

## **Asia Pacific Security Testing Market - Growth, Trends, Covid-19 Impact, and Forecasts (2023 - 2028)**

Market Report | 2023-01-23 | 120 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:**

Asia Pacific Security Testing Market is expected to register a CAGR of 10% during the forecast period 2022-2027.

#### Key Highlights

The demand for security testing in this region is expected to increase with the escalation in the number of attacks that countries in the region are battling every day. Both private companies and governments are battling cyber-attacks on their networks every day. Singapore was under siege from cyber-criminals last year, and for 229 days, cyber-criminals plundered and phished data out from government sites. Other countries like India, the Philippines, and South Korea also face constant cyber-attacks.

As enterprises consider providing comprehensive visibility along with advanced layer security, including intrusion prevention, web filtering, threat protection, and application control, they face a major challenge managing these point products with no integration and lack of visibility.

Security Testing will ensure that the systems and applications on a network it is secure or not. The evolution of Dynamic application security testing beyond the security testing of back-end web applications has opened up new avenues for the security testing market. They now have the capabilities to test next-generation applications. The ability of some of the testing providers to enable interaction between their static and dynamic security testing techniques provides more detailed information, which is quite useful in QA testing to provide more meaningful results to developers.

It has been estimated that over 99% of actual attacks are listed as known Common Vulnerabilities and Exposures (CVEs). A traditional defense is probing the system using manual or automatic vulnerability scanning techniques. However, this produces a lot of redundant and irrelevant information that does not shed any light as to whether a hacker can use the vulnerability to reach a critical asset. The only solution today is human penetration testing, but infrequent testing does not reflect the network's dynamic nature, especially in today's virtual and cloud-based environments.

These solutions are used to protect both web-based and mobile-based applications from vulnerabilities and threats by installing

**Scotts International. EU Vat number: PL 6772247784**

tel. 0048 603 394 346 e-mail: [support@scotts-international.com](mailto:support@scotts-international.com)

[www.scotts-international.com](http://www.scotts-international.com)

encryption applications and various security testing procedures during the application development life cycle. Business applications hold critical organizational data and are the target of cybercriminals.

The emergence of HTML5, which requires higher levels of maturity and adoption, is driving innovation in DAST. The emergence of cloud computing, along with the ability to offer Testing as a Service (TaaS) with the flexibility to test sensitive applications on-premises and outsource others, has enabled firms across various sectors like BFSI, Government, and Public Sector, Healthcare, and Retail to include testing in their operations.

## APAC Security Testing market Trends

### Transition to online payment methods

In the Asia Pacific, investments in security-oriented products such as security testing, endpoint security, VPN, and firewalls bumped up due to the increased spending by both governments and enterprises (particularly in the banking, telecom, and professional services industry). Australia and India are the next two largest countries in terms of security spending due to the presence of a large number of businesses catering to domestic as well as international customers.

Demand for safety when online triggered user growth amidst the transition of the financial industry into digitization. According to the 2021 Kaspersky Digital Payment Report, more than 50% of the surveyed noted a surge in digital payment methods during the pandemic for its convenience during the pandemic with nearly 90% of Asian respondents reported having used mobile payment apps at least once in the last year.

The Philippines registered the highest growth in new e-cash adopters at 37%, followed by India (23%), Australia (15%), Vietnam (14%), Indonesia (13%), and Thailand (13%). The lowest number of first-time online payment users were recorded in China (5%), South Korea (9%), and Malaysia (9%).

Despite the lower percentage of users, its large population ensures sufficient cash flow. China has been a leader in mobile payments in APAC even before the pandemic, maintaining a steady flow of users. The country's most prominent payment channels include, Alipay and WeChat Pay, which were boosted even further by the pandemic. The increase in users is also reflected by an increase in malicious actors, looking for loopholes in the infrastructure. Concerns over any possible cracks have encouraged governments to control financial malware.

### Increase in attacks and government regulatory crackdowns during the pandemic

Security breaches minimize investor confidence. In the context of countries, data breaches can adversely affect the inflow of foreign direct investments, which can cause fluctuations in an economy. Apart from the financial aspects, security breaches in government bodies can affect public security, which is an all-time major concern of any government. Realizing these facts, governments have been focusing on security-testing frameworks. They are trying hard to make businesses and governmental organizations aware of possible threats in various forms and encourage them to integrate efficient cyber security and risk management practices.

Cyber-attacks amid the Covid-19 pandemic increased by almost 300% in 2020 in the country to reach 1,158,208 compared to 394,499 in 2019, according to the data from Computer Emergency Response Team (CERT-In). But cyber experts claimed the spike could be linked to an increase in online activity last year, particularly during the lockdown imposed to check the Covid-19 spread. However, they blamed a lack of cybersecurity awareness for phishing and malware attacks.

India also witnessed the highest number of domain name system or DNS attacks in 2020 with 12.13 attacks per organization,

**Scotts International. EU Vat number: PL 6772247784**

tel. 0048 603 394 346 e-mail: [support@scotts-international.com](mailto:support@scotts-international.com)

[www.scotts-international.com](http://www.scotts-international.com)

even though the cost of attacks in the country decreased by 6.08% to INR 5.97 crores, according to International Data Corporation's DNS Threat Report.

India's technology ecosystem is evolving at a massive rate; domestically grown startups are going global and global giants are investing in Indian markets at a fast pace. However, 2020 witnessed a series of data breaches on Indian startups. For instance, Juspay, a payment processing company, faced a breach that led to a leak of over 35 million records.

## APAC Security Testing market Competitor Analysis

The Asia Pacific security testing market is significantly competitive with the presence of several players in the market. These players are continuously adopting various strategies, such as mergers & acquisitions, product developments, partnerships, and collaborations, among others, to increase their market presence and acquire more customers.

May 2021 - Nexon Asia Pacific announced their accreditation with the official CREST-Approved organization, enabling them to independently assess and ensure proficiency and compliance in the practice and delivery of Penetration Testing.

### 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 Threat of New Entrants
  - 4.2.2 Bargaining Power of Buyers
  - 4.2.3 Bargaining Power of Suppliers
  - 4.2.4 Threat of Substitute Products
  - 4.2.5 Intensity of Competitive Rivalry
- 4.3 Value Chain / Supply Chain Analysis
- 4.4 Assessment of the Impact of COVID-19 on the Market

#### 5 MARKET DYNAMICS

- 5.1 Market Drivers
  - 5.1.1 Proliferation of Existing Malware that is Continually Attacking Devices
  - 5.1.2 Increasing Number of Connected Devices

**Scotts International. EU Vat number: PL 6772247784**

tel. 0048 603 394 346 e-mail: support@scotts-international.com

www.scotts-international.com

- 5.1.3 Transition to online payment methods
- 5.2 Market Restraints
  - 5.2.1 Hesitation to adopt ne digitization techniques
- 5.3 Technology Snapshot

## 6 Market Segmentation

- 6.1 Deployment Model
  - 6.1.1 On-premise
  - 6.1.2 Cloud
- 6.2 Type of Service
  - 6.2.1 Application Security Testing
    - 6.2.1.1 Introduction
      - 6.2.1.1.1 Mobile Application Security Testing
      - 6.2.1.1.2 Web Application Security Testing
      - 6.2.1.1.3 Cloud Application Security Testing
      - 6.2.1.1.4 Enterprise Application Security Testing
    - 6.2.1.2 Testing Method
      - 6.2.1.2.1 SAST
      - 6.2.1.2.2 DAST
      - 6.2.1.2.3 IAST
      - 6.2.1.2.4 RASP
    - 6.2.2 Network Security Testing
      - 6.2.2.1 Introduction
        - 6.2.2.1.1 Firewall Testing
        - 6.2.2.1.2 Intrusion Detection/Intrusion Prevention Testing
        - 6.2.2.1.3 VPN Testing
        - 6.2.2.1.4 URL Filtering
  - 6.3 Testing Tools
    - 6.3.1 Penetration Testing Tools
    - 6.3.2 Software Testing Tools
    - 6.3.3 Web Testing Tools
    - 6.3.4 Code Review Tools
    - 6.3.5 Others
  - 6.4 End-User Industry
    - 6.4.1 Government
    - 6.4.2 Healthcare
    - 6.4.3 BFSI
    - 6.4.4 Manufacturing
    - 6.4.5 Retail
    - 6.4.6 IT and Telecommunications
    - 6.4.7 Others
  - 6.5 Country
    - 6.5.1 China
    - 6.5.2 India
    - 6.5.3 Japan
    - 6.5.4 Others

**Scotts International. EU Vat number: PL 6772247784**

tel. 0048 603 394 346 e-mail: [support@scotts-international.com](mailto:support@scotts-international.com)

[www.scotts-international.com](http://www.scotts-international.com)

## 7 Vendor Market Share

## 8 COMPETITIVE LANDSCAPE

### 8.1 Company Profiles

#### 8.1.1 HP

#### 8.1.2 IBM

#### 8.1.3 Veracode

#### 8.1.4 McAfee

#### 8.1.5 Cisco Systems Inc

#### 8.1.6 Core Security Technologies

#### 8.1.7 Cigital Inc

#### 8.1.8 Offensive Security

#### 8.1.9 Applause App Quality Inc

#### 8.1.10 Accenture PLC

#### 8.1.11 ControlCase LLC

#### 8.1.12 Paladion Networks

#### 8.1.13 Maveric Systems

#### 8.1.14 Netcraft

#### 8.1.15 Synerzip

## 9 INVESTMENT ANALYSIS

## 10 MARKET OPPORTUNITIES AND FUTURE TRENDS

**Scotts International. EU Vat number: PL 6772247784**

tel. 0048 603 394 346 e-mail: [support@scotts-international.com](mailto:support@scotts-international.com)

[www.scotts-international.com](http://www.scotts-international.com)

**Asia Pacific Security Testing Market - Growth, Trends, Covid-19 Impact, and Forecasts (2023 - 2028)**

Market Report | 2023-01-23 | 120 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*	<input type="text"/>	Phone*	<input type="text"/>
First Name*	<input type="text"/>	Last Name*	<input type="text"/>
Job title*	<input type="text"/>		
Company Name*	<input type="text"/>	EU Vat / Tax ID / NIP number*	<input type="text"/>
Address*	<input type="text"/>	City*	<input type="text"/>
Zip Code*	<input type="text"/>	Country*	<input type="text"/>
		Date	<input type="text" value="2026-02-27"/>
		Signature	

**Scotts International. EU Vat number: PL 6772247784**

tel. 0048 603 394 346 e-mail: support@scotts-international.com

www.scotts-international.com



**Scotts International. EU Vat number: PL 6772247784**

tel. 0048 603 394 346 e-mail: [support@scotts-international.com](mailto:support@scotts-international.com)

[www.scotts-international.com](http://www.scotts-international.com)