

# **Vietnam Application Security Market, By Testing Type (Static Application Security Testing, Dynamic Application Security Testing, Interactive Application Security Testing), By Component (Services, Solution), By Organization Size (Large Enterprises, Small & Medium Enterprises), By Deployment Type (Cloud, On-Premises), By Industry vertical (Government & Defense, Healthcare, IT & Telecom, Government, Education, Others), By Region, Competition, Forecast and Opportunities, 2019-2029F**

<https://marketpublishers.com/r/V278FA1C5FBBEN.html>

Date: June 2024

Pages: 83

Price: US\$ 3,500.00 (Single User License)

ID: V278FA1C5FBBEN

## **Abstracts**

Vietnam Application Security Market was valued at USD 843.25 Million in 2023 and is anticipated to project robust growth in the forecast period with a CAGR of 13.79% through 2029F. Vietnam's Application Security market pertains to the strategies and technologies implemented to safeguard software applications from cyber threats, ensuring their confidentiality, integrity, and availability. The market is witnessing a notable surge, primarily propelled by the accelerating digitalization of businesses across diverse sectors. As companies increasingly rely on software applications to streamline operations and deliver services, the imperative for robust security measures becomes paramount.

This growth trajectory is further fueled by the escalating sophistication and frequency of cyber attacks, prompting organizations to prioritize investments in application security solutions. Heightened awareness, coupled with the repercussions of high-profile data breaches, underscores the criticality of fortifying defenses against evolving

threats.

Regulatory mandates and compliance standards also exert significant influence, compelling businesses to shore up their security posture and adhere to stringent data protection regulations. In response, organizations are embracing advanced technologies and methodologies to detect and mitigate security risks effectively. The proliferation of cloud computing, mobile technologies, and Internet of Things (IoT) devices expands the attack surface, necessitating comprehensive security measures. As applications and data become increasingly distributed across diverse environments, the demand for robust security solutions continues to escalate.

In essence, the growth prospects of the Vietnam Application Security market are intricately tied to the imperative for businesses to fortify their digital infrastructure against cyber threats amidst the backdrop of accelerating digital transformation and regulatory pressures. As organizations navigate this landscape, the adoption of robust application security solutions will remain a strategic imperative to mitigate risks and safeguard critical assets.

## Key Market Drivers

### Digital Transformation Initiatives Driving Demand

Vietnamese businesses are undergoing rapid digital transformation, fueled by evolving consumer preferences and technological advancements. This shift towards digitization necessitates a heightened focus on application security as organizations increasingly rely on software applications to drive operational efficiency and customer engagement. With the proliferation of digital channels and platforms, the attack surface for cyber threats expands, prompting businesses to invest in robust security measures to safeguard their digital assets and ensure uninterrupted business operations. By prioritizing application security, businesses can not only mitigate risks but also enhance their competitive advantage by demonstrating a commitment to protecting customer data and maintaining the integrity of their applications.

### Regulatory Landscape and Compliance Requirements

The regulatory environment in Vietnam is becoming increasingly stringent concerning data protection and cybersecurity, necessitating a proactive approach to application security. With the introduction of laws such as the Law on Cybersecurity and alignment with global standards like GDPR, organizations face heightened accountability for

securing sensitive data. Compliance with data privacy regulations requires the implementation of robust security measures to protect against unauthorized access and data breaches. Additionally, adherence to risk management frameworks such as the NIST Cybersecurity Framework is essential for organizations to assess and mitigate application security risks effectively. By aligning with regulatory requirements and establishing robust incident response protocols, businesses can mitigate legal and financial risks while preserving customer trust and loyalty.

## Evolving Threat Landscape and Technological Advancements

The cybersecurity landscape is continuously evolving, with threat actors employing increasingly sophisticated techniques to exploit vulnerabilities in software applications. In response, the application security market is witnessing a wave of innovation driven by advancements in technology. Next-generation application security solutions equipped with threat intelligence, behavioral analytics, and machine learning capabilities are enabling organizations to detect and respond to emerging threats in real-time. Moreover, the adoption of a 'shift left' approach, integrating security practices into the software development lifecycle, is becoming increasingly prevalent. By embracing innovative technologies and proactive security measures, businesses can mitigate risks, enhance their security posture, and safeguard their digital assets against evolving cyber threats.

## Key Market Challenges

### Evolving Threat Landscape and Technological Adaptation

Vietnam's application security market faces a significant challenge in keeping pace with the rapidly evolving threat landscape. As cyber threats become increasingly sophisticated and diverse, the methods of attack on applications have grown more complex and harder to detect. This dynamic threat environment is exacerbated by the rise of advanced persistent threats, zero-day vulnerabilities, and state-sponsored cyber activities. Businesses must continuously update and adapt their security measures to defend against these emerging threats. The challenge lies not only in identifying and mitigating these sophisticated attacks but also in the necessity for continuous investment in cutting-edge technologies and cybersecurity expertise.

To address this challenge, Vietnamese enterprises need to invest heavily in advanced security solutions such as artificial intelligence (AI)-powered threat detection, machine learning algorithms for anomaly detection, and blockchain technology for

secure data transactions. However, this requires a substantial financial commitment and a robust understanding of these technologies, which are often lacking. Moreover, the rapid digital transformation in Vietnam means that many businesses are still in the nascent stages of their cybersecurity journeys. They may not have the necessary infrastructure or skilled personnel to implement and maintain these advanced security measures. Thus, the combination of a fast-evolving threat landscape and the high cost of technological adaptation presents a formidable challenge for Vietnam's application security market.

Furthermore, the regulatory environment adds another layer of complexity. With new data protection regulations and cybersecurity laws being enacted, businesses must ensure compliance while simultaneously upgrading their security frameworks. This regulatory pressure can divert resources away from proactive security investments toward compliance-related expenditures. For Vietnamese businesses, particularly small and medium-sized enterprises (SMEs), which form the backbone of the economy, balancing these demands can be particularly challenging. Therefore, the evolving threat landscape and the necessity for technological adaptation pose a substantial obstacle that requires a strategic and well-resourced response.

### Skill Shortage and Workforce Development

Another critical challenge confronting the Vietnam application security market is the acute shortage of skilled cybersecurity professionals. Despite the burgeoning demand for application security experts, the supply of qualified personnel has not kept pace. This gap is particularly pronounced in specialized areas such as application security testing, secure software development, and incident response. The skill shortage is a multifaceted issue stemming from inadequate cybersecurity education and training, limited professional development opportunities, and a lack of industry-academic collaboration to cultivate relevant skills.

The educational infrastructure in Vietnam has traditionally lagged in producing graduates with the necessary cybersecurity expertise. While there are numerous IT graduates, only a small fraction possess the specialized skills required for application security roles. This inadequacy is due in part to outdated curricula that do not align with the latest industry standards and practices. Moreover, there is a dearth of hands-on training programs that provide real-world experience in tackling cybersecurity threats. As a result, businesses often find it difficult to recruit individuals who are immediately capable of handling the complexities of modern application security.

Workforce development is further hampered by the rapid technological changes and the continuous emergence of new security threats, which necessitate ongoing education and skills enhancement. However, opportunities for continuous professional development are limited, leaving many professionals with outdated skills. This situation is exacerbated by the high turnover rates in the cybersecurity field, where skilled professionals are often lured by lucrative offers from abroad, leading to a brain drain. Companies are then compelled to invest considerable time and resources into training new employees, which can be both time-consuming and costly.

Additionally, there is an urgent need for stronger collaboration between industry and academic institutions to address the skills gap. Industry-driven certification programs, internships, and collaborative research projects can help bridge this gap by providing students with practical skills and up-to-date knowledge. However, fostering such collaborations requires concerted efforts and investments from both sectors. Addressing the skill shortage challenge is imperative for the growth of Vietnam's application security market, as a well-trained and adequately skilled workforce is essential for implementing robust security measures and responding effectively to cyber threats.

## Key Market Trends

### Adoption of Artificial Intelligence and Machine Learning in Security Solutions

The Vietnam application security market is increasingly adopting artificial intelligence (AI) and machine learning (ML) technologies to enhance security solutions. These advanced technologies are pivotal in identifying and mitigating complex cyber threats that traditional security measures might miss. AI and ML algorithms can analyze vast amounts of data to detect patterns and anomalies indicative of potential security breaches. By leveraging these technologies, businesses can proactively address security vulnerabilities and respond swiftly to emerging threats.

