as the use of mobile and web applications are increasing the attack surface, and so vigorous security strategies are needed.

The United States stands out as a key market disruptor, driven by the nation's highly

developed technical environment and the rising number of cyberattacks that target applications in industries like retail, healthcare, and finance. Adoption is accelerated by strict regulatory frameworks like HIPAA, PCI DSS, and CCPA that require strong security measures. The need for sophisticated application security solutions is being driven by the quick transition to cloud-based apps and remote work settings, which increases risks. Innovations in threat detection and prevention technology is encouraged by the existence of top cybersecurity firms and significant R&D expenditures. Furthermore, the incorporation of AI and ML in security technologies and the spread of DevSecOps practices is fueling the market expansion. The growing enterprise awareness about application security is positively influencing the market. The IMARC Group's report shows that the United States application security market is expected to reach US\$ 8.68 Billion by 2032.

APPLICATION SECURITY MARKET TRENDS:

Increasing Cyber Threats

In most cases, the need for application security services arises from the growing cyber risks as the companies continue to sustain a number of complex and sophisticated attacks that target apps. These dangers, which include distributed denial-of-service (DDoS) attacks, SQL injections, and cross-site scripting, take advantage of software flaws to steal confidential information, interfere with business operations, or result in monetary loss. Due to more people relying on internet, mobile, and cloud-based apps, there is an increase in the attack surface for hackers. Companies also seem to understand the requirement of strong application security measures due to famous breaches and ransomware incident. Companies in the e-commerce, healthcare and banking sectors, which process sensitive consumer data are extremely at risk and therefore they are investing heavily in appropriate security measures.

Digital transformation

Because more sectors are depending on digital apps and technology, the market for application security is being driven by digital transformation. The attack surface is growing as businesses use cloud computing, IoT, AI, and big data analytics, making applications more vulnerable to cyberattacks. Strong security solutions are necessary to safeguard sensitive data and stop breaches as a result of the quick development and rollout of online and mobile applications to improve customer experiences and optimize operations. Furthermore, using microservices architecture and integrating third-party APIs is creating additional vulnerabilities that call for sophisticated application security

solutions. Businesses are further compelled to give application security top priority in their digital initiatives because of regulatory compliance requirements like the CCPA and GDPR.

Remote work trends

Because of the growing dependence on cloud-based apps and collaboration tools, which are easy targets for cyberattacks, remote work trends are positively influencing the market. Employees can access company resources from a variety of devices and places, frequently via unprotected networks, as a result of the shift to remote and hybrid work patterns. Strong security measures are now more important than ever to safeguard private information and apps. Organizations must invest in application security solutions since remote work settings are more vulnerable to threats like phishing, credential theft, and illegal access. Furthermore, application security measures are integrated with the use of secure online gateways, virtual private networks (VPNs), and identity and access management (IAM) systems.

APPLICATION SECURITY INDUSTRY SEGMENTATION:

IMARC Group provides an analysis of the key trends in each sub-segment of the global application security market report, along with forecasts at the global, regional and country level from 2026-2034. Our report has categorized the market based on component, type, testing type, deployment mode, organization size, and industry vertical.

Analysis by Component:

Solution

Services

Solution stands as the largest component in 2025, holding 67.2% of the market. Because it plays a vital role in protecting applications from constantly changing cyberthreats, the solution sector leads the application security market. To proactively identify, stop, and mitigate vulnerabilities, organizations place a high priority on implementing complete security solutions, such as web application firewalls (WAF), runtime application self-protection (RASP), and static and dynamic application security testing (SAST and DAST) technologies. Strong solutions are more in demand as

companies embrace digital transformation and become more dependent on cloud-based apps and secure software. These systems are more successful because they incorporate cutting-edge technology like artificial intelligence (AI) and machine learning (ML), which allow for automatic response and real-time threat identification. In order to meet data protection standards, innovative application security solutions are also adopted due to regulatory compliance requirements.

