



Developing a Resilient Web Defense

Why it is critical for organizations in Southeast Asia to adopt a holistic security strategy to protect against web application attacks

Table of Contents

- 03 Business Implications of Data Breaches and Web Defacement**
 - 03 — Impact of Data Breaches and Web Defacement
 - 04 — Importance of Web Application Security in Reducing the Risk of Data Breaches
- 05 Web Application Attack Trends in Southeast Asia**
 - 05 — Understanding the Top Five Web Application Attack Types
 - 07 — Notable Data Breaches and Web Defacement Attacks in Southeast Asia
- 08 WAF Adoption Situation Analysis in Southeast Asia**
 - 08 — Customer Buying Behavior Analysis: A Compliance-driven Approach
 - 09 — Snapshot of the WAF Landscape in Singapore, Malaysia, Thailand, Indonesia, the Philippines, and Vietnam
 - 10 — Singapore
 - 10 — Malaysia
 - 11 — Thailand
 - 11 — Indonesia
 - 11 — Philippines
 - 11 — Vietnam
 - 12 — From Reactive Prevention to Proactive Detection
- 13 Key Considerations for WAF Selection**
 - 13 — Consideration 1: Form Factor
 - 14 — Consideration 2: Level of Security Protection
 - 15 — Consideration 3: Operation Effectiveness and Total Cost of Ownership (TCO)
 - 15 — Other Considerations: Adoption, Security Ecosystem, and Local Support
- 16 The Last Word**
 - 16 — Moving Beyond Compliance to Business Enabler: Web Application Security as a Strategic Imperative for the Digital Economy
 - 17 — Envisioning the Future: Web Application Security for the Internet of Things
- 18 About Penta Security Systems**
 - 18 — Company Overview
 - 19 — Global WAF Market Performance
 - 20 — Global WAF Appliance Market Performance
 - 21 — WAF Solutions Market Performance in Asia-Pacific
- 22 About Frost & Sullivan**
- 23 Appendix**

Business Implications of Data Breaches and Web Defacement

Impact of Data Breaches and Web Defacement

Major consequences such as damage to company reputation, interruption to business operations, and legal exposure can negatively impact an organization's bottom line, placing cyber security at the top of the company agenda.

Across the globe, including the Asia-Pacific, the frequency and volume of cyber security incidents such as data breaches and web defacement continue to rise to unprecedented levels. Almost all industries are potential targets including retail, financial services, IT, public sector, critical infrastructure, manufacturing, and other services. Major consequences such as damage to company reputation, interruption to business operations, and legal exposure can negatively impact an organization's bottom line, placing cyber security at the top of the company agenda.

Security breaches can also lead to declines in share value and market position, as well as increase the risk exposure of other participants along the company value chain such as its suppliers, partners, and customers. In addition, the need for organizations to adopt targeted cyber security strategies and tools is now more important than ever with increased regulatory oversight requiring mandatory data breach incident reporting, not to mention the likelihood of heavy fines.

The section below examines several critical consequences of data breach and web defacement activities.

1. Loss of brand and reputation
Data breach or web defacement activities can impact the brand name and reputation of a company. The incidents also place the IT function under scrutiny and can adversely affect customer trust, creating negative media coverage for the firm. Partners doing business with the firm could also suffer from loss of business, further impacting the firm's ability to attract talent, suppliers, and investors.

Thus, it is essential for companies to maintain their security posture by investing in technologies, processes, and people. By having the right security posture, a company can safeguard its reputation by quickly responding to any data breach.

2. Financial losses and drop in share value
A company succumbing to web defacement or a data breach is bound to face financial losses, bringing down its shareholder value and profitability, and hampering future business opportunities. Apart from negatively impacting existing partners and suppliers, other functions such as sales, marketing, and IT are likely to suffer as well.

3. Penalties and fines

Globally, many countries are putting in place strict regulations to minimize the risk of data breaches. New legislation in a growing number of countries requires organizations compromised by a data breach to report the incident and potentially be subject to hefty fines and penalties, escalating financial costs further. Investigations show that a company's failure to comply with stipulated regulatory procedures could lead to severe penalties and even force the resignation of the company CEO.

One notable example is the European Union's General Data Protection Regulation (GDPR) which can impose a fine of EUR20 million on companies for non-compliance. Organizations based in Southeast Asian countries collecting EU citizen data are also subject to this penalty if a data breach occurs.

4. Loss of intellectual property

Theft of intellectual property, be it trade secrets, R&D efforts or patents, from a data breach incident can weaken a firm's competitive advantage and position in the market. For example, leakage of a company's price list in highly competitive industries could be detrimental to its profitability, causing it to potentially lose out to competitors.

5. Other intangible costs

Apart from tangible costs, a data breach can also have serious intangible effects. A hacker can steal sensitive company information, install malware, carry out privilege escalation, and such acts, which will negatively impact business operations in the long run. Small firms, in particular are at higher risk as they may not have protection in the form of insurance or appropriate strategies in place.

Importance of Web Application Security in Reducing the Risk of Data Breaches

Organizations failing to secure their web applications face multitude data risks and threats including information theft (e.g., passwords, customer information), damage to client relationships, revoked licenses, and potential legal repercussions. Web application security becomes even more crucial given that stakeholders provide personal data for decision-making at various levels of the business.

Cyber attackers can easily detect if the network layer is not secure and if the applications have valuable data. To respond to this growing threat, companies in fields such as financial services and healthcare need to comply with an increasing number of regulations, like the Payment Card Industry Data Security Standard (PCI-DSS) and Health Insurance Portability and Accountability Act (HIPAA), or face high fines.

There are a wide variety of web threats hostile parties use to attack systems and attempt to cripple critical infrastructure.

Threats include stealing customer data, like names, dates of birth, telephone numbers, and email addresses, adding the website to a botnet of infected sites, and even hijacking or crashing the site. When a web defacement occurs, it creates unauthorized changes to the web appearance by replacing the company logo, content or web pages.

Given the increasing popularity of web applications, security should be a key priority in developing secure applications. Web application security should be tested at every stage of the software development lifecycle and integrated as a part of their overall security strategy. Companies need to have response teams in place and a designated Chief Information Security Officer (CISO) who can prepare a crisis management plan and manage the application security needs of the business.

Web Application Attack Trends In Southeast Asia

Understanding the Top Five Web Application Attack Types

This section explores web application attack trends in major Southeast Asian countries.

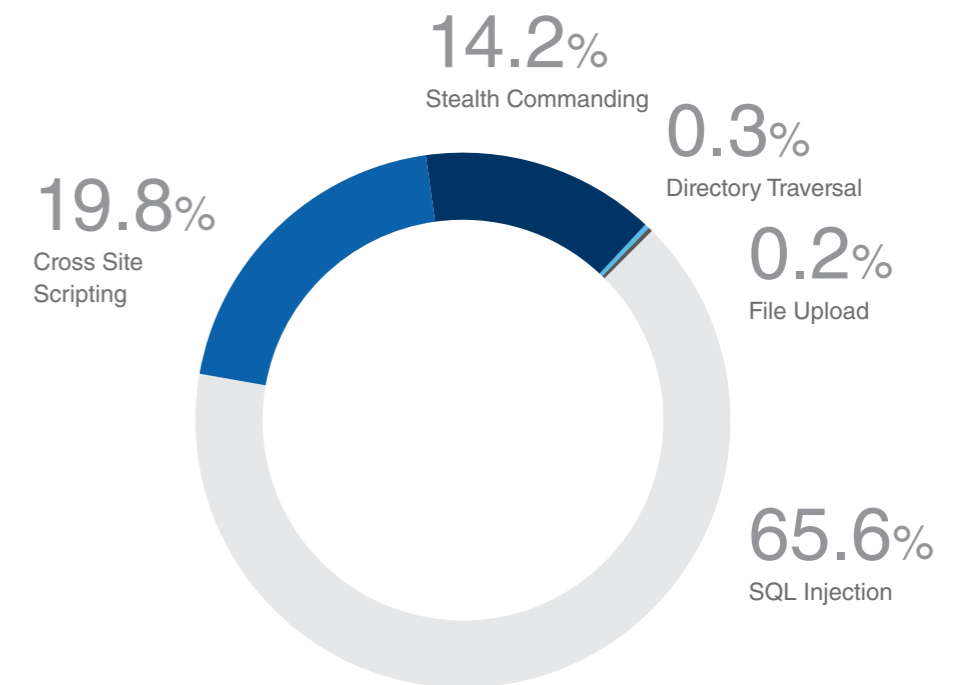
Web application firewalls (WAFs) were used to detect the five most common types of web application attacks.