AI-driven security solutions are particularly effective in identifying zero-day vulnerabilities and sophisticated attack vectors, providing a crucial layer of defense against increasingly sophisticated cybercriminals. Machine learning models can be trained to recognize normal behavior within applications, enabling them to flag deviations that may signify malicious activity. This continuous learning process allows for adaptive security measures that evolve in tandem with the threat landscape.

The trend towards AI and ML adoption is driven by the need for more efficient and effective security solutions capable of handling the growing volume and complexity of

cyber threats. As Vietnamese businesses undergo digital transformation, the integration of these advanced technologies into their security frameworks is becoming essential. Companies that invest in AI and ML-based security solutions are likely to gain a competitive edge by enhancing their ability to protect sensitive data and maintain robust cybersecurity postures.

### Increasing Focus on DevSecOps Integration

Another significant trend in the Vietnam application security market is the increasing focus on integrating security practices into the DevOps process, known as DevSecOps. This approach emphasizes the importance of embedding security measures throughout the software development lifecycle, rather than treating security as an afterthought. By incorporating security from the outset, businesses can identify and address vulnerabilities early in the development process, reducing the risk of security breaches in deployed applications.

DevSecOps promotes a culture of shared responsibility for security among development, operations, and security teams. This collaborative approach ensures that security considerations are integrated into every phase of development, from initial design to final deployment. The adoption of DevSecOps practices is facilitated by the use of automated security tools that can perform continuous security testing and monitoring, providing real-time feedback to developers.

The trend towards DevSecOps is gaining momentum as businesses recognize the benefits of this proactive approach to application security. By integrating security into the development process, companies can achieve faster delivery of secure applications, improve compliance with security standards, and enhance their overall security posture. As Vietnamese enterprises increasingly adopt agile and DevOps methodologies, the integration of DevSecOps practices is becoming a critical component of their application security strategies.

### Growth of Managed Security Service Providers

The growth of managed security service providers (MSSPs) is a notable trend in the Vietnam application security market. MSSPs offer outsourced security services, providing businesses with access to expert security resources and technologies without the need for substantial internal investments. This trend is particularly beneficial for small and medium-sized enterprises (SMEs) that may lack the in-house expertise and financial resources to implement comprehensive security measures.



MSSPs provide a range of services, including threat monitoring, incident response, vulnerability management, and compliance support. By partnering with MSSPs, businesses can benefit from continuous monitoring and rapid response to security incidents, ensuring that their applications are protected around the clock. The scalability of MSSP services allows businesses to tailor their security solutions to their specific needs and budget constraints.

The increasing reliance on MSSPs is driven by the growing complexity of the threat landscape and the shortage of skilled cybersecurity professionals. By leveraging the expertise of MSSPs, Vietnamese businesses can enhance their security capabilities and focus on their core operations. This trend is expected to continue as more businesses recognize the value of outsourcing their security functions to specialized providers, enabling them to stay ahead of evolving cyber threats and maintain robust security postures.

## Segmental Insights

### Testing Type Insights

In 2023, the Static Application Security Testing segment dominated the Vietnam Application Security Market and is anticipated to maintain its leadership throughout the forecast period. This dominance is driven by its integral role in the early stages of software development, enabling the identification and rectification of vulnerabilities in the source code before applications go live. The Vietnamese market highly values this proactive approach, prioritizing robust and secure software solutions. Additionally, increasing regulatory requirements and the need for compliance with international security standards have led organizations to adopt Static Application Security Testing tools more extensively. Growing awareness of cyber threats and the associated financial and reputational risks has also fueled demand for comprehensive security measures, with Static Application Security Testing being a fundamental component. Government initiatives to bolster cybersecurity infrastructure and promote best practices among businesses have further accelerated adoption. Rapid digital transformation and the proliferation of software applications across various sectors, including banking, finance, healthcare, and e-commerce, have heightened the need for rigorous security testing to protect sensitive data and ensure operational integrity. Consequently, organizations are increasingly investing in advanced Static Application Security Testing solutions to enhance their security posture and mitigate risks. This segment is expected to remain dominant in the Vietnam Application Security Market,

supported by its critical role in ensuring software security and compliance, as well as the growing emphasis on preventive security measures in an evolving threat landscape.

## Component Insights

In 2023, the Solution segment led the Vietnam Application Security Market and is projected to maintain its dominance throughout the forecast period. This market dominance is attributed to several strategic factors. Solutions, comprising various software and tools tailored for detecting and mitigating security vulnerabilities, stand as vital assets in safeguarding applications against increasingly sophisticated cyber threats. Vietnamese enterprises prioritize investments in comprehensive application security solutions to shield critical data and uphold operational integrity. The escalating frequency of cyber attacks and data breaches has elevated awareness and urgency surrounding application security, propelling demand for robust solutions offering real-time protection and advanced threat detection capabilities. Furthermore, the evolving regulatory landscape in Vietnam, characterized by stricter compliance requirements, compels businesses to embrace advanced security solutions to avert penalties and uphold customer trust. The rapid digital transformation across sectors like finance, healthcare, and e-commerce has amplified reliance on software applications, intensifying the imperative for effective security measures. Solutions are favored for their scalability, seamless integration, and ability to deliver comprehensive security coverage throughout the application lifecycle. Moreover, technological innovations within security solutions, including the integration of artificial intelligence and machine learning for heightened threat detection and response capabilities, render them increasingly appealing to organizations seeking state-of-the-art protection. Government initiatives aimed at fortifying cybersecurity infrastructure and fostering best practices further bolster the adoption of advanced security solutions. Consequently, businesses are increasingly allocating resources towards these solutions to ensure compliance, safeguard sensitive information, and mitigate risks associated with cyber threats. Hence, the Solution segment is poised to retain its prominent position in the Vietnam Application Security Market, driven by its indispensable role in addressing the multifaceted security challenges confronting contemporary enterprises.

## Regional Insights

In 2023, South Vietnam emerged as the dominant region in the Vietnam Application Security Market and is anticipated to uphold its leadership throughout the forecast period. This dominance is rooted in various strategic factors unique to the region. South Vietnam, encompassing key economic hubs such as Ho Chi Minh City and its



surrounding areas, represents a dynamic business landscape characterized by a robust digital infrastructure and a thriving technology ecosystem. The region's prominence is further fueled by its concentration of multinational corporations, large enterprises, and rapidly growing startups, all of which prioritize the implementation of comprehensive application security measures to safeguard their digital assets and maintain competitive advantage. Additionally, South Vietnam's strategic geographical location and connectivity to global markets position it as a hub for international trade and investment, driving heightened awareness and investment in cutting-edge security solutions to mitigate cyber risks and ensure business continuity. Furthermore, the region's proactive regulatory environment, coupled with initiatives aimed at fostering innovation and cybersecurity resilience, reinforces the adoption of advanced application security technologies among businesses. The presence of leading cybersecurity firms and research institutions also contributes to South Vietnam's dominance in the market, facilitating the development and deployment of innovative security solutions tailored to the region's specific needs and challenges. As digital transformation accelerates across industries such as finance, e-commerce, and telecommunications, South Vietnam remains at the forefront of adopting and adapting emerging technologies, including artificial intelligence and cloud-based security solutions, to address evolving cyber threats effectively. With these factors driving sustained growth and investment in application security, South Vietnam is poised to maintain its dominance in the Vietnam Application Security Market, supported by its vibrant economy, technological leadership, and proactive approach to cybersecurity.

## Key Market Players

Check Point Software Technologies Ltd.

Palo Alto Networks, Inc.

Broadcom Inc

IBM Corporation

Fortinet, Inc.

Cisco Systems, Inc.

McAfee, LLC

Trend Micro Incorporated

Qualys, Inc.

Rapid7, Inc.