Analysis by Type:

Web Application Security

Mobile Application Security

Due to the extensive use of web applications across industries and their high susceptibility to cyber threats, web application security is the most popular type in the market. Because of their heavy reliance on online applications for data interchange, customer interaction, and operational efficiency, organizations are particularly vulnerable to attacks like distributed denial-of-service (DDoS), SQL injection, and cross-site scripting (XSS). The need for strong online application security measures is increased by the expanding use of digital platforms, cloud-based services, and e-commerce. Secure web application environments are also required for compliance with laws like GDPR, PCI DSS, and HIPAA. The adoption of advanced solutions like runtime application self-protection (RASP) and web application firewalls (WAFs) is fueled by their ability to identify and neutralize real-time threats.

Analysis by Testing Type:

Static Application Security Testing (SAST)

Dynamic Application Security Testing (DAST)

Interactive Application Security Testing (IAST)

Runtime Application Self-Protection (RASP)

Static application security testing (SAST) leads the market with 38.6% of market share in 2025. Because it can find vulnerabilities early in the development lifecycle, lowering

costs and increasing productivity, static application security testing (SAST) is the most popular testing type in the market. SAST ensures strong code quality by assisting developers in identifying security vulnerabilities at the root level through source code, binaries, or bytecode analysis prior to application deployment. Its proactive strategy fits nicely with the increasing use of DevSecOps techniques, which include security into the development process. Because it offers thorough coverage across programming languages and frameworks, it is popular and appropriate for a wide range of applications. Organizations are also encouraged to implement comprehensive code analysis to prevent breaches by regulatory compliance standards like GDPR and PCI DSS.

Analysis by Deployment Mode:

On-premises

Cloud-based

On-premises stand as the largest component in 2025, holding 62.5% of the market. Because it appeals to companies that value control, security, and compliance, on-premises deployment is the most popular deployment mode in the application security industry. On-premises solutions are preferred by businesses managing sensitive data, especially those in sectors like government, healthcare, and finance, because they offer direct control over data management and storage. By minimizing dependency on outside vendors, this deployment approach lowers the possibility of security flaws in cloud services. Organizations also employ on-premises solutions to protect data sovereignty and compliance with local laws due to strict regulatory requirements like GDPR and HIPAA. These solutions are highly regarded because they enable firms to customize security measures to meet their unique requirements. Moreover, on-premises deployment is frequently chosen by businesses with outdated systems or poor internet access to guarantee smooth integration.

Analysis by Organization Size:

Large Enterprises

Small and Medium-sized Enterprises

Large enterprises lead the market with 60.0% of market share in 2025. Due to their enormous IT infrastructure, massive data volumes, and increased susceptibility to cyber threats, large organizations hold a dominant position in the market. These companies frequently work in a variety of sectors and regions, which makes them appealing targets for sophisticated cyberattacks like ransomware, data breaches, and advanced persistent threats (APTs). Large corporations make significant investments in complete application security solutions, such as web application firewalls (WAFs), runtime application self-protection (RASP), and static and dynamic application security testing (SAST and DAST), to protect important consumer and corporate data. Adopting strong security measures is additionally required for these firms by regulatory compliance, including GDPR, HIPAA, and PCI DSS. Their operational and financial size also makes it possible for them to spend heavily in cutting-edge technology like artificial intelligence (AI) and machine learning (ML) for real-time threat identification.

Analysis by Industry Vertical:

BFSI

Healthcare

IT and Telecom

Manufacturing

Government and Public Sector

Retail and E-Commerce

Others

IT and telecom leads the market with 27.5% of market share in 2025. Because of its vital role in managing enormous volumes of sensitive data and enabling worldwide communication, the IT and telecom sector is the largest industry vertical in the application security market. Since these sectors deal with consumer information, financial transactions, and communication networks, they are frequently the targets of cyberattacks, such as ransomware, DDoS attacks, and data breaches. The requirement for strong application security solutions is increasing due to the quick adoption of cloud computing, 5G networks, and IoT technologies, which are further increasing their attack

surface. IT and telecom firms are also required to give data protection top priority under regulatory frameworks, such as the CCPA and GDPR. Additionally, the need for web application firewalls and static and dynamic application security testing (SAST and DAST) is fueled by their reliance on sophisticated software and web applications for operations and consumer interaction.