Data in this section is sourced from the Southeast Asia Web Application Threat Trend (WATT) Report by Penta Security Systems.

The overall study examines attack data in relation to the top five web application attack techniques, based on the analysis of logs collected from January 1 to December 31, 2016. The most prevalent types of attacks in the region are SQL Injection, Cross Site Scripting, Stealth Commanding, Directory Traversal, and File Upload. Definitions of each attack type can be found in the Appendix.

1. Overview of the top web application attacks in Southeast Asia

Detections by Web Attack Rule, Southeast Asia, 2016



Source: Southeast Asia Web Application Threat Trend (WATT) Report, Penta Security Systems

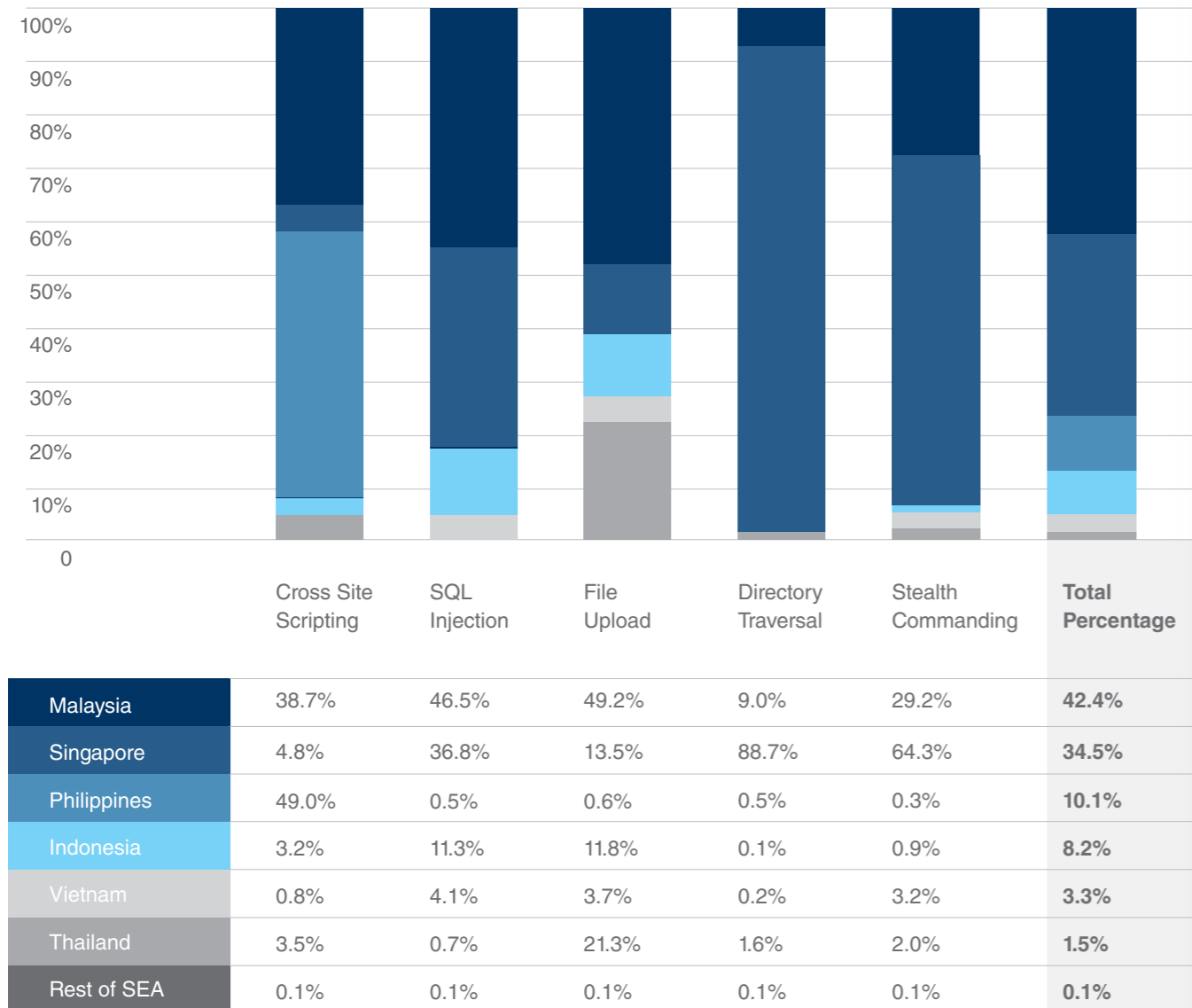
Based on the report findings, SQL Injection attacks had the highest occurrence in Southeast Asia, followed by Cross Site Scripting, Stealth Commanding, Directory Traversal, and File Upload.

SQL Injection is one of the most common types of web application attacks. Most successful SQL Injection attacks can cause substantial information leakage (data breach). The threat can then escalate to exploits using the leaked information, such as performing fraudulent transactions using stolen login credentials. Automated tools for SQL Injection attacks can easily be found online.

Stealth commanding attacks are intended to execute unauthorized code. By attaching a malicious server-side script to the input, an attacker can execute the desired command and obtain information. This attack is severe as the whole web server can be under the hacker's control. The attack can be prevented with the establishment of an input value verification procedure or HTTP request verification function in WAF.

2. Prevalence of web application attacks in Southeast Asian countries

Detection of Web Attacks by Country, Southeast Asia, 2016



Source: Southeast Asia Web Application Threat Trend (WATT) Report, Penta Security Systems

The exhibit above illustrates the different types of web attacks infiltrating major Southeast Asian countries. Malaysia and Singapore are hotspots for suspicious web activities, accounting for nearly 42.4% and 34.5% respectively of all attacks in Southeast Asia in 2016.

- File Upload and SQL Injection attacks most frequently detected in Malaysia at 49.2% and 46.5% respectively.
- Directory Traversal attacks, which mainly use automated tools, and Stealth Commanding attacks detected in Singapore at 88.7% and 64.3%, respectively.

- The Philippines had the highest percentage of Cross Site Scripting attacks (49.0%) in Southeast Asia, recording an overall 10.1% and ranking 3rd highest in the region.
- Indonesia, Vietnam, and Thailand accounted for 8.2%, 3.3%, and 1.5% of web application attacks respectively.
- The rest of Southeast Asia, covering Cambodia, Brunei, Laos, and Myanmar, accounted for 0.1% of the total.

Notable Data Breaches and Web Defacement Attacks in Southeast Asia

A report published by the Cyber Security Agency of Singapore stated that there were nearly 1,800 reports of website defacement cases in 2016 alone, which continues to be a prevalent threat to the online presence of businesses in Singapore.

In August 2016, a 22-year-old became the first person in Singapore to be convicted for committing a financial crime using hacking techniques. The hacker managed to infiltrate several websites, stealing customers' log-in details to access their email, PayPal, and Groupon accounts and perform fraudulent purchases worth more than SGD70,000. The sentence was a jail term of 28 months, in violation of 20 offenses under the Computer Misuse and Cybersecurity Act. The criminal reportedly used hacking software to execute SQL attacks on web applications, stealing databases of information containing usernames and passwords.¹

Injection techniques were also used to create defacements as a form of hacktivism to share resentment against certain government agencies or businesses. A report published by the Cyber Security Agency of Singapore stated that there were nearly 1,800 reports of website defacement cases in 2016 alone, which continues to be a prevalent threat to the online presence of businesses in Singapore.²

Malaysian telecommunication service providers and mobile virtual network operators encountered a major breach that led to 46.2 million mobile subscribers' personal data being compromised and leaked on an online forum. The breach exposed subscribers' home addresses, identity card numbers, and SIM card information.

In addition, three databases belonging to medical practitioners comprising 81,309 personal data records were also leaked.³ The breach was discovered in early October 2017; however, sources reported that the incident is likely to be related to a data breach that occurred as early as 2014.⁴

Other than database leaks, the vulnerability of web assets were exploited when hackers took over 27 Malaysian websites in a web defacement attack during the 2017 SEA Games. The case was seen as backlash from Indonesian-based hacktivists in response to a blunder in which their national flag had been printed upside down in the event's official souvenir booklet.⁵

In July 2017, a hacking group known as 1937CN attacked two of Vietnam's largest airports as well as its local carrier Vietnam Airlines. The hack attempt hijacked flight information screens and sound systems in the Hanoi and Ho Chi Minh City airports, and also involved the dumping of about 400,000 Vietnam Airlines passengers' information online.⁶

The cyber attack on the Commission On Elections (COMELEC) in the Philippines has been one of the country's largest breaches. In April 2016, hackers infiltrated COMELEC's database, defaced its website, and exposed 55 million voters' personal information and the names of the parties they were supporting.⁷

¹Ronald Loh, "Hacker spent \$70k using victims' e-mails, Paypal and Groupon accounts", The New Paper, August 18, 2015, <http://www.np.sg/>.

²Irene Tham, "1,800 website defacements in Singapore in 2016 just tip of the iceberg: CSA", The Straits Times, September 15, 2017, <http://www.straitstimes.com/>.

³Vijandren, "46.2 million Malaysian mobile phone numbers leaked from 2014 data breach", Lowyat.net, October 30, 2017, <https://www.lowyat.net>.

⁴Telco data leak involves data from 2014, says deputy minister", The Malaysian Insight, December 12, 2017, <https://www.themalaysianinsight.com>.

⁵Lee Kah Leng, "Indonesian hacker group defaces Malaysian websites following flag blunder", The Star Online, August 21, 2017, <https://www.thestar.com.my>.

⁶Pierluigi Paganini, "China 1937CN Team hackers attack airports in Vietnam", Security Affairs, July 31 2016, <http://securityaffairs.co/>.

⁷Waqas, "Anonymous hacks Philippines Election Commission, leaks 55 million voter data", HackRead, April 9 2016, <https://www.hackread.com>.

WAF Adoption Situation Analysis in Southeast Asia

Customer Buying Behavior Analysis: A Compliance-driven Approach

With rising Internet penetration, the opportunities for Southeast Asian enterprises to connect, engage, and sell to customers are tremendous. The need to interact with customers to enhance business operations via the web interface in a safe manner is leading many businesses to pay considerable attention to the security of their web systems.

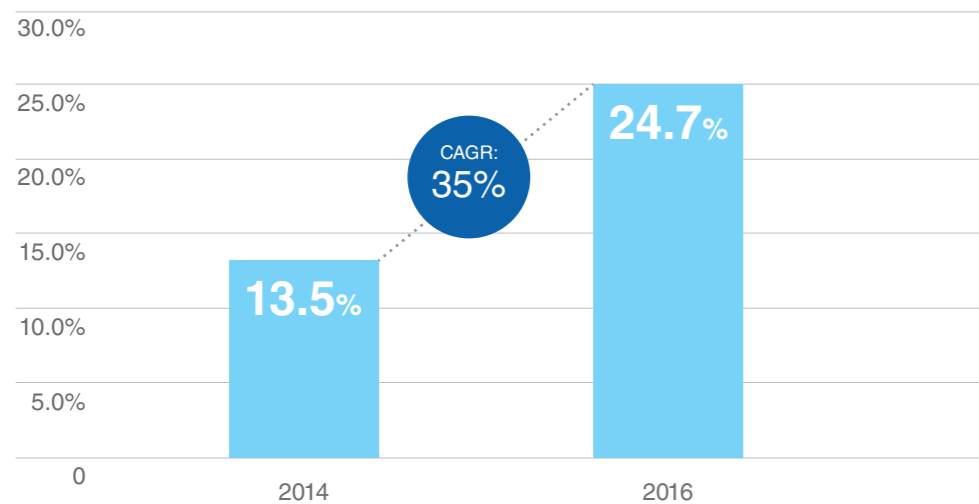
The growing reliance on web applications as an essential business tool is making it a prime target for cybercriminals. Hackers are increasingly exploiting web application vulnerabilities, targeting web servers, databases, and related web infrastructure to gain unauthorized access to privileged information.

Conventional security technologies such as firewalls are no longer adequate to prevent these threats, requiring enterprises to adopt more advanced security technologies that can provide protection capabilities at all network, application, and database levels.

To address this issue, a growing number of enterprises in the region are adopting WAF solutions, representing a robust CAGR of 35.0% from 2013–2016.

The market saw tremendous uptake in 2016, growing by 44.0% year-on-year (YoY). The WAF market has almost doubled in two years, reflecting the importance of WAF solutions for regional businesses in Southeast Asia.

WAF Solutions Market: Revenue Forecast, Southeast Asia, 2014–2016



Source: Frost & Sullivan

While the adoption of WAF solutions continues to grow in Southeast Asia, it is largely reactive as many enterprises still adopt a compliance-driven and prevention-centric approach. For example, enterprises responding to regulatory requirements such as PCI-DSS and local data protection acts.

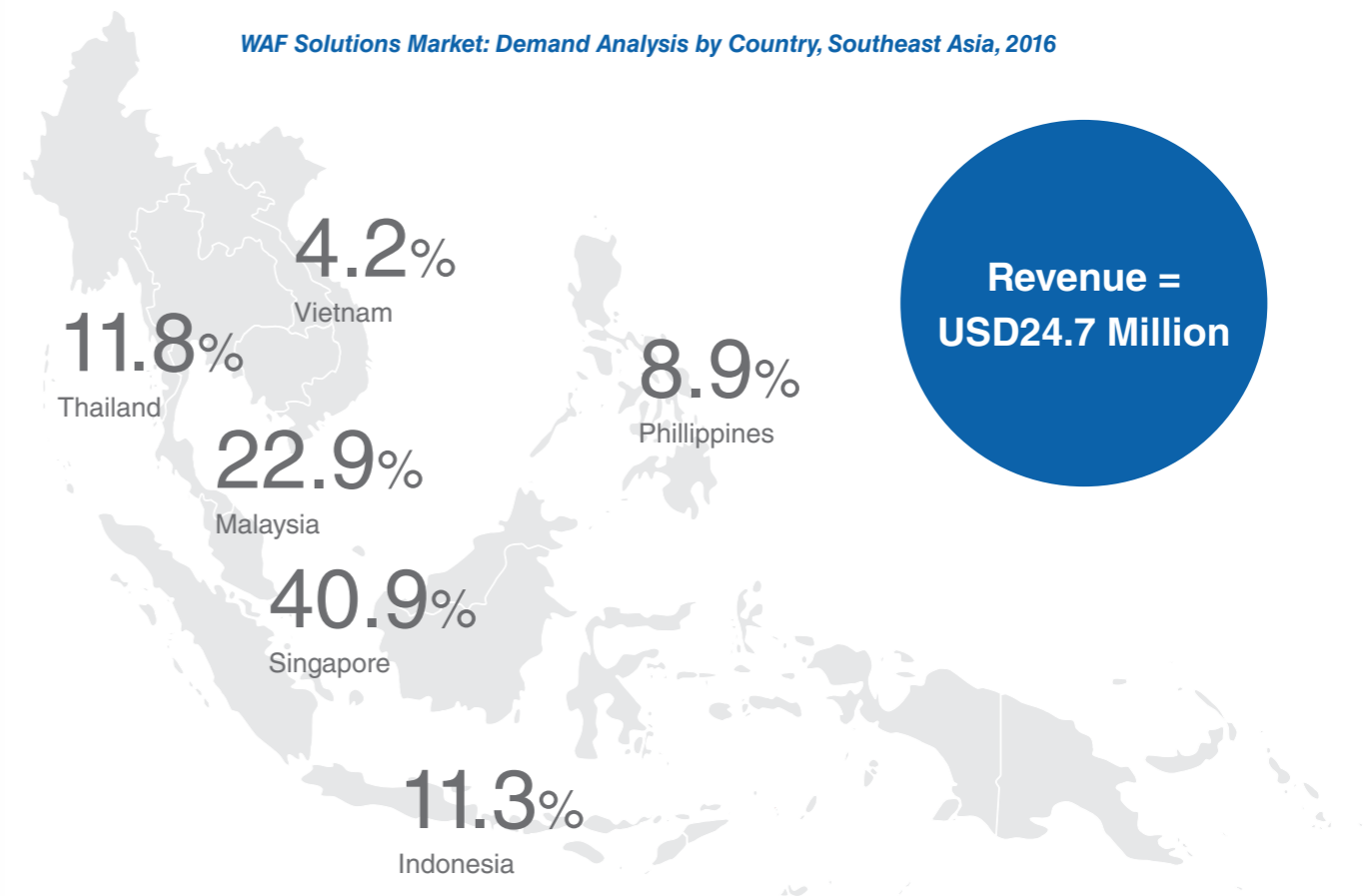
Given the regulatory pressure, businesses in the region take a compliance-driven approach to meeting their security requirements, particularly the banking, financial services and insurance (BFSI), e-commerce, and retail sectors. For Southeast Asian countries, the motivation to comply with regulations is often for audit purposes and to avoid fines and penalties.