Report Scope:

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

Vietnam Application Security Market, By Testing Type:

Static Application Security Testing

Dynamic Application Testing

Interactive Application Security Testing

Vietnam Application Security Market, By Component:

Solutions

Services

Vietnam Application Security Market, By Organization Size:

Small & Medium Enterprise

Large Enterprise

Vietnam Application Security Market, By Deployment Type:

Cloud

On-premises

Vietnam Application Security Market, By Industry vertical:

Government & Defense

Healthcare

IT & Telecom

Government

Education

Others

Vietnam Application Security Market, By Region:

North Vietnam

South Vietnam

Central Vietnam

Competitive Landscape

Company Profiles: Detailed analysis of the major companies present in the Vietnam Application Security Market.

Available Customizations:

Vietnam Application Security Market report with the given market data, Tech Sci 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).

## Contents

### **1. SERVICE OVERVIEW**

- 1.1. Market Definition
- 1.2. Scope of the Market
  - 1.2.1. Markets Covered
  - 1.2.2. Years Considered for Study
  - 1.2.3. Key Market Segmentations

### **2. RESEARCH METHODOLOGY**

- 2.1. Objective of the Study
- 2.2. Baseline Methodology
- 2.3. Formulation of the Scope
- 2.4. Assumptions and Limitations
- 2.5. Sources of Research
  - 2.5.1. Secondary Research
  - 2.5.2. Primary Research
- 2.6. Approach for the Market Study
  - 2.6.1. The Bottom-Up Approach
  - 2.6.2. The Top-Down Approach
- 2.7. Methodology Followed for Calculation of Market Size & Market Shares
- 2.8. Forecasting Methodology
  - 2.8.1. Data Triangulation & Validation

### **3. EXECUTIVE SUMMARY**

### **4. IMPACT OF COVID-19 ON VIETNAM APPLICATION SECURITY MARKET**

### **5. VOICE OF CUSTOMER**

### **6. VIETNAM APPLICATION SECURITY MARKET OVERVIEW**

### **7. VIETNAM APPLICATION SECURITY MARKET OUTLOOK**

- 7.1. Market Size & Forecast
  - 7.1.1. By Value
- 7.2. Market Share & Forecast

7.2.1.By Testing Type (Static Application Security Testing, Dynamic Application Security Testing, Interactive Application Security Testing)

7.2.2.By Component (Services, Solution)

7.2.3.By Organization Size (Large Enterprises, Small & Medium Enterprises)

7.2.4.By Deployment Type (Cloud, On-Premises)

7.2.5.By Industry vertical (BFSI, Government, Healthcare, Retail, IT)

7.2.6.By Region (North Vietnam, South Vietnam, Central Vietnam)

7.3. By Company (2023)

7.4. Market Map

## **8. NORTH VIETNAM APPLICATION SECURITY MARKET OUTLOOK**

8.1. Market Size & Forecast

8.1.1.By Value

8.2. Market Share & Forecast

8.2.1.By Testing Type

8.2.2.By Component

8.2.3.By Organization Size

8.2.4.By Deployment Type

8.2.5.By Industry vertical

## **9. SOUTH VIETNAM APPLICATION SECURITY MARKET OUTLOOK**

9.1. Market Size & Forecast

9.1.1.By Value

9.2. Market Share & Forecast

9.2.1.By Testing Type

9.2.2.By Component

9.2.3.By Organization Size

9.2.4.By Deployment Type

9.2.5.By Industry vertical

## **10. CENTRAL VIETNAM APPLICATION SECURITY MARKET OUTLOOK**

10.1. Market Size & Forecast

10.1.1. By Value

10.2. Market Share & Forecast

10.2.1. By Testing Type

10.2.2. By Component



- 10.2.3. By Organization Size
- 10.2.4. By Deployment Type
- 10.2.5. By Industry vertical

## **11. MARKET DYNAMICS**

- 11.1. Drivers
- 11.2. Challenges

## **12. MARKET TRENDS AND DEVELOPMENTS**

## **13. COMPANY PROFILES**

- 13.1. Check Point Software Technologies Ltd.
  - 13.1.1. Business Overview
  - 13.1.2. Key Revenue and Financials
  - 13.1.3. Recent Developments
  - 13.1.4. Key Personnel/Key Contact Person
  - 13.1.5. Key Product/Services Offered
- 13.2. Palo Alto Networks, Inc.
  - 13.2.1. Business Overview
  - 13.2.2. Key Revenue and Financials
  - 13.2.3. Recent Developments
  - 13.2.4. Key Personnel/Key Contact Person
  - 13.2.5. Key Product/Services Offered
- 13.3. Broadcom Inc
  - 13.3.1. Business Overview
  - 13.3.2. Key Revenue and Financials
  - 13.3.3. Recent Developments
  - 13.3.4. Key Personnel/Key Contact Person
  - 13.3.5. Key Product/Services Offered
- 13.4. IBM Corporation
  - 13.4.1. Business Overview
  - 13.4.2. Key Revenue and Financials
  - 13.4.3. Recent Developments
  - 13.4.4. Key Personnel/Key Contact Person
  - 13.4.5. Key Product/Services Offered
- 13.5. Fortinet, Inc.
  - 13.5.1. Business Overview

- 13.5.2. Key Revenue and Financials
- 13.5.3. Recent Developments
- 13.5.4. Key Personnel/Key Contact Person
- 13.5.5. Key Product/Services Offered
- 13.6. Cisco Systems, Inc.
  - 13.6.1. Business Overview
  - 13.6.2. Key Revenue and Financials
  - 13.6.3. Recent Developments
  - 13.6.4. Key Personnel/Key Contact Person
  - 13.6.5. Key Product/Services Offered
- 13.7. McAfee, LLC
  - 13.7.1. Business Overview
  - 13.7.2. Key Revenue and Financials
  - 13.7.3. Recent Developments
  - 13.7.4. Key Personnel/Key Contact Person
  - 13.7.5. Key Product/Services Offered
- 13.8. Trend Micro Incorporated
  - 13.8.1. Business Overview
  - 13.8.2. Key Revenue and Financials
  - 13.8.3. Recent Developments
  - 13.8.4. Key Personnel/Key Contact Person
  - 13.8.5. Key Product/Services Offered
- 13.9. Qualys, Inc.
  - 13.9.1. Business Overview
  - 13.9.2. Key Revenue and Financials
  - 13.9.3. Recent Developments
  - 13.9.4. Key Personnel/Key Contact Person
  - 13.9.5. Key Product/Services Offered
- 13.10. Rapid7, Inc.
  - 13.10.1. Business Overview
  - 13.10.2. Key Revenue and Financials
  - 13.10.3. Recent Developments
  - 13.10.4. Key Personnel/Key Contact Person
  - 13.10.5. Key Product/Services Offered

## **14. STRATEGIC RECOMMENDATIONS**

## **15. ABOUT US & DISCLAIMER**

## I would like to order

Product name: Vietnam Application Security Market, By Testing Type (Static Application Security Testing, Dynamic Application Security Testing, Interactive Application Security Testing), By Component (Services, Solution), By Organization Size (Large Enterprises, Small & Medium Enterprises), By Deployment Type (Cloud, On-Premises), By Industry vertical (Government & Defense, Healthcare, IT & Telecom, Government, Education, Others), By Region, Competition, Forecast and Opportunities, 2019-2029F

Product link: <https://marketpublishers.com/r/V278FA1C5FBBEN.html>

Price: US\$ 3,500.00 (Single User License / Electronic Delivery)

If you want to order Corporate License or Hard Copy, please, contact our Customer Service:

[info@marketpublishers.com](mailto:info@marketpublishers.com)

## Payment

To pay by Credit Card (Visa, MasterCard, American Express, PayPal), please, click button on product page <https://marketpublishers.com/r/V278FA1C5FBBEN.html>

To pay by Wire Transfer, please, fill in your contact details in the form below:

First name:  
Last name:  
Email:  
Company:  
Address:  
City:  
Zip code:  
Country:  
Tel:  
Fax:  
Your message:

**\*\*All fields are required**

Customer signature \_\_\_\_\_

Please, note that by ordering from marketpublishers.com you are agreeing to our Terms

& Conditions at <https://marketpublishers.com/docs/terms.html>

To place an order via fax simply print this form, fill in the information below  
and fax the completed form to +44 20 7900 3970