Regional Analysis:

North America

United States

Canada

Asia Pacific

China

Japan

India

South Korea

Australia

Indonesia

Others

Europe

Germany

France

United Kingdom

Italy

Spain

Russia

Others

Latin America

Brazil

Mexico

Others

Middle East and Africa

In 2025, North America accounts for the largest market share of 40.5%. Because of its highly developed technological infrastructure, widespread adoption of digital transformation, and concentration of top cybersecurity companies, North America leads the market. There are a number of significant enterprises and various organizations in industries, including information technology, healthcare, and finance in this region, which call for robust application security measures because the threats keep evolving. The increase in the number of cyberattacks and stringent data protection regulations, such as CCPA and GDPR, is also creating a demand for such integrated security solutions. In North America, the application security products are also complemented by the competitive landscape of the security solutions providers and continuous innovations like artificial intelligence (AI) and machine learning (ML).

KEY REGIONAL TAKEAWAYS:

UNITED STATES APPLICATION SECURITY MARKET ANALYSIS

In 2025, United States accounts for 79.40% of the total North America IT services market share. In the USA, due to the growing need for a digital presence in all areas and the rising threats, the application security market is expanding at a rapid pace. The demand for security service providers indicates an increased need for protection of digital assets. The rapid growth of cloud computing, mobile apps and IoT devices is

resulting in increased attack surfaces for enterprises and thus, enhanced application security is required. In addition, organizations are required to strengthen their security measures on account of compliance issues, such as the California Consumer Privacy Act (CCPA) and the Health Insurance Portability and Accountability Act (HIPAA). Also, the growing complexity of cyber threats, including AI-led attacks, is motivating a lot of organizations to implement newer systems and devices. Moreover, industries, such as healthcare, finance, and retail, that contain sensitive information are more focused in application securing. Thus, the US application security market is increasing in the background of growing complexity of the cyber environment, for robust protection of data breaches as well as compliance with critical regulations.

ASIA PACIFIC APPLICATION SECURITY MARKET ANALYSIS

In the Asia-Pacific region, the market is primarily driven by the rapid expansion of digitalization and the increasing frequency of cyber threats. This heightened threat environment is pushing businesses to invest in stronger application security measures. The region's rapid growth in sectors like banking, telecommunications, and e-commerce, combined with the proliferation of mobile applications and IoT devices, makes enterprises more vulnerable to cyberattacks. Stricter data protection regulations in countries like India and China are further driving the demand for secure application solutions. Additionally, the rise of advanced persistent threats (APTs) and the growing awareness among the masses about data privacy risks are motivating businesses to adopt proactive security measures, ensuring they protect sensitive customer data and comply with regulatory standards.

EUROPE APPLICATION SECURITY MARKET ANALYSIS

The application security market in Europe is experiencing strong growth, driven by stringent data protection regulations like the General Data Protection Regulation (GDPR) and the increasing prevalence of cyberattacks. As European companies adapt to these regulatory demands, securing applications is becoming a critical focus. Additionally, the rapid adoption of artificial intelligence (AI) is contributing to the need for more advanced security measures. As AI integration accelerates, so does the complexity of securing applications, particularly in sectors like finance, healthcare, and retail, which handle large volumes of sensitive data. The rise of digital transformation initiatives, coupled with the increasing sophistication of cyber threats, is driving the demand for comprehensive application security solutions that protect against emerging risks and ensure compliance with evolving regulations.

LATIN AMERICA APPLICATION SECURITY MARKET ANALYSIS

Latin America is increasingly focused on strengthening application security due to the rapid adoption of digital technologies and rising cyber threats. Over the past year, the region has seen a rise in cyberattacks, with industries like banking, healthcare, and telecommunications facing significant risks due to their handling of sensitive data. As digital adoption is accelerating, businesses are prioritizing enhanced application security to mitigate these risks. Stricter regional data protection regulations are also encouraging organizations to adopt advanced security solutions to ensure compliance and safeguard their operations.

MIDDLE EAST AND AFRICA APPLICATION SECURITY MARKET ANALYSIS

The Middle East and Africa region is witnessing a significant rise in demand for application security solutions, driven by increasing cyber threats. This growing threat landscape is encouraging businesses, particularly in sectors like banking, energy, and government, to strengthen their security frameworks. As digital transformation is accelerating, the need to protect applications against cyberattacks is becoming more critical. Additionally, with tightening regulations in countries like the UAE and Saudi Arabia, organizations are prioritizing secure application solutions to mitigate risks and ensure compliance with emerging data protection laws.

COMPETITIVE LANDSCAPE:

To handle evolving cyberthreats and satisfy the rising need for strong security solutions, major competitors in the market are constantly developing. To offer thorough protection throughout the application lifetime, they concentrate on creating cutting-edge solutions including web application firewalls (WAFs), runtime application self-protection (RASP), static application security testing (SAST), and dynamic application security testing (DAST). To improve real-time threat identification and response capabilities, many are utilizing machine learning (ML) and artificial intelligence (AI). Common tactics to guarantee smooth deployment and scalability include cooperation with cloud service providers and integration with DevSecOps procedures. To keep ahead of new risks and legal requirements, these businesses also make significant investments in research and development (R&D) activities.

The report provides a comprehensive analysis of the competitive landscape in the application security market with detailed profiles of all major companies, including:

Black Duck Software, Inc.

Capgemini

Checkmarx Ltd

Cisco Systems, Inc.

Cloudflare, Inc.

Contrast Security

International Business Machines Corporation

NTT DATA, Inc.

Open Text Corporation

Qualys, Inc.

Rapid7

Veracode

Contents

1 PREFACE

2 SCOPE AND METHODOLOGY

- 2.1 Objectives of the Study
- 2.2 Stakeholders
- 2.3 Data Sources
 - 2.3.1 Primary Sources
 - 2.3.2 Secondary Sources
- 2.4 Market Estimation
 - 2.4.1 Bottom-Up Approach
 - 2.4.2 Top-Down Approach
- 2.5 Forecasting Methodology

3 EXECUTIVE SUMMARY

4 INTRODUCTION

- 4.1 Overview
- 4.2 Key Industry Trends

5 GLOBAL APPLICATION SECURITY MARKET

- 5.1 Market Overview
- 5.2 Market Performance
- 5.3 Impact of COVID-19
- 5.4 Market Forecast

6 MARKET BREAKUP BY COMPONENT

- 6.1 Solution
 - 6.1.1 Market Trends
 - 6.1.2 Market Forecast
- 6.2 Services
 - 6.2.1 Market Trends
 - 6.2.2 Market Forecast

7 MARKET BREAKUP BY TYPE

7.1 Web Application Security

7.1.1 Market Trends

7.1.2 Market Forecast

7.2 Mobile Application Security

7.2.1 Market Trends

7.2.2 Market Forecast

8 MARKET BREAKUP BY TESTING TYPE

8.1 Static Application Security Testing (SAST)

8.1.1 Market Trends

8.1.2 Market Forecast

8.2 Dynamic Application Security Testing (DAST)

8.2.1 Market Trends

8.2.2 Market Forecast

8.3 Interactive Application Security Testing (IAST)

8.3.1 Market Trends

8.3.2 Market Forecast

8.4 Runtime Application Self-Protection (RASP)

8.4.1 Market Trends

8.4.2 Market Forecast

9 MARKET BREAKUP BY DEPLOYMENT MODE

9.1 On-premises

9.1.1 Market Trends

9.1.2 Market Forecast

9.2 Cloud-based

9.2.1 Market Trends

9.2.2 Market Forecast

10 MARKET BREAKUP BY ORGANIZATION SIZE

10.1 Large Enterprises

10.1.1 Market Trends

10.1.2 Market Forecast

10.2 Small and Medium-sized Enterprises

- 10.2.1 Market Trends
- 10.2.2 Market Forecast

11 MARKET BREAKUP BY INDUSTRY VERTICAL

- 11.1 BFSI
 - 11.1.1 Market Trends
 - 11.1.2 Market Forecast
- 11.2 Healthcare
 - 11.2.1 Market Trends
 - 11.2.2 Market Forecast
- 11.3 IT and Telecom
 - 11.3.1 Market Trends
 - 11.3.2 Market Forecast
- 11.4 Manufacturing
 - 11.4.1 Market Trends
 - 11.4.2 Market Forecast
- 11.5 Government and Public Sector
 - 11.5.1 Market Trends
 - 11.5.2 Market Forecast
- 11.6 Retail and E-Commerce
 - 11.6.1 Market Trends
 - 11.6.2 Market Forecast
- 11.7 Others
 - 11.7.1 Market Trends
 - 11.7.2 Market Forecast

12 MARKET BREAKUP BY REGION

- 12.1 North America
 - 12.1.1 United States
 - 12.1.1.1 Market Trends
 - 12.1.1.2 Market Forecast
 - 12.1.2 Canada
 - 12.1.2.1 Market Trends
 - 12.1.2.2 Market Forecast
- 12.2 Asia-Pacific
 - 12.2.1 China
 - 12.2.1.1 Market Trends

- 12.2.1.2 Market Forecast
- 12.2.2 Japan
 - 12.2.2.1 Market Trends
 - 12.2.2.2 Market Forecast
- 12.2.3 India
 - 12.2.3.1 Market Trends
 - 12.2.3.2 Market Forecast
- 12.2.4 South Korea
 - 12.2.4.1 Market Trends
 - 12.2.4.2 Market Forecast
- 12.2.5 Australia
 - 12.2.5.1 Market Trends
 - 12.2.5.2 Market Forecast
- 12.2.6 Indonesia
 - 12.2.6.1 Market Trends
 - 12.2.6.2 Market Forecast
- 12.2.7 Others
 - 12.2.7.1 Market Trends
 - 12.2.7.2 Market Forecast
- 12.3 Europe
 - 12.3.1 Germany
 - 12.3.1.1 Market Trends
 - 12.3.1.2 Market Forecast
 - 12.3.2 France
 - 12.3.2.1 Market Trends
 - 12.3.2.2 Market Forecast
 - 12.3.3 United Kingdom
 - 12.3.3.1 Market Trends
 - 12.3.3.2 Market Forecast
 - 12.3.4 Italy
 - 12.3.4.1 Market Trends
 - 12.3.4.2 Market Forecast
 - 12.3.5 Spain
 - 12.3.5.1 Market Trends
 - 12.3.5.2 Market Forecast
 - 12.3.6 Russia
 - 12.3.6.1 Market Trends
 - 12.3.6.2 Market Forecast
 - 12.3.7 Others

- 12.3.7.1 Market Trends
- 12.3.7.2 Market Forecast
- 12.4 Latin America
 - 12.4.1 Brazil
 - 12.4.1.1 Market Trends
 - 12.4.1.2 Market Forecast
 - 12.4.2 Mexico
 - 12.4.2.1 Market Trends
 - 12.4.2.2 Market Forecast
 - 12.4.3 Others
 - 12.4.3.1 Market Trends
 - 12.4.3.2 Market Forecast
- 12.5 Middle East and Africa
 - 12.5.1 Market Trends
 - 12.5.2 Market Breakup by Country
 - 12.5.3 Market Forecast

13 SWOT ANALYSIS

- 13.1 Overview
- 13.2 Strengths
- 13.3 Weaknesses
- 13.4 Opportunities
- 13.5 Threats

14 VALUE CHAIN ANALYSIS

15 PORTERS FIVE FORCES ANALYSIS

- 15.1 Overview
- 15.2 Bargaining Power of Buyers
- 15.3 Bargaining Power of Suppliers
- 15.4 Degree of Competition
- 15.5 Threat of New Entrants
- 15.6 Threat of Substitutes

16 PRICE ANALYSIS

17 COMPETITIVE LANDSCAPE

17.1 Market Structure

17.2 Key Players

17.3 Profiles of Key Players

17.3.1 Black Duck Software, Inc.

17.3.1.1 Company Overview

17.3.1.2 Product Portfolio

17.3.1.3 Financials

17.3.1.4 SWOT Analysis

17.3.2 Capgemini

17.3.2.1 Company Overview

17.3.2.2 Product Portfolio

17.3.2.3 Financials

17.3.2.4 SWOT Analysis

17.3.3 Checkmarx Ltd

17.3.3.1 Company Overview

17.3.3.2 Product Portfolio

17.3.4 Cisco Systems, Inc.

17.3.4.1 Company Overview

17.3.4.2 Product Portfolio

17.3.4.3 Financials

17.3.4.4 SWOT Analysis

17.3.5 Cloudflare, Inc.

17.3.5.1 Company Overview

17.3.5.2 Product Portfolio

17.3.5.3 Financials

17.3.5.4 SWOT Analysis

17.3.6 Contrast Security

17.3.6.1 Company Overview

17.3.6.2 Product Portfolio

17.3.7 International Business Machines Corporation

17.3.7.1 Company Overview

17.3.7.2 Product Portfolio

17.3.7.3 Financials

17.3.7.4 SWOT Analysis

17.3.8 NTT DATA, Inc.

17.3.8.1 Company Overview

17.3.8.2 Product Portfolio

17.3.9 Open Text Corporation

- 17.3.9.1 Company Overview
- 17.3.9.2 Product Portfolio
- 17.3.9.3 Financials
- 17.3.9.4 SWOT Analysis
- 17.3.10 Qualys, Inc.
 - 17.3.10.1 Company Overview
 - 17.3.10.2 Product Portfolio
 - 17.3.10.3 Financials
- 17.3.11 Rapid7
 - 17.3.11.1 Company Overview
 - 17.3.11.2 Product Portfolio
 - 17.3.11.3 Financials
- 17.3.12 Veracode
 - 17.3.12.1 Company Overview
 - 17.3.12.2 Product Portfolio

List Of Tables

LIST OF TABLES

Table 1: Global: Application Security Market: Key Industry Highlights, 2025 and 2034

Table 2: Global: Application Security Market Forecast: Breakup by Component (in Million USD), 2026-2034

Table 3: Global: Application Security Market Forecast: Breakup by Type (in Million USD), 2026-2034

Table 4: Global: Application Security Market Forecast: Breakup by Testing Type (in Million USD), 2026-2034

Table 5: Global: Application Security Market Forecast: Breakup by Deployment Mode (in Million USD), 2026-2034

Table 6: Global: Application Security Market Forecast: Breakup by Organization Size (in Million USD), 2026-2034

Table 7: Global: Application Security Market Forecast: Breakup by Industry Vertical (in Million USD), 2026-2034

Table 8: Global: Application Security Market Forecast: Breakup by Region (in Million USD), 2026-2034

Table 9: Global: Application Security Market: Competitive Structure

Table 10: Global: Application Security Market: Key Players

List Of Figures

LIST OF FIGURES

- Figure 1: Global: Application Security Market: Major Drivers and Challenges
- Figure 2: Global: Application Security Market: Sales Value (in Billion USD), 2020-2025
- Figure 3: Global: Application Security Market Forecast: Sales Value (in Billion USD), 2026-2034
- Figure 4: Global: Application Security Market: Breakup by Component (in %), 2025
- Figure 5: Global: Application Security Market: Breakup by Type (in %), 2025
- Figure 6: Global: Application Security Market: Breakup by Testing Type (in %), 2025
- Figure 7: Global: Application Security Market: Breakup by Deployment Mode (in %), 2025
- Figure 8: Global: Application Security Market: Breakup by Organization Size (in %), 2025
- Figure 9: Global: Application Security Market: Breakup by Industry Vertical (in %), 2025
- Figure 10: Global: Application Security Market: Breakup by Region (in %), 2025
- Figure 11: Global: Application Security (Solution) Market: Sales Value (in Million USD), 2020 & 2025
- Figure 12: Global: Application Security (Solution) Market Forecast: Sales Value (in Million USD), 2026-2034
- Figure 13: Global: Application Security (Services) Market: Sales Value (in Million USD), 2020 & 2025
- Figure 14: Global: Application Security (Services) Market Forecast: Sales Value (in Million USD), 2026-2034
- Figure 15: Global: Application Security (Web Application Security) Market: Sales Value (in Million USD), 2020 & 2025
- Figure 16: Global: Application Security (Web Application Security) Market Forecast: Sales Value (in Million USD), 2026-2034
- Figure 17: Global: Application Security (Mobile Application Security) Market: Sales Value (in Million USD), 2020 & 2025
- Figure 18: Global: Application Security (Mobile Application Security) Market Forecast: Sales Value (in Million USD), 2026-2034
- Figure 19: Global: Application Security (Static Application Security Testing-SAST) Market: Sales Value (in Million USD), 2020 & 2025
- Figure 20: Global: Application Security (Static Application Security Testing-SAST) Market Forecast: Sales Value (in Million USD), 2026-2034
- Figure 21: Global: Application Security (Dynamic Application Security Testing-DAST) Market: Sales Value (in Million USD), 2020 & 2025
- Figure 22: Global: Application Security (Dynamic Application Security Testing-DAST)

Market Forecast: Sales Value (in Million USD), 2026-2034

Figure 23: Global: Application Security (Interactive Application Security Testing-IAST) Market: Sales Value (in Million USD), 2020 & 2025

Figure 24: Global: Application Security (Interactive Application Security Testing-IAST) Market Forecast: Sales Value (in Million USD), 2026-2034

Figure 25: Global: Application Security (Runtime Application Self-Protection-RASP) Market: Sales Value (in Million USD), 2020 & 2025

Figure 26: Global: Application Security (Runtime Application Self-Protection-RASP) Market Forecast: Sales Value (in Million USD), 2026-2034

Figure 27: Global: Application Security (On-premises) Market: Sales Value (in Million USD), 2020 & 2025

Figure 28: Global: Application Security (On-premises) Market Forecast: Sales Value (in Million USD), 2026-2034

Figure 29: Global: Application Security (Cloud-based) Market: Sales Value (in Million USD), 2020 & 2025

Figure 30: Global: Application Security (Cloud-based) Market Forecast: Sales Value (in Million USD), 2026-2034

Figure 31: Global: Application Security (Large Enterprises) Market: Sales Value (in Million USD), 2020 & 2025

Figure 32: Global: Application Security (Large Enterprises) Market Forecast: Sales Value (in Million USD), 2026-2034

Figure 33: Global: Application Security (Small and Medium-sized Enterprises) Market: Sales Value (in Million USD), 2020 & 2025

Figure 34: Global: Application Security (Small and Medium-sized Enterprises) Market Forecast: Sales Value (in Million USD), 2026-2034

Figure 35: Global: Application Security (BFSI) Market: Sales Value (in Million USD), 2020 & 2025

Figure 36: Global: Application Security (BFSI) Market Forecast: Sales Value (in Million USD), 2026-2034

Figure 37: Global: Application Security (Healthcare) Market: Sales Value (in Million USD), 2020 & 2025

Figure 38: Global: Application Security (Healthcare) Market Forecast: Sales Value (in Million USD), 2026-2034

Figure 39: Global: Application Security (IT and Telecom) Market: Sales Value (in Million USD), 2020 & 2025

Figure 40: Global: Application Security (IT and Telecom) Market Forecast: Sales Value (in Million USD), 2026-2034

Figure 41: Global: Application Security (Manufacturing) Market: Sales Value (in Million USD), 2020 & 2025

Figure 42: Global: Application Security (Manufacturing) Market Forecast: Sales Value (in Million USD), 2026-2034

Figure 43: Global: Application Security (Government and Public Sector) Market: Sales Value (in Million USD), 2020 & 2025

Figure 44: Global: Application Security (Government and Public Sector) Market Forecast: Sales Value (in Million USD), 2026-2034

Figure 45: Global: Application Security (Retail and E-Commerce) Market: Sales Value (in Million USD), 2020 & 2025

Figure 46: Global: Application Security (Retail and E-Commerce) Market Forecast: Sales Value (in Million USD), 2026-2034

Figure 47: Global: Application Security (Other Industry Verticals) Market: Sales Value (in Million USD), 2020 & 2025

Figure 48: Global: Application Security (Other Industry Verticals) Market Forecast: Sales Value (in Million USD), 2026-2034

Figure 49: North America: Application Security Market: Sales Value (in Million USD), 2020 & 2025

Figure 50: North America: Application Security Market Forecast: Sales Value (in Million USD), 2026-2034

Figure 51: United States: Application Security Market: Sales Value (in Million USD), 2020 & 2025

Figure 52: United States: Application Security Market Forecast: Sales Value (in Million USD), 2026-2034

Figure 53: Canada: Application Security Market: Sales Value (in Million USD), 2020 & 2025

Figure 54: Canada: Application Security Market Forecast: Sales Value (in Million USD), 2026-2034

Figure 55: Asia-Pacific: Application Security Market: Sales Value (in Million USD), 2020 & 2025

Figure 56: Asia-Pacific: Application Security Market Forecast: Sales Value (in Million USD), 2026-2034

Figure 57: China: Application Security Market: Sales Value (in Million USD), 2020 & 2025

Figure 58: China: Application Security Market Forecast: Sales Value (in Million USD), 2026-2034

Figure 59: Japan: Application Security Market: Sales Value (in Million USD), 2020 & 2025

Figure 60: Japan: Application Security Market Forecast: Sales Value (in Million USD), 2026-2034

Figure 61: India: Application Security Market: Sales Value (in Million USD), 2020 & 2025

Figure 62: India: Application Security Market Forecast: Sales Value (in Million USD), 2026-2034

Figure 63: South Korea: Application Security Market: Sales Value (in Million USD), 2020 & 2025

Figure 64: South Korea: Application Security Market Forecast: Sales Value (in Million USD), 2026-2034

Figure 65: Australia: Application Security Market: Sales Value (in Million USD), 2020 & 2025

Figure 66: Australia: Application Security Market Forecast: Sales Value (in Million USD), 2026-2034

Figure 67: Indonesia: Application Security Market: Sales Value (in Million USD), 2020 & 2025

Figure 68: Indonesia: Application Security Market Forecast: Sales Value (in Million USD), 2026-2034

Figure 69: Others: Application Security Market: Sales Value (in Million USD), 2020 & 2025

Figure 70: Others: Application Security Market Forecast: Sales Value (in Million USD), 2026-2034

Figure 71: Europe: Application Security Market: Sales Value (in Million USD), 2020 & 2025

Figure 72: Europe: Application Security Market Forecast: Sales Value (in Million USD), 2026-2034

Figure 73: Germany: Application Security Market: Sales Value (in Million USD), 2020 & 2025

Figure 74: Germany: Application Security Market Forecast: Sales Value (in Million USD), 2026-2034

Figure 75: France: Application Security Market: Sales Value (in Million USD), 2020 & 2025

Figure 76: France: Application Security Market Forecast: Sales Value (in Million USD), 2026-2034

Figure 77: United Kingdom: Application Security Market: Sales Value (in Million USD), 2020 & 2025

Figure 78: United Kingdom: Application Security Market Forecast: Sales Value (in Million USD), 2026-2034

Figure 79: Italy: Application Security Market: Sales Value (in Million USD), 2020 & 2025

Figure 80: Italy: Application Security Market Forecast: Sales Value (in Million USD), 2026-2034

Figure 81: Spain: Application Security Market: Sales Value (in Million USD), 2020 & 2025

Figure 82: Spain: Application Security Market Forecast: Sales Value (in Million USD), 2026-2034

Figure 83: Russia: Application Security Market: Sales Value (in Million USD), 2020 & 2025

Figure 84: Russia: Application Security Market Forecast: Sales Value (in Million USD), 2026-2034

Figure 85: Others: Application Security Market: Sales Value (in Million USD), 2020 & 2025

Figure 86: Others: Application Security Market Forecast: Sales Value (in Million USD), 2026-2034

Figure 87: Latin America: Application Security Market: Sales Value (in Million USD), 2020 & 2025

Figure 88: Latin America: Application Security Market Forecast: Sales Value (in Million USD), 2026-2034

Figure 89: Brazil: Application Security Market: Sales Value (in Million USD), 2020 & 2025

Figure 90: Brazil: Application Security Market Forecast: Sales Value (in Million USD), 2026-2034

Figure 91: Mexico: Application Security Market: Sales Value (in Million USD), 2020 & 2025

Figure 92: Mexico: Application Security Market Forecast: Sales Value (in Million USD), 2026-2034

Figure 93: Others: Application Security Market: Sales Value (in Million USD), 2020 & 2025

Figure 94: Others: Application Security Market Forecast: Sales Value (in Million USD), 2026-2034

Figure 95: Middle East and Africa: Application Security Market: Sales Value (in Million USD), 2020 & 2025

Figure 96: Middle East and Africa: Application Security Market: Breakup by Country (in %), 2025

Figure 97: Middle East and Africa: Application Security Market Forecast: Sales Value (in Million USD), 2026-2034

Figure 98: Global: Application Security Industry: SWOT Analysis

Figure 99: Global: Application Security Industry: Value Chain Analysis

Figure 100: Global: Application Security Industry: Porter's Five Forces Analysis

I would like to order

Product name: Application Security Market Size, Share, Trends and Forecast by Component, Type, Testing Type, Deployment Mode, Organization Size, Industry Vertical, and Region, 2026-2034

Product link: <https://marketpublishers.com/r/A7D7E03056B6EN.html>

Price: US\$ 3,999.00 (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/A7D7E03056B6EN.html>