Investment in WAF solutions to protect reputation, intellectual property, and infrastructure is currently a lower priority among enterprises in the region, likely due to the shortage of skilled resources and expertise related to applications and security.

Many enterprises deploy WAF for auditing purposes, setting it in monitoring or detection mode since receiving too many false positive alerts generated from the WAF could result in higher overheads and operational costs for enterprises. This leads them to turn off the prevention mode that can block actual web attacks. The focus is more on availability, service performance, and creating a hassle-free experience for customers. Southeast Asian enterprises do not appear to prioritize corporate risk management strategies, but mainly follow compliance requirements.

Snapshot of the WAF Landscape in Singapore, Malaysia, Thailand, Indonesia, the Philippines, and Vietnam

WAF Solutions Market: Demand Analysis by Country, Southeast Asia, 2016



Source: Frost & Sullivan Asia-Pacific Web Application Firewall Solutions Market, Forecast to 2021

Major Adopters in Southeast Asia

Singapore

In 2016, Singapore had the largest WAF market in Southeast Asia, recording 67.9% YoY growth, the most robust among all Southeast Asian countries. The government, BFSI, service providers, and e-commerce are the strongest industry verticals for WAF adoption, representing a combined market share of 73.5% of the overall market. There has been significant adoption in other verticals as well, including healthcare, media, and information technology/information technology-enabled services (IT/ITES).

Despite more businesses in Singapore shifting to cloud services, on-premises solutions remain prominent, contributing a higher share of revenue to the overall market at 52.3% in 2016. However, adoption of virtualization, cloud, and IoT technologies are anticipated to expand as businesses in Singapore embrace new technologies to transform their operations.

Under the Singapore Cybersecurity Bill, Cybersecurity Act 2018, organizations that are classified by the Commissioner as a Critical Information Infrastructure (CII) must furnish information on the design, configuration, and security of the CII. The Commissioner may issue a written directive for action to be taken in relation to a cyber security threat, enforce compliance with a code of practice or standard, or conduct an audit on the owner(s) on their compliance with the act.

If there is willful non-compliance by the owner, he/she will be found guilty of an offense and be liable on conviction to a fine not exceeding SGD100,000 or imprisonment for a term not exceeding two years.⁸ The bill is expected to stimulate an increase in WAF adoption, especially for identified CII companies in government, BFSI, aviation, healthcare, land transport, maritime, media, security and emergency, water, energy and info-communication sectors.

Malaysia

In 2016, Malaysia accounted for 22.9% of the WAF market, making it the second largest in Southeast Asia. Investment in WAF solutions increased significantly by 24.9% in 2016. Similar to the deployment trend in Singapore, the majority of enterprises in Malaysia opt for on-premises solutions, primarily driven by compliance needs. BFSI, government, service providers, and e-commerce verticals were the top spenders of WAF solutions in the country with a market share of 29.8%, 24.2%, 13.3%, and 11.9%, respectively.

Moving forward, with more stringent requirements for compliance and the e-commerce boom under the Digital Economy strategy, investment in WAF solutions is projected to accelerate in the forecast period.

Organizations in Malaysia must ensure the privacy and security of consumers' personal data and comply with the Personal Data Protection Standards as governed by the Personal Data Protection Act of 2010. Willful non-compliance could subject the offender to a fine of up to RM100,000 or imprisonment not exceeding two years or both.⁹

The capital market industry needs to comply with the Guidelines on Management of Cyber Risk by the Securities Commission (SC) of Malaysia, while the BFSI sector must adhere to the Guidelines of Management of IT Environment (GPIS 1) issued by Bank Negara Malaysia.¹⁰ These guidelines serve as primary drivers for organizations in Malaysia to adopt WAF as a primary tool to protect consumers' personal data while maintaining the availability of online services.

Rest of Emerging Southeast Asia

Thailand

The WAF market in Thailand recorded a moderate growth rate of 16.9% YoY with a revenue of USD2.9 million in 2016. Among verticals, BFSI, service providers, and e-commerce were the top spenders, accounting for 30.7%, 19.5%, and 16.3%, respectively. The government sector recorded a steady growth of 37.8% following the launch of its Digital Economy Policy and plan to strengthen Internet security, boosting the adoption of application security among public sector agencies.

Demand is set to increase when the sector-specific laws and regulatory notifications take effect governing the security of personal data. The sectors affected would include government agencies, telecommunications, BFSI, healthcare, consumer credit and electronic payment services. Organizations must apply for an electronic payment license to explain how it can protect users' information before the license can be granted, as regulated by the Royal Decree on Electronics Payments.¹¹

Indonesia

In 2016, Indonesia was the second-fastest growing WAF market in Southeast Asia, expanding by 65.8% to attain a total revenue of USD2.8 million. The government, BFSI, IT/ITES as well as online gaming, and entertainment sectors were the top spenders of WAF solutions, contributing 22.9%, 21.7%, and 20.8%, respectively.

Demand for WAF is expected to surge given its role as a gatekeeper in protecting consumers' personal data in light of the Ministry of Communication and Informatics' introduction of the Protection of Personal Data in Electronic Systems (MOCI Regulation) on December 1, 2016.

The regulation requires organizations to adopt agreements ensuring minimum service levels, information security of IT services, and implementation of internal communication security. Failure in compliance could result in temporary dismissal of activities for an organization.¹²

Philippines

The WAF market in the Philippines recorded slower growth in 2016 in comparison to the top markets in the region, contributing to only 8.9% of the overall regional market share. That stated, market growth has been at a rapid pace in recent years. The overall market reported high double-digit revenue growth of 49.9% YoY, anticipating to prevail as the country builds up its security posture.

The National Privacy Commission implemented the Data Privacy Act of 2012, Section 28, "Guidelines for Technical Security Measures," stating the need to implement safeguards to protect the computer network from unauthorized access, as well as the need to perform regular monitoring breaches.¹³ These guidelines are likely to encourage organizations to review their data protection strategy, primarily, web application online services.

Vietnam

Unlike other Southeast Asian countries, the Vietnamese WAF market remained relatively nascent; attaining a revenue of US\$1.0 million in 2016, accounted for 4.2% of the regional market. WAF adoption in Vietnam is limited and mainly compliance-driven due to the low attention on application security.

However, this is expected to change with increasing consumer awareness and legislation strengthening personal data protection information security. BFSI and government sectors are the main adopters of these solutions due to their need for compliance and protection of customer data. The Ministry of Information and Communications released the Law on Network Information Security (Law no: 86/2015/QH13) effective July 1, 2016.¹⁴

The section on the protection of personal information security in the network stresses the need for organizations to adopt appropriate managerial and technical measures to protect personal data, and also requires them to take remedial and blocking measures as soon as there are identified incidents or risks.¹⁵ Failure to do so may result in penalties imposed on the organization or individual.

⁸Cyber Security Agency of Singapore, "Cybersecurity Bill, Bill No. 2/2018", Jan 8, 2018. <https://www.csa.gov.sg/>.

⁹Jabatan Perlindungan Data Peribadi, "Laws of Malaysia, Act 709, Personal Data Protection Act 2010), June 10, 2010. <http://www.pdp.gov.my/>.

¹⁰Securities Commission Malaysia, "Guidelines on management of cyber risk", Oct 31, 2016. <https://www.sc.com.my/>.

¹¹Tilleke & Gibbins, "Data Security and Cybercrime in Thailand" Feb 8, 2017. <https://www.lexology.com/>.

¹²DLA Piper, "Data Protection Laws of the World: Indonesia", Jan 24, 2018. <https://www.dlapiperdataprotection.com/>.

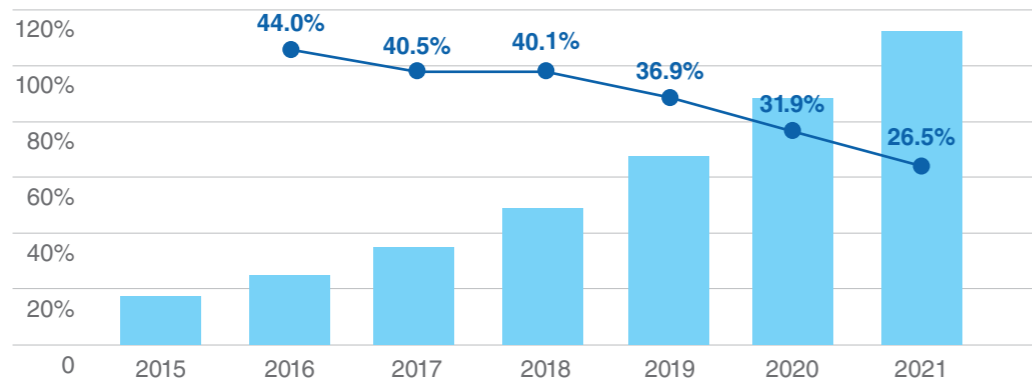
¹³National Privacy Commission, "Implementing Rules and Regulations of the Data Privacy Act of 2012" August 24, 2016. <https://privacy.gov.ph/>.

¹⁴Ministry of Information and Communications, "Legal Documents: Law No. 86/2015/QH13", accessed Feb 1, 2018. <http://english.mic.gov.vn/>.

¹⁵National Assembly, Socialist Republic of Vietnam "Law on Network Information Security", Nov 19, 2015. <http://english.mic.gov.vn/>.

From Reactive Prevention to Proactive Detection

Forecast for WAF Market, Southeast Asia, 2015–2021



Revenue (USD Mn)	17.1	24.7	34.7	48.6	66.5	87.8	111.0
------------------	------	------	------	------	------	------	-------

Source: Frost & Sullivan Asia-Pacific Web Application Firewall Solutions Market, Forecast to 2021

The overall WAF solutions market in Southeast Asia is projected to record robust momentum in the next five years with greater awareness about cyber security and stricter regulatory policies.

With governments in the region increasing their focus on eGovernment, smart cities, and connected industries, the need for privacy and data protection is more important than ever. As the threat landscape evolves with increasing web application attacks, it is critical for all enterprises to have an advanced WAF solution to protect their web-based applications, either in the traditional web or cloud environment.

As a result, businesses in the region are looking beyond compliance and prevention to invest in advanced threat detection capabilities as they recognize the vulnerabilities of conventional security tools in keeping the attacks away from their corporate networks.

It is vital for organizations to be equipped with capabilities to detect and respond to these advanced threats, which requires them to look beyond the traditional WAF features.

Traditional WAF solutions are only capable of preventing and blocking known threats, based on the preset rules and signature-based detection techniques (whitelisting and blacklisting), which are unable to detect advanced and unknown threats, such as low and slow DDoS attacks, and zero-day attacks.

These require advanced detection features using signature-less detection techniques that can detect, learn, and adapt to the changes of advanced threats, and which are particularly crucial for enterprises that have critical applications and data to protect.

Web Application Firewall (WAF) is a security technology, either hardware or software, placed in front of the web server to protect applications from attacks aimed at exploiting their vulnerabilities. WAFs monitor, filter or block data packets traveling to and from a web server by intercepting Hypertext Transfer Protocol (HTTP) requests, to identify and block potential malicious requests from reaching the web server.

WAFs can protect applications from different threats such as Open Web Application Security Project (OWASP) Top 10 risks, application layer distributed denial-of-service (DDoS), Cross Site Scripting (XSS), and Structured Query Language (SQL) Injection, among others, hence protecting the databases connected to these applications to prevent a data breach.

Key Considerations for WAF Selection

There are different types of WAF solutions in the market featuring diverse technologies and features. WAFs are also available in various forms that can be deployed in different modes to suit the unique goals, business needs, and priorities of an organization.

Enterprises should consider the following points in choosing a suitable WAF:

Consideration 1: Form Factor

A WAF can be in different form factors, which include physical hardware appliances, virtual appliances, or cloud-based services. Regardless of form factor, a WAF can be deployed either inline with an application server or as a reverse proxy that inspects both external HTTP/s request and web servers' responses, to detect and block malicious traffic. Choosing the right form factor can be a difficult task requiring the IT team to have a good understanding of the scope and priorities of their organizations.

Physical appliances:

Companies that have huge application stacks and critical data in their data centers can consider the physical appliance as it offers many advantages such as high performance, low latency, high privacy, and in-house ownership and management which can be crucial for forensics. On-premises WAFs are also known to be more flexible in deployment within the data center. Configuration is possible in proxy mode or inline mode, as well as other customizations that may be necessary when the WAF is deployed within an enterprise with unique web application processes.

Virtual appliances:

If a company migrates its application stacks to the cloud, the virtual appliance would be suitable due to its strong scalability and ease of configuration to adapt to changes made to the application stack in the cloud environment. The virtual WAF is the ideal option for businesses that want to deploy the WAF close to the applications. However, a virtual appliance alone may not be able to perform well when the whole infrastructure becomes more sophisticated, with changes in the applications and network functions.

A hybrid model blending hardware and virtual appliances would be a better solution to help an organization deal with these challenges. It would allow them to protect applications beyond the traditional premises without compromising performance.

Cloud-based WAF:

Cloud-based WAFs provide ease of deployment, high scalability, and flexibility of a subscription model, with minimum requirements for network infrastructure changes, and hassle-free management for security teams.



Consideration 2: Level of Security Protection

Protection against the most common threats:

Regardless of vendors and technologies, a WAF should have key features and capabilities, including protection against the Open Web Application Security Project's (OWASP) Top 10 most critical web application security risks. Popular attacks include SQL Injection, Cross Site Scripting, and DDoS, to name a few.

The WAF should have the capability to detect common application exploits and threats targeting known application vulnerabilities. Businesses of all sizes need to look at these basic features when considering a WAF as they offer maximum security protection against the most common threats that organizations encounter while making its management and handling efficient and easy to use.

Maximum threat protection with fast and accurate advanced threat detection capabilities:

Enterprise-grade WAFs with advanced features are suitable for large businesses that have a vast number of critical applications, business services, and sensitive data that need protection.

Other than the standard features, WAFs should also be able to perform advanced detection and protection capabilities against application layer DDoS, zero-day attacks, fraudulent transactions, cross-site request forgery (CSRF), and automated threats, and support other capabilities such as SSL visibility.

An intelligent WAF should have capabilities to perform full traffic package analysis leveraging different techniques such as using heuristics and semantics for detection as these techniques enable the WAF to recognize advanced threats without requiring signature updates while providing low false positives. This is important for organizations that need to maintain and protect applications beyond the traditional premises (servers or data centers), such as in the cloud or when embedded in IoT devices.

Detailed logging and threat intelligence can provide security teams with more visibility into the application traffic traveling across environments, from public cloud to private cloud and IoT devices. This information helps them identify potential attacks and data breaches faster and more accurately, reducing the management overhead of security teams.

Consideration 3: Operation Effectiveness and Total Cost of Ownership (TCO)

Regardless of form factor and how advanced the WAF is, the ultimate goal of an organization when selecting a WAF is the business impact it can bring. A good WAF solution should not only enable enterprises to comply with regulations, protect applications, and ensure data safety from cyber attacks, but it should also help businesses save time and operational costs in deployment, operation, and maintenance.

Simple and intuitive user interface:

For enterprises lacking sufficient internal resources and strong application security expertise, a WAF with simple-to-use, intuitive controls and reporting features in the dashboard or console can benefit the security team. These features provide detailed visibility on threat areas they should focus on, helping them save time on remediating vulnerabilities and reducing operational costs.

Ease of deployment, configuration, and maintenance:

The rapid changes and high service demands do not allow enterprises to take a long time in deploying a WAF. Difficulties in configuration and maintaining a WAF could also introduce security misconfiguration risks for organizations.

In this regard, organizations should consider an easy-to-deploy-and-maintain WAF solution with strong support from the vendor.

Reducing the total cost of ownership (TCO):

For large businesses with complex application infrastructure, a high-end WAF can provide the performance power and features required for management. Small and medium businesses (SMBs) or a business with less critical applications, data, and services may not need to invest in high-end WAFs with advanced features.

Enterprises should consider a vendor that provides a line-up offering multiple price points, to find the most suitable WAF that matches their requirements. Complicated configurations, lengthy deployment times, or lackluster vendor support could affect opportunity costs and create additional operation overhead. The WAF selection factors ensure reduced TCO for the organization in the overall context of risk management and business impact.

Other Considerations: Adoption, Security Ecosystem, and Local Support

Enterprises should take into account other factors, such as the vendor's adoption rate in the regions of operation, its security ecosystem, and ability to deliver reliable support locally.

A vendor that provides a security portfolio which extends beyond web application security, such as database security, can offer a more comprehensive and integrated approach to security.

The ecosystem factor is also essential as applications are developed and used in different contexts and environments, requiring a more comprehensive approach to protection in addition to the WAF solution.

The ability to deliver strong local support is crucial, which can be done via a direct team or through local partners. As WAF configuration requires substantial knowledge and expertise in application security, businesses need local support to understand the rapid changes in web applications, IT environments, and the widening threat landscape.

The Last Word

Moving Beyond Compliance to Business Enabler: Web Application Security as a Strategic Imperative for the Digital Economy

Moving forward, most countries and businesses will need to comply with stricter digital regulations as more business operations are conducted on digital platforms requiring robust security measures.

While complying with stricter regulations is a significant push factor by the authorities, businesses may only do the minimum to meet the standards. It is vital for business leaders to understand the dire implications of inadequate web application security (as discussed in Section 1), and how investments in creating a defense-in-depth approach is a business enabler rather than a cost center. Superior web application security could potentially become a differentiator in the digital economy, allowing businesses to gain a competitive advantage with a stronger cyber posture, building trust with consumers in protecting their confidential data from cyber attacks.

As businesses, especially those in e-commerce evolve further, they need to protect against financial fraud, identity theft, disruption of services, and exposure of sensitive customer data. Vulnerable areas include weak input sanitization, broken authentication and session management, and insufficient monitoring and logging, among others. Governments are increasingly adopting digital practices and require solid web application security posture to protect against fraudulent use of digital payment systems, data theft, misuse of data and hacking of digital wallets.

Organizations therefore need to know where and how to protect their digital assets online. One recommendation is to seek advice from qualified security consultants to help decide the best form factor and level of security protection required, followed by an evaluation of security efficacy and total cost of ownership before making an informed decision about the right WAF solution and related security tools.

Envisioning the Future: Web Application Security for the Internet of Things

The growing adoption of IoT is creating a wave of ubiquitous connectivity, leading to the availability of new possibilities such as connected cars, driverless trucks, smart homes, connected gadgets (televisions, thermostats, lights, door locks, and refrigerators), as well as sensors improving the efficiency of power generation, water, and transportation systems.

Despite the significant opportunities IoT brings, the technology also raises several security risks for businesses and consumers. With a vast number of connected devices, IoT is particularly vulnerable to security attacks both virtually and physically. For instance, with interconnected devices, data that gets collected can be hacked easily and misused.

Criminals can hack into Internet-controlled automobile devices such as horns, engine, brakes, and dashboard displays, potentially causing severe accidents. With so many interconnected devices generating personal and financial information, cybercriminals also have ample opportunity to disrupt operations.

The entry points for threats that are bound to escalate in the future include insecure web interfaces, applications with insufficient authentication or authorization functionality, and insecure network services, among others. Today, electronics manufacturers are looking to add features that can connect their products to the Internet, often compromising the compatibility of the software and hardware. Hackers detecting any vulnerabilities in these products can remotely attack the set of interconnected devices from anywhere in the world.

In light of these risks, it is necessary for manufacturers to properly test systems and adopt the needed level of security mechanisms to protect IoT-connected devices. Web application security, therefore, should be the primary consideration for IoT to succeed in this space.

About Penta Security Systems



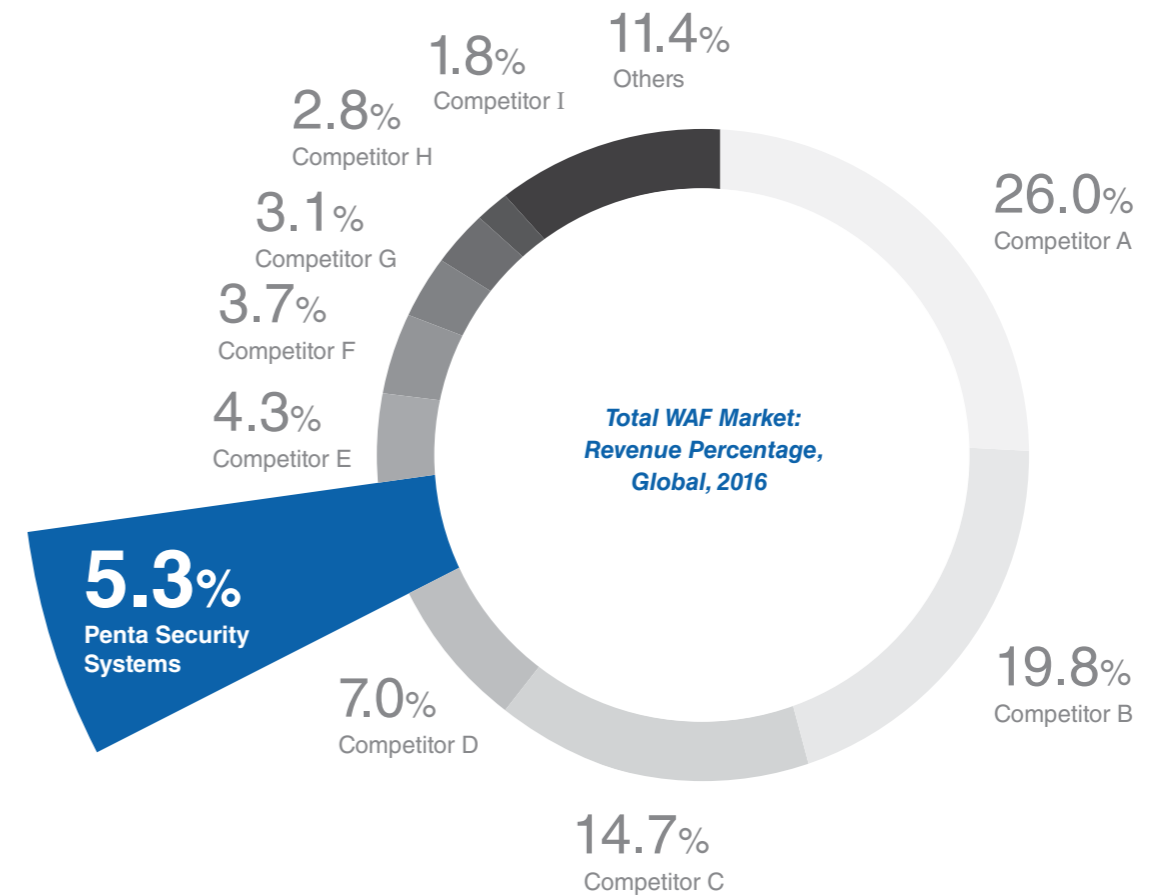
Company Overview

Penta Security Systems is a global provider of application security solutions based in Seoul, South Korea. The company offers a wide range of web, data, and authentication security solutions including WAF, data encryption solutions, and single sign-on (SSO).

Penta Security Systems offers multiple WAF options to help protect customers' applications across data centers, cloud infrastructure, and virtual environments. WAPPLES is a comprehensive WAF solution available as either a physical appliance or virtual appliance (WAPPLES-SA). WAPPLES uses a proprietary logic operation detection engine known as Contents Classification and Evaluation Processing (COCEP™) that uses semantic and heuristic analysis techniques to detect and block known and unknown threats. The solution uses a logic-based analysis engine to deliver low false positive rates and prevent data leakage.

Penta Security Systems offers IoT-specific safeguards such as AutoCrypt for complete protection of connected cars, using PKI for authentication of endpoints (AutoCrypt PKI) and encryption to secure communications (AutoCrypt V2X). AutoCrypt AFW is a specialized firewall for connected car systems that uses logic-based analysis instead of signatures to detect and block threats and unwanted activities.

Global WAF Market Performance



Source: Frost & Sullivan Global Web Application Firewall Market Analysis, Forecast to 2021

The global WAF market is populated by a few well-established participants and emerging players, according to Frost & Sullivan analysis. The top three vendors control the majority of the WAF market share, offering WAF appliances, WAF modules for ADCs, and cloud-based WAF services.

In the appliance market segment, Competitor A and Competitor C are the two leading vendors. In particular, Competitor A is one of the most highly-regarded vendors in the market based on its reliable product performance, continued product development, and years of experience in the WAF market.

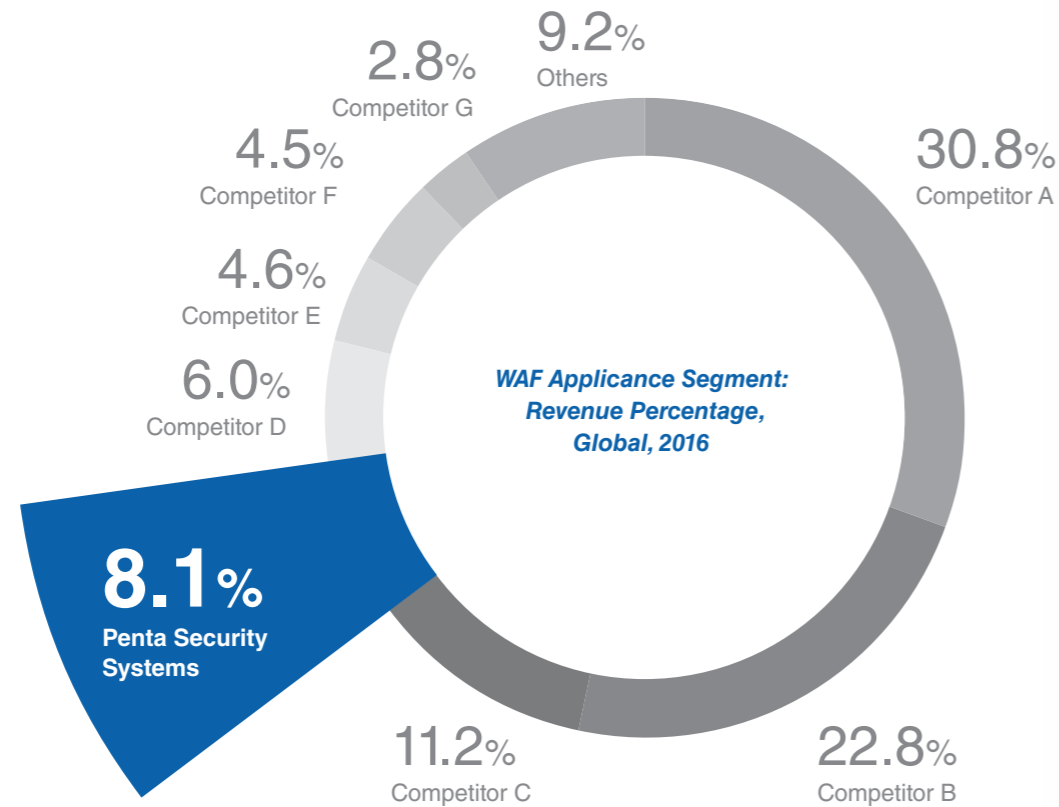
In the services market segment, Competitor B emerged as the leading vendor, followed by Competitor A. Competitor B's success is the result of a strong value proposition of integrated CDN optimization, WAF security,

and availability assurance (DDoS mitigation), plus advanced security capabilities such as API protection and bot management and security. Additionally, the services market segment is seeing an increase in competition as vendors that have traditionally offered on-premises solutions are now also introducing cloud services.

Penta Security Systems ranks among the top five in the global WAF solutions market, consolidating its market leadership in the Asia-Pacific. Penta Security Systems primarily focuses on the South Korea market, while also serving customers in Thailand, Malaysia, Singapore, and Japan, among others. The company also has a small presence in North America, with a sales office in Texas.

Penta Security Systems ranks among the top five in the global WAF solutions market, consolidating its market leadership in the Asia-Pacific.

Global WAF Appliance Market Performance



Source: Frost & Sullivan Global Web Application Firewall Market Analysis, Forecast to 2021

Governments are increasingly adopting digital practices and require solid web application security posture to protect against the fraudulent use of digital payment systems, data theft, misuse of data, and hacking of digital wallets.

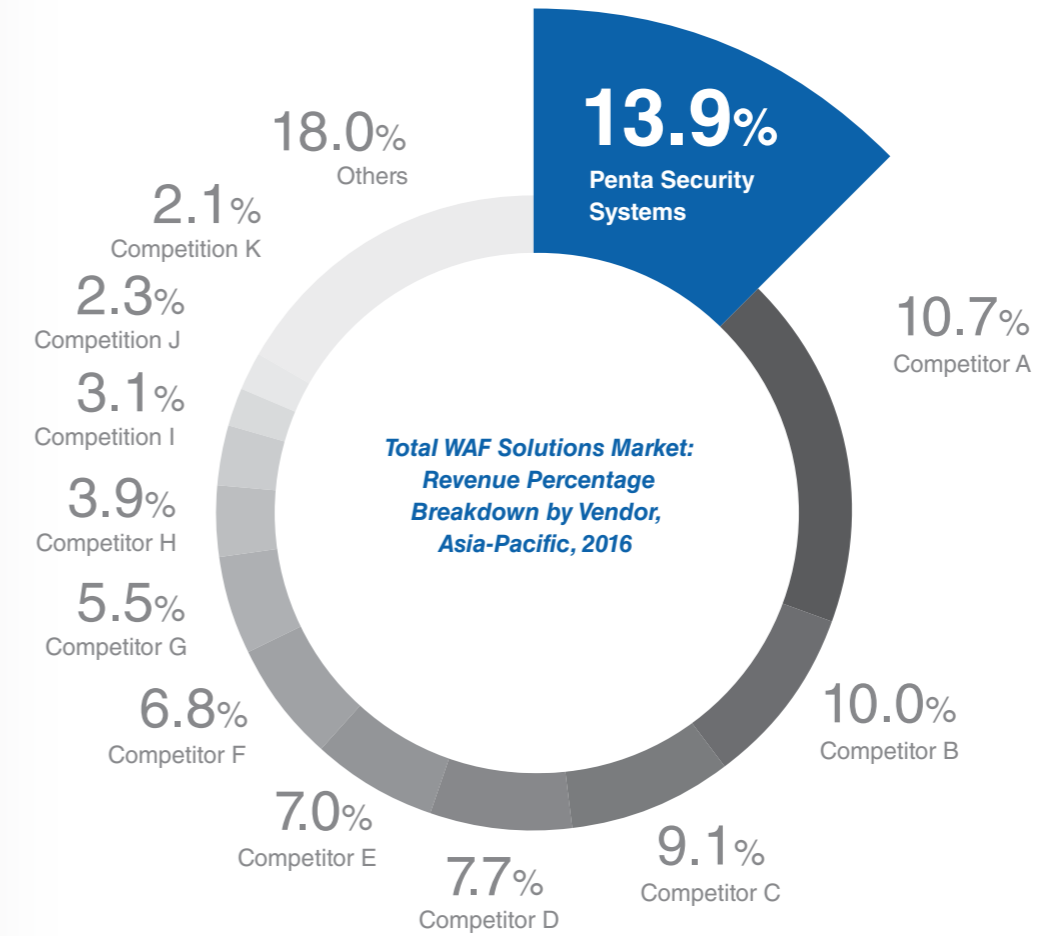
The WAF application segment includes virtual and physical appliances. WAF vendors offer a range of appliances from 50 Mbps to high-end appliances capable of more than 40 Gbps throughput.

Large enterprises dominate the WAF application segment due to the high investment cost requiring substantial IT budget and willingness to pay for best-of breed security technologies. As a result, the average price of WAF products is anticipated to remain steady. The top eight vendors in the WAF application segment are mostly global WAF vendors.

As the global WAF market relies on WAF product performance and market expertise, Competitors A and B maintained their leadership positions because of their effectiveness in protecting against OWASP Top 10 threats and their low false positive rates.

In the global WAF appliance market, Penta Security has the 4th largest market share globally. While Asia-Pacific remains its primary revenue contributor, Penta Security Systems' proven performance continues to strengthen its market share and revenues in the other regions as well.

WAF Solutions Market Performance in Asia-Pacific



Source: Frost & Sullivan Asia-Pacific Web Application Firewall Solutions Market, Forecast to 2021

Headquartered in South Korea, Penta Security Systems continues to maintain its market leadership in the Asia-Pacific WAF market with its next-generation WAF solutions. Penta Security Systems plans to expand its footprint to other Asia-Pacific countries, alongside its focus in South Korea, with increasing demand for its on-premises and virtual software solutions.

Frost & Sullivan analysis indicates increasing market penetration in the Asia-Pacific WAF solutions market by Penta Security Systems and Competitor C. Competitor A emerged at the top for cloud-based WAF solutions, while Competitor B excelled in both application and cloud-based services.

Penta Security Systems is proactively forging partnerships with local cloud service providers in various Asia-Pacific countries. Apart from its strong presence in South Korea, the company has a branch office and partnerships with cloud service providers in Japan.

In 2016, Penta Security Systems teamed up with a key managed security service provider in Singapore to penetrate further into the Southeast Asian market.

Its solutions' capabilities are not only limited to signature matching, but also include its proprietary intelligent security engine.

Penta Security Systems plans to expand its footprint to other Asia-Pacific countries, alongside its focus in South Korea, with increasing demand for its on-premises and virtual software solutions.

About Frost & Sullivan

We Accelerate Growth

Frost & Sullivan is a growth partnership company focused on helping our clients achieve transformational growth as they are impacted by an economic environment dominated by accelerating change, driven by disruptive technologies, mega trends, and new business models.

The research practice conducts monitoring and analyzing technical, economic, mega trends, competitive, customer, best practices and emerging markets research into one system which supports the entire “growth cycle,” and enables clients to have a complete picture of their industry, as well as how all other industries are impacted by these factors.

www.frost.com

Appendix

Definition of Web Application Attacks

Cross Site Scripting (XSS)

An attack technique classified under the OWASP Top 10, where attackers inject malicious script in input fields that get stored in the web application. This, in turn, gets executed on the client side without the user being aware when the website loads in their browser.

SQL Injection

An attack technique that exploits a database by injecting a query into vulnerable input fields. By manipulating the input value of the client with the execution of an unintended SQL statement, SQL Injection can cause massive data leakage. It is classified under the “Injection” category in the OWASP Top 10.

File Upload

An attack technique where the attacker is able to upload a malicious file to gain access to the application or system. This enables the attacker to take over the system and remotely execute commands on the server computer. It is classified under the “Security Misconfiguration” category in the OWASP Top 10.

Directory Traversal

An attack technique aimed at accessing files or directories outside of the attacker’s access privileges or areas that are not available for public access. It is classified as “Broken Access Control” in the OWASP Top 10.

Stealth Commanding


An attack technique that obtains information by injecting server-side script in an input field to execute malicious system commands in the server. It is classified under the “Injection” category of the OWASP Top 10.

For more information on the OWASP Top 10 2017 most critical web application security risks, go to https://www.owasp.org/index.php/Top_10-2017_Top_10.

We Accelerate Growth

WWW.FROST.COM

Auckland	Colombo	London	Paris	Singapore
Bahrain	Detroit	Manhattan	Pune	Sophia Antipolis
Bangkok	Dubai	Mexico City	Rockville Centre	Sydney
Beijing	Frankfurt	Miami	San Antonio	Taipei
Bengaluru	Iskandar, Johor Bahru	Milan	Sao Paulo	Tel Aviv
Bogota	Istanbul	Mumbai	Seoul	Tokyo
Buenos Aires	Jakarta	Moscow	Shanghai	Toronto
Cape Town	Kolkata	New Delhi	Shenzhen	Warsaw
Chennai	Kuala Lumpur	Oxford	Silicon Valley	Washington D.C.



ABOUT FROST & SULLIVAN

Frost & Sullivan is a growth partnership company focused on helping our clients achieve transformational growth as they are impacted by an economic environment dominated by accelerating change, driven by disruptive technologies, mega trends, and new business models. The research practice conducts monitoring and analyzing technical, economic, mega trends, competitive, customer, best practices and emerging markets research into one system which supports the entire “growth cycle”, which enables clients to have a complete picture of their industry, as well as how all other industries are impacted by these factors.

[Contact us: Start the discussion](#)

To join our Growth Partnership, please visit www.frost.com

Copyright Notice

The contents of these pages are copyright © Frost & Sullivan. All rights reserved. Except with the prior written permission of Frost & Sullivan, you may not (whether directly or indirectly) create a database in an electronic or other form by downloading and storing all or any part of the content of this document. No part of this document may be copied or otherwise incorporated into, transmitted to, or stored in any other website, electronic retrieval system, publication or other work in any form (whether hard copy, electronic or otherwise) without the prior written permission of Frost & Sullivan.