FROST & SULLIVAN

Frost Industry Quotient (IQ): Asia Pacific Web Application Firewall Vendors, 2013

CONTENTS

1. Market Definition and Scope 3

2. Market Assessment 5

3. Industry Trends 7

4. Frost IQ Matrix: Asia Pacific Web Application Firewall Vendors, 2013 10

5. Profiles of Web Application Firewall Vendors 11

5.1 F5 Networks 11

5.2 Imperva 11

5.3 Penta Security Systems 12

5.4 Barracuda Networks 13

5.5 Citrix Systems 13

5.6 NSFOCUS 14

5.7 Venustech 14

5.8 Piolink 15

5.9 MonitorApp 15

5.10 Trinity Soft 16

6. The Analyst Word 16

7. Frost IQ Methodology 18

ASIA PACIFIC WEB APPLICATION FIREWALL VENDORS, 2013

1. Market Definition & Scope:

The growing reliance on web applications to drive business processes has led to a greater adoption of Web Application Firewall (WAF) solutions for many organizations in Asia Pacific. Web applications allow companies to conduct their businesses in a more effective manner, be it in facilitating a better user experience for both customers and employees alike, or by reducing operational costs. However, one of the key challenges in employing web applications has been the increased vulnerability to cyber activities such as cross-site scripting and SQL injections, activities that allow attackers to gain unauthorised access to privileged information. With organizations facing a rising number of application-layer attacks and more regulatory compliance requirements nowadays, this has led to greater WAF adoption among enterprises.

A WAF implements an input/output control on the application layer of the Open System Interconnection (OSI) network architecture model. By subjecting HTTP/S conversations to a set of rules and parameters, the WAF is able to uncover attack streams which may be hitting a web application. More importantly, the ability to customize rules to specific applications also allows the WAF to enhance their protection and guard against increasingly targeted attacks.

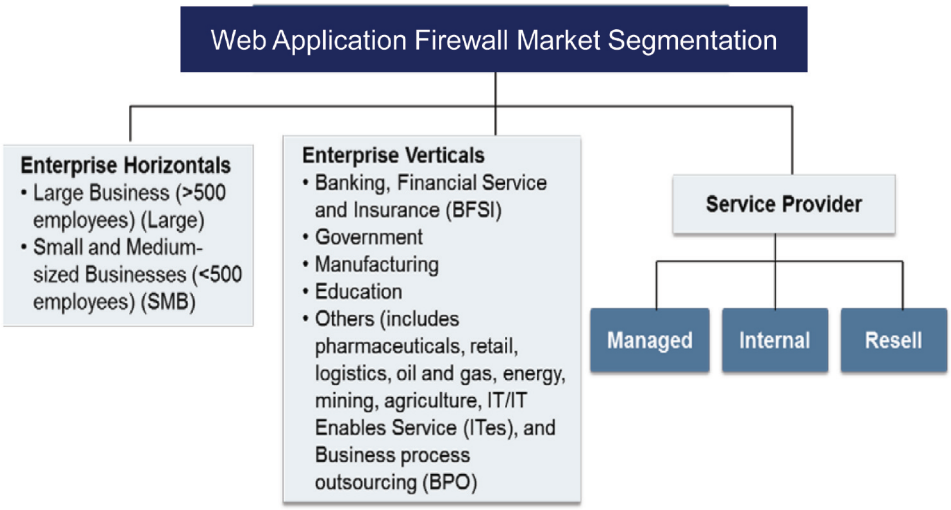
In many ways, the adoption of web applications to drive both internal (employee-facing) and external (customer-facing) business processes has highlighted the need for the WAF solution. This has exacerbated the necessity for enterprises to ensure, firstly, their web deployments are always up and running and operating at optimal levels and secondly, the websites, and the databases containing critical data which they are connected to, are adequately protected.

Across Asia Pacific, there is growing awareness towards securing web applications due to more stringent regulatory compliance required of companies when dealing with critical personal information on the web, such as Internet banking and e-commerce transactions. In light of this, WAF investment continues to grow, as more businesses start utilizing web applications and more countries implement laws that require these companies to make client data protection their top priority.

Figure 1: Key Web Application Firewall Form Factors

The increased utilization of web applications to drive business operations has led enterprises in the region to look at different form factors of WAF, be it standalone WAF appliances, integrated WAF on an Application Delivery Controller (ADC) platform, or software WAF solutions (see Figure 1). In doing so, they are looking to provide greater security and availability support to critical applications for both their customers and business partners alike. Figure 2 below exhibits the relevant market segmentations in terms of enterprise-size, industry and the type of services providers that the WAF market covers in this study.

Figure 2: Web Application Firewall Market Segmentation



Source: Frost & Sullivan analysis

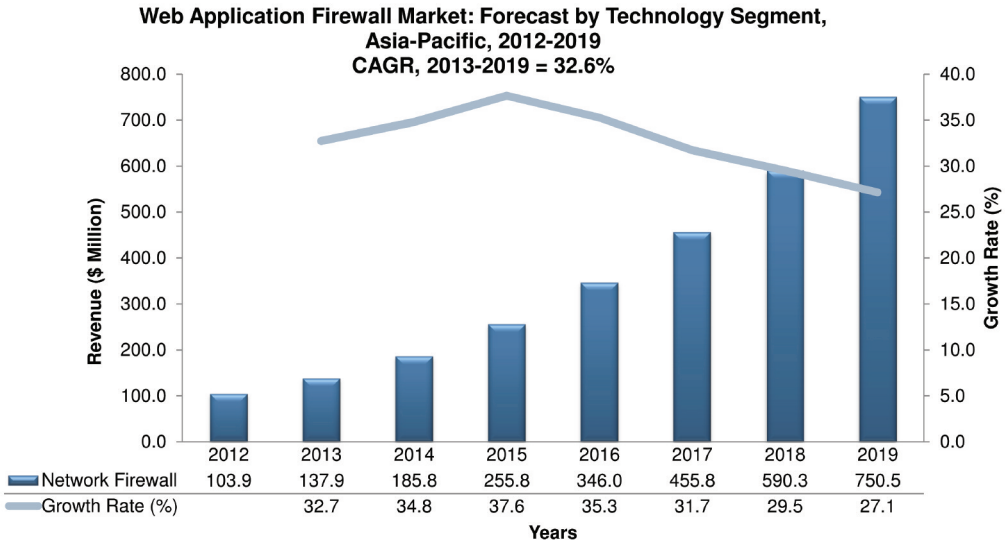
2. Market Assessment: Size and Forecast

The Asia Pacific Web Application Firewall (WAF) market (see Figure 3) is expected to grow at a CAGR of 32.6 percent over the forecast period from 2013 to 2019, with total market size likely to hit US$750.5 million by 2019. With the current market size standing at US$103.9 million in 2012, our forecasts are indicative of the tremendous growth potential in the segment. As a result, growth momentum is likely to be robust throughout the entire forecast period, with the market growth rate expected to peak in the next two years.

Standalone appliances remain the preferred form factor in the Asia Pacific WAF segment, and accounted for 77.7 percent of the market. Although cost effective integrated WAF solutions are becoming more popular, standalone versions are still viewed as being more robust and secure in protecting mission-critical web applications. This is expected to change though, as businesses, such as service providers and Small & Medium Businesses (SMBs) start to utilize integrated WAF solutions for their lower costs and ease of use.

Indeed, enterprises are increasingly looking towards WAF as an integrated feature, such as those offered as an add-on in the Application Delivery Controller (ADC) platform. ADCs are deployed to reduce network traffic load and accelerate application performance through compression, connection multiplexing, reduction of chatty protocols, in addition to traditional server load balancing. As such, their role as the guardians of web traffic heading into the backend servers makes building WAF capabilities into the ADC solutions a logical proposition.

Figure 3: Web Application Firewall Market Sizing and Forecast, 2012 – 2019



Note: All figures are rounded. The base year is 2012. Source: Frost & Sullivan analysis

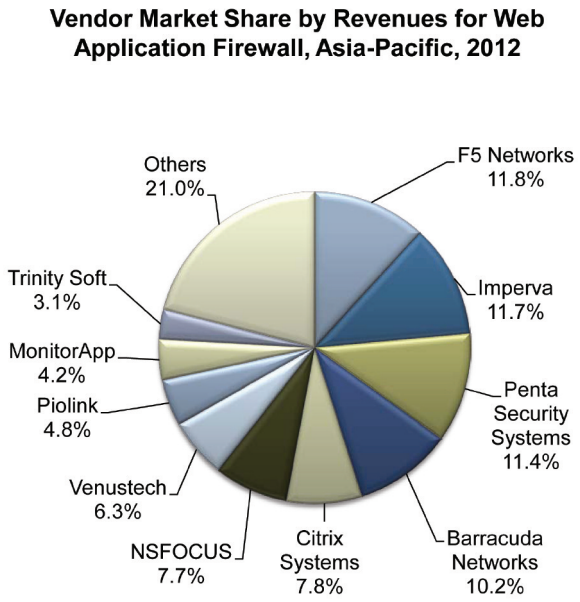
Competitive Landscape

The WAF market in Asia Pacific remains a relatively fragmented market, with no particular vendor dominating the segment. The top 10 WAF solution providers in the Asia Pacific are F5 Networks, Imperva, Penta Security Systems, Barracuda Networks, Citrix Systems, NSFOCUS, Venustech, Piolink, MonitorApp and Trinity Soft (see Figure 4). Many of these top vendors have built up a strong market presence of their own in respective regions, whilst local vendors such as NSFOCUS and Venustech from China, and Penta Security from South Korea, continue to dominate their home markets. In a way, the relatively large pool of strong players in the market is reflective of the nascent nature of the Asia Pacific WAF market.

The strength of these major players has come mainly from the local presence that each has been able to build up in the respective regions, be it their local teams or network of channel partners. Similarly, the South Korean and Chinese WAF vendors are also able to leverage on their intimate understanding of the local security threat environments. WAF vendors also compete based on cost, performance and branding of their WAF offerings. Barracuda, for example, targets price sensitive businesses with their focus on offering value-for-money solutions. In contrast, F5 positions itself as an application-centric vendor with strength in understanding how applications work, be it in terms of performance or security. Imperva, on the other hand, focuses on its reputation as a best-in-class security-centric WAF player, with complementary solutions in database security, helping to further enhance its value proposition.

The growing interest in integrated WAF solutions means that vendors offering both standalone WAF and WAF as an add-on will likely do better in the near future. The highest growth rates among the top 10 vendors came from Venustech at 62.1 percent on a YoY growth basis, followed by F5 with a YoY growth of 53.5 percent. In particular, the impressive performance of the Chinese vendor, Venustech, can be attributed to the vendor's decision to move away from selling IPS-based WAF solutions towards a full-fledged WAF solution, with their large IDS/IPS client base moving with them into the WAF space.

Figure 4: Asia Pacific Web Application Firewall Vendors Market Share (2012)



Source: Frost & Sullivan

Market Share

In 2012, the major regions in the WAF market in terms of market size in Asia Pacific are Greater China, South Korea and Japan. These 3 regions captured a total of 77.3 percent market share. Greater China was the largest contributor at 29.9 percent of the market share, followed by South Korea with 27.9 percent and Japan with 19.4 percent. Strong growth is expected in Greater China as enterprises become more informed towards the importance of having a WAF and the differences it has with network-based firewalls that operate at the network layer. Verticals such as government and BFSI have also witnessed a growing recognition and implementation of WAF solutions. The robust outlook is expected to contribute to a CAGR of 34.4 percent in the next few years, which will see Greater China capturing close to one third of the overall Asia Pacific market share at the end of the forecast period.

In terms of market growth rate, the Indian WAF market, being in a relatively nascent stage, is expected to be the fastest growing market in Asia Pacific. The market is forecasted to grow at a CAGR of 52.0 percent and reach a size of US$32.6 million by 2019. In addition, this region has seen many vendors offer integrated WAF solutions in order to provide a cheaper solution targeted at SMBs. This is due to the increasing adoption of web applications by Indian SMBs to improve the cost effectiveness of their business operations and cater to the rapidly increasing pool of Internet users in the country. Furthermore, the cost of WAF products is likely to be driven down further, with more vendors expected to enter the market during the forecast period.

3. Industry Trends

Regulatory

2012 observed a jump in attacks on web applications, mainly through cross-site scripting (XSS) and SQL injection attack vectors. Moreover, public knowledge about such attacks increased significantly, following an application server attack on Sony's PlayStation Network that saw 77 million sets of user data compromised in April 2011. As such, legislators have started to move with greater urgency and improve regulatory and compliance laws such as the Payment Card Industry Data Security Standard (PCI DSS) and Australia's Privacy Act.

At the overall level, due to the growing trend of virtualization, cloud computing and enterprise mobility, the use of web applications, which is a central component to many of these emerging trends, is likely to become more prevalent. Yet, a rise in web application usage will increase the likelihood of data breaches via the application layer of the OSI. Moreover, with the cyberspace remaining a highly unregulated arena, groups such as cyber criminals and cyber 'hacktivists' have caused plenty of worry among enterprises, especially with regards to their web-based assets. In light of these concerns, enterprises are looking to either adopt or enhance their WAF setup to comply with new regulation and compliance laws, and to defend against an increasing number of such cyber attacks.

Economic

The global economy experienced a turbulent 2012 with concerns over the health of the Euro zone's sovereign debt and the financial sector. The uncertainty has inevitably weighed down business and consumer sentiment in countries across the Asia Pacific region. Amid the deteriorating external environment, the GDP for the Asia Pacific region as a whole grew by 4.1 percent in 2012 according to the IMF, the same growth rate that was recorded in 2011. Larger Asia Pacific economies turned to web-based technologies in an attempt to enhance their business competitiveness and bring about greater cost efficiencies, especially with cloud computing and mobile devices becoming more prevalent. The Achilles heel for the smaller Asia Pacific economies remains the weaker stream of trade activities across the world, along with their weaker appreciation towards the value offered by technology, which has seen growth rates of several markets in 2012 being reduced to half of what they were in 2011.

The global macro-economic uncertainties remained a key constraint in IT spending, with most enterprises preferring to take a more prudent approach. However, strong domestic markets which witnessed the introduction of timely fiscal reforms, continued to attract investments from foreign enterprises. Many of them were also looking to leverage on the untapped opportunities in Asia Pacific, so as to counter the market sluggishness experienced in Europe and the US.

On the WAF front, the perception of Asia Pacific as a business growth region led many enterprises to invest in web installations, and subsequently WAF, as they look to increase their business competitiveness. In particular, enterprises are migrating business processes over to the web in their attempt to realize greater cost and productivity benefits. As such, despite the prevailing mood of fiscal prudence, the WAF market continues to see rising adoption levels across the Asia Pacific region, especially for enterprises which are leveraging on web applications to generate more business for their companies.

Technology

Growing concerns over the consequences of data breaches, coupled with an increasing need for companies to utilize web applications to enable or optimize business operations has helped to stimulate spending in the WAF market. Differing forms of SQL injections have traditionally been the more effective methods of application level attacks on the OSI and such attacks have existed for over a decade. However, the recent cases of high profile attacks, coupled with their rising volume, have led to greater understanding by governments and corporations towards the threats posed by SQL injections and cross-site scripting attacks. There is also greater urgency shown by these enterprises towards the need for them to safeguard important privileged information on their end.

The development trends in WAF are gradually moving towards integration with application delivery, with the technology being offered as an add-on to Application Delivery Controllers (ADCs). This convergence of technologies allows for greater network-awareness in WAF and leads to a more intelligent and holistic way of protecting web applications that do not replicate similar techniques across the ADC and WAF stages. Moreover, observing web traffic is useful in predicting SQL injection attacks since some 'hacktivist' activities have shown a pattern of starting with a Distributed Denial of Service (DDoS) attack before following up with a SQL injection. Thus, the ability for integrated WAF on ADC platforms to have greater visibility into web traffic patterns of applications during and prior to an attack, will further prevent enterprises' systems from being compromised.

Besides convergence between WAF and ADC technologies, the strategic importance of WAF also means that there is potential for WAF to integrate with other complementary security technologies. In particular, the increasing role of web applications in facilitating critical employee and customer facing processes has also highlighted the need for WAF to work in tandem and more seamlessly with security technologies protecting the backend databases. This is especially pertinent given that the web applications are often fronting data stores which contain highly sensitive information, such as those relating to monetary transactions or personal data. Likewise, the rising prevalence of Advanced Persistent Threats (APTs) also suggests that there could be value for WAF platforms in future to incorporate more features aimed at mitigating these highly sophisticated and intelligent cyber attacks and remediating the security setup in the event of a security breach.

Customer Behaviour

With the concept of 'doing more with less' resonating soundly among enterprises in Asia Pacific, enterprises are clearly set on wanting greater value from their solution providers at lower costs. Therefore, it is no surprise to see more enterprises opting for integrated solutions such as those offering WAF on ADC platforms. Many enterprises are also beginning to demand more security features in their ADC solutions, given how the convergence of the two technologies are able to offer great synergies.

However, for enterprises which are using web applications to run business-critical activities, such as monetary transactions involving customers, standalone WAF solutions remained the preferred option, with most preferring the robustness and performance levels offered by such solutions. The different buying centers that often exist in an enterprise setup, be it the applications team, the security team or the networking team, have also led to some enterprises wanting to adopt a more silo approach and opt for standalone WAF solutions. This is due to the fact that many of these teams may have different perspectives and priorities towards WAF requirements and procurement.

Competition

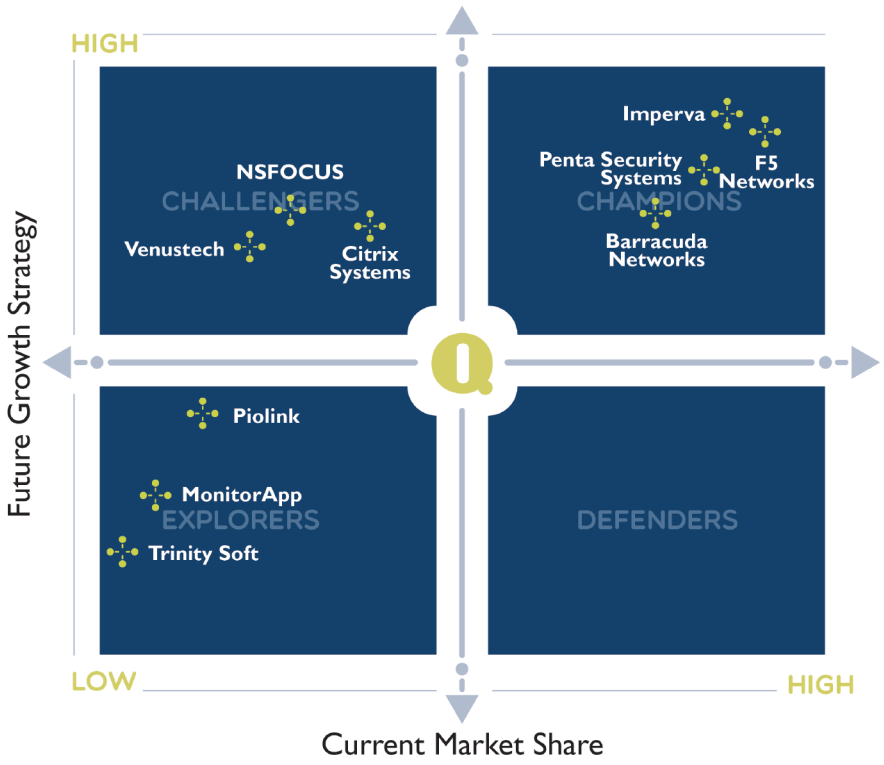
Competition among the key players in the Asia Pacific region remains fierce in the WAF market. Due to the relatively nascent nature of the market, vendors have had to introduce innovative strategies in their business plans to gain a leading edge in the market. Security vendors are competing mostly on cost and branding to distinguish themselves from other players in the market. Vendors are also targeting the need by enterprises to adhere to PCI-DSS compliance by introducing built-in auditor-friendly compliance reports. Furthermore, providing software-based solutions is becoming more popular among WAF vendors as they seek to cater to the needs of cost-conscious enterprises. Besides the new perspectives on the technological front, WAF vendors are creating market buzz across the region through road shows, end-user events and promotions. Last but not least, there is a need for greater market education in the WAF segment, given that enterprises today still perceive the WAF in the narrow definition of a compliance tool, rather than other business value it brings, such as preventing costly downtime from happening.

4. Frost IQ Matrix: Web Application Firewall Vendors, 2013

Frost & Sullivan evaluated the top 10 web application firewall vendors in Asia Pacific, based on their market share performance in CY2012. Besides market share, the following criteria were also considered in the Frost IQ matrix:

- Product/service strategy;
- People and skills strategy;
- Ecosystem strategy; and
- Business strategy.

Figure 5: Frost IQ Matrix 2013 – Web Application Firewall Vendors



5. Profile of Web Application Firewall Vendors

5.1 F5 Networks

F5 Networks currently leads the WAF market in Asia Pacific by relying on its strong market positioning and presence in the ADC market. In 2012, F5 introduced an application security assessment solution, together with WhiteHat Sentinel, Cenzic Hailstorm and IBM Rational AppScan in order to help businesses streamline the mitigation of web application-based risks and providing proactive network and application-layer protection. As part of the integration, existing users of the F5 Big-IPASM will have access to a 60-day free assessment of their websites with WhiteHat Sentinel for protecting web operations continuously.

In addition to integration with vulnerability scanners, F5 also offers its Big-IP ASM as a stand-alone solution. The ability of F5 to offer the WAF both as a standalone solution and as an add-on module on their ADC platform also means that customers have the flexibility of choosing whichever option best suits their needs. This gives the vendor the ability to offer highly customized solution bundles to customers, thus enhancing their appeal even further.

Strengths

F5 has established a strong brand name as an application-centric vendor with solutions which are highly application-fluent. This means that enterprises are quick to shortlist the vendor when it comes to their WAF requirements. F5's Big-IP ASM has also made headway into blocking of attacks based on geo-locational parameters. By integrating their WAF and ADC solutions, F5 has introduced a multi-faceted platform comprising of features such as caching, compression, SSL offload, and TCP optimization. Its solution exists both in the physical or virtual form to cater to the varied demands of enterprises in managing their applications..

Challenges

Despite the strengths of F5 in application delivery, F5 continues to suffer from a lack of mindshare as a security specialist, which has affected its appeal among customers adopting a 'security first' policy. The vendor has also not been doing as well in countries such as Greater China and South Korea, due to its lack of strong distribution channels in the markets, as well as the competitive prices offered by local vendors in these countries.

5.2 Imperva

Imperva's WAF solution, SecureSphere, continues to enjoy excellent mindshare in the WAF security market, largely due to the cutting-edge technology it offers. The protection it offers against the OWASP top 10 attacks, together with its reporting capabilities are particularly well-known among the enterprise space, and attracts many large enterprises with high security requirements in the region. Moreover, the vendor's ability to enable its WAF solution to communicate and work seamlessly with its database security solution has also strengthened its value proposition in the eyes of enterprises. This is particularly true given the growing need for enterprises to protect the sensitive data that sits behind business-critical web applications. Following Cisco's announcement on the discontinuity of its ACE WAF, Cisco embarked on a partnership with Imperva to host the SecureSphere Web Application Firewall on the Nexus and virtual services appliances. Imperva has also announced the introduction of a cloud-based WAF service, Incapsula, in order to target business from SMBs which may not have the resources for a physical WAF solution.

Strengths

Imperva benefits from the enterprise perception that it is one of the pioneering vendors in the WAF space. Its SecureSphere Business Security Suite targets large enterprises with its full range of Web Application, Database and File security. Imperva's X2500, X4500 and X6500 models include redundant hot-swappable components to increase uptime of the system, giving SecureSphere an all-round WAF security solution and allowing it to position itself as a best-in-class WAF solution. Its strong presence in the database security segment also enables the vendor to offer all-round security capabilities across web users, web applications, workflow processes and business data.

Challenges

Nonetheless, the lack of an integrated solution offering WAF as an add-on option on the ADC platform means that options are limited to Imperva's customers, especially with regards to customization. This also means that Imperva is unable to fully cater to customers who are looking for converged platforms, particularly from the mid-tier and SMB horizontal segments.

5.3 Penta Security Systems

The South Korean WAF vendor, Penta Security Systems remained a key vendor in the Asia Pacific WAF market in 2012. Penta Security's WAF product, Wapples, won the EAL 4 rating certificate from the National Intelligence Services in November 2012, which is the highest level of international common criteria recognition. Other products from the WAPPLES series include the WAPPLES MS, which allows for integrated groups of WAPPLES units, and WAPPLES V-series that offers a virtual, cloud based WAPPLES unit. Penta Security has also recently partnered with key service providers in South Korea to provide its V-Series to SMBs. This is implemented by operating the WAPPLES V-series on top of a VMware hypervisor and Xen server.

Strengths

Penta Security continues to maintain its status as a leading web application firewall vendor. It holds many patents in attack detection techniques in Korea, Japan and the US, and is PCI-DSS compliant. Penta Security's intelligent WAF, which utilizes a logic engine to detect attacks based on attack mechanisms, is what differentiates the company from the other players as it does not need to maintain a large number of attack signatures. This allows it to reduce latency.

Challenges

Despite its strength in the WAF arena, Penta Security lacks the know-how in terms of Application Delivery Controllers and hence is unable to capitalize on the recent trend in WAF-ADC integration. Likewise, it is only starting to expand its footprint into markets beyond South Korea, such as Australia and ASEAN.

5.4 Barracuda Networks

Barracuda Networks is a security and storage solution vendor with a focus on providing affordable and cost effective WAF solutions. In 2012, Barracuda launched new security capabilities for its Web Application Firewall product, targeting botnets and application-level DDoS attacks. The new security capabilities are made available following the firmware release of 7.7 on their WAF solution. The vendor has been very active in the northern parts of Asia Pacific, such as the Chinese, Japanese and Korean markets, organizing more frequent education seminars for the channel and end customers alike, with the aim of strengthening the vendor's reputation and visibility in the markets.

Strengths

Due to its products being priced competitively, Barracuda continues to appeal strongly to budget-conscious enterprises, such as small-sized e-commerce and media firms, or start-ups. Among the large enterprises, Barracuda has also gained a growing mindshare as a specialist in ADCs, with its 460 to 960 models offering a full range of ADC capabilities, despite it being positioned as a standalone solution. Its growing presence in the ADC market has allowed the vendor to cross-sell its WAF offerings as a result.

Challenges

The vendor's performance was constrained by its narrow focus in the region. Barracuda is primarily focused in the Chinese, Japanese and South Korean markets. Its lack of a 'best-in-class' reputation in the WAF segment has also limited its appeal among security-savvy enterprises.

5.5 Citrix Systems

Citrix Systems is a well-established brand name in the virtualization and application delivery segments. As a result, the vendor is able to tap on its presence in the ADC space to drive forth its WAF business. Specifically, Citrix is able to offer an end-to-end value proposition from virtual servers to virtual desktops, allowing it to create many cross-selling opportunities between products, including cross-selling its WAF solution on its NetScaler ADC platform.

Strengths

The vendor's strengths lie in it being known as an application-centric vendor, which means that it is able to build up strong credibility as a WAF vendor capable of protecting against application layer attacks. Its NetScaler AppFirewall utilizes both attack signatures and a learning engine that is able to detect unusual and unexpected behaviours from applications or services in the system. Furthermore, the fact that the AppFirewall can be fully integrated into its NetScaler ADC platform or exist as a standalone solution is also a plus point for enterprise customers.

Challenges

Citrix remains heavily focused on its end-to-end value proposition in the virtualization arena, thus resulting in a lack of focus on its WAF product line. Such an approach has also resulted in the vendor suffering from dilution to its positioning as a WAF specialist.

5.6 NSFOCUS

NSFOCUS has been the largest WAF vendor in China over the past few years. The large installed base the vendor has in China alone, has enabled NSFOCUS to become the sixth largest WAF vendor in the Asia Pacific market in 2012. In the Greater China WAF market, NSFOCUS also enjoys 25.6 percent of the market, making it the market leader for the region as well. Besides its WAF portfolio, NSFOCUS is one of the top network security product and services providers in the mainland Chinese market. The vendor has put in continuous efforts to expand its footprint globally and aspires to become a global leader in the field of information security.

Strengths

Besides enhancing its WAF functionalities and platform performance, NSFOCUS has put in significant R&D focus and efforts on strengthening both the attack and defend capabilities in its WAF solution. This approach is key to differentiating the vendor's WAF solution over competitors and also contributes to NSFOCUS's aim of being a best-of-breed WAF vendor. The vendor also enjoys a very strong reputation and mindshare in the Chinese market. From the business performance perspective, in addition to its traditional key vertical market, such as the government sector, other vertical markets such as telecoms and FSI have also witnessed a strong boost in terms of demand.

Challenges

In 2012, the vendor put in concerted efforts to push its WAF solution into international markets. However, its success was limited due to the lack of local presence and a weak channel setup that the vendor has at this point of time. The vendor may consider having more global certifications for its WAF solution, in order to enhance its standing as a credible solution in the international market.

5.7 Venustech

Venustech is a leading network security vendor in the Chinese market, known especially for its Intrusion Detection System (IDS) solution. The vendor first introduced its WAF solution in 2000, a product which was based on the same platform as its IDS solution. This approach was not well-received in the market, which meant that the mindshare and business presence of Venustech remained relatively weak. In 2011, Venustech did a product refresh and migration for its WAF solution, which improved the vendor's positioning and market share in the WAF market, significantly.

Strengths

Venustech witnessed a strong YoY growth in the Chinese WAF market, registering a high growth rate of more than 60 percent. The growth was mainly driven by the product enhancement made by the vendor when it transitioned its WAF solution from the traditional Intrusion Detection System (IDS)-based platform to a new platform. This helped to significantly enhance enterprise perceptions towards Venustech's credentials and commitment in the WAF market. Moreover, 2012 also saw Venustech actively promoting its WAF solution in the market. In addition, the vendor released several high-end models with throughput of more than 10G.

Challenges

At present, the international edition of Venustech's WAF solution is limited. It will take some time for the vendor to be able to enjoy success beyond its home market, China. A limited percentage of its clientele is also coming from the private sector in China. This offers tremendous growth potential for the vendor.

5.8 Piolink

Piolink is a market leader in the South Korean ADC market and this has helped the vendor to make a sizable foray into the WAF market as well. Piolink's WAF product, WEB FRONT, won the EAL 4 rating certificate from the National Intelligence Services in 2008, which is the highest level of international common criteria recognition in the country. Both the WEB FRONT GS and SE models also won the GS (Good Software) certification from the Korea Testing Laboratory. Piolink is also able to offer customers its WAF offerings as either a stand-alone solution, or as an add-on feature on top of its ADC solution. WEB FRONT's ability to offer virtual logic in its physical solutions also attracted many enterprises to the solution.

Strengths

As the market leader in the South Korean ADC market, Piolink enjoys a good reputation and strong mindshare in the country. Its financial stability and commitment to technology leads it to invest heavily into R&D.. With its security switch and WAF solutions, Piolink is trying to extend its product portfolio and build up its business presence in Japan and China as well.

Challenges

Its weak reputation outside the Korean market, along with a perceived attention bias towards its ADC business remain the biggest challenges for Piolink, particularly if it is looking to expand its presence across the Asia Pacific region.

5.9 MonitorApp

MonitorApp is a South Korean WAF vendor and its solution, the WEB Insight SG, also received the EAL 4 rating certificate from the National Intelligence Services. MonitorApp provides physical and virtual WAF solutions which can work across 8 logical scenarios. To provide better performance in high-end solutions, MonitorApp added Web-acceleration into the WEB Insight SG platform. MonitorApp also provides cloud WAF service to customers through a partnership with Innogrid (cloud, CDN service provider). This is particularly useful among customers who are moving more functions into the cloud and who are not too keen to install hardware appliances on their premises.

Strengths

MonitorApp remains highly committed to technology excellence and solution R&D. The majority of its employees are working in the R&D division. Its main products are the database firewall, VoIP firewall and Web application firewall. The vendor has also put in much effort to offer better customer service and provide user friendly interfaces.

Challenges

MonitorApp is keen to expand its business footprint into other markets in Asia Pacific such as Japan, Thailand and Malaysia. However, the vendor still suffers from a weak reputation and low visibility levels.

5.10 Trinity Soft

Consistent with the other key South Korean WAF vendors, Trinity Soft is also a recipient of the EAL 4 rating certificate, which is awarded by the National Intelligence Services for its WEBS-RAY solution. The vendor tried expanding its business beyond the South Korean market by striking a partnership with Insidepro. Trinity Soft upgraded its monitoring utility named WEBS-RAY I-UI, which can provide a monitoring dashboard without having to install any applications into the PC and it just works via an Internet browser. One UI can control multiple WAF solutions and it can also check real-time monitoring and equipment as well as logs for intrusion detection..

Strengths

Trinity Soft has established a good reputation in the government sector. The vendor hopes to replicate its success in the public sector in the private sector as well.

Challenges

Trinity Soft is only focusing on the South Korean market, which means it will face growth limitations at the Asia Pacific level.

6. Analyst Word

With more enterprises looking to migrate key business functions over to the web and utilize web applications to drive business processes, the need for WAF will only become more pronounced in future. As cyber attacks and threats become more sophisticated, enterprises will require the security intelligence and application fluency offered by WAF technology, in order to protect their business-critical web installations from increasingly prevalent application layer attacks.

Technology convergence has seen vendors looking to offer WAF as an integrated feature on the ADC platform. The synergies created by combining the two application-centric technologies have resulted in more enterprises looking at such options, especially those looking to have the best of both worlds in the area of application performance and security.

Among the more security-conscious enterprises, however, many may still opt for standalone WAF solutions due to their robustness and the high performance levels. Some in this group are also looking for the WAF platform to incorporate more security capabilities into the solution, be it features protecting against Advanced Persistent Threats (APTs) or Distributed Denial-of-Service (DDoS) attacks. The ability for the WAF solution to communicate and work together seamlessly with other complementary security technologies, such as database security, is also emerging as a key differentiator for some WAF vendors.

The relatively nascent state of the WAF market in Asia Pacific means that the competitive landscape remains highly fragmented, with many local players in markets such as China and South Korea proving to be strong vendors in their respective markets. Their localized understanding towards both the market dynamics as well as the threat landscape continues to provide the local companies with the necessary tools and knowledge to compete effectively against the global vendors.

As WAF gradually becomes a critical and strategic security component in a cloud-centric era, many global vendors are expected to cast greater attention on what is still a relatively niche segment. Industry consolidation is likely to happen sooner rather than later, as technology vendors look to include WAF technology in either their solution or services portfolio, to allay the concerns that their enterprise customers may have towards the 'webification' of business processes. Such dynamics are also expected to drive greater innovation in the WAF market, as vendors seek to enhance the value offered by their WAF platforms, with more enterprises looking for WAF to be offered as a multi-faceted solution platform.

In light of the growing importance of WAF technology, enterprises will do well to keep themselves abreast of the latest developments in the market. The criticality of WAF will also differ across different enterprises, with some opting to drive mission-critical processes via web applications, whilst others may look to take on a more conservative approach. As such, the WAF requirements will also differ across enterprises and it is thus pertinent for enterprises to do a mapping of their needs against what the various WAF vendors are offering.

7. Note of FrostIQ Methodology

The focus of FrostIQ is to provide a balanced assessment of selected markets. The markets are those that have been tracked rigorously by Frost & Sullivan analysts over a period of time. Data that has been collected, such as vendor revenue, is scrutinized and forms part of the input for the Frost IQ matrix.

The study approach provides a mix of quantitative and qualitative assessment. The Frost IQ matrix has two major attributes. They are market share and future growth strategy.

1. Market Share

Market share information is derived from Frost & Sullivan research programs. These research programs include market trackers and syndicated research reports. From the regular research which is conducted at quarterly, semi-annual or annual intervals, analysts build a strong revenue database relating to vendors in the market.

According to the Frost IQ Matrix, the X-axis measures the share on a percentage scale. The divide line on the matrix is set at 50 percent of the market share of the leading player in that market.

2. Growth Strategy

Frost & Sullivan considers 4 main components in the growth strategy assessment part of Frost IQ. The guiding principle is that these components and their subcomponents should follow the MECE (Mutually Exclusive and Comprehensively Exhaustive) test. The proposed components are as follows:

- Product/ service strategy
- People and skills strategy
- Ecosystem strategy
- Business strategy

There is an equal weightage to all the components with measurement on a 10 point scale. The dividing line on the Y-axis is at the mid-point i.e. a weighted score of 5 on a 10 point scale. Analysts will provide feedback on the industry participants on the above parameters based on continual market research and analysis.

Details of the sub-components are available, if required.

ABOUT FROST & SULLIVAN

Frost & Sullivan, the Growth Partnership Company, works in collaboration with clients to leverage visionary innovation that addresses the global challenges and related growth opportunities that will make or break today's market participants. For more than 50 years, we have been developing growth strategies for the Global 1000, emerging businesses, the public sector and the investment community. Is your organization prepared for the next profound wave of industry convergence, disruptive technologies, increasing competitive intensity, Mega Trends, breakthrough best practices, changing customer dynamics and emerging economies? Contact Us: Start the Discussion

Contact
Tel: +65.6890.0999
Email: apacfrost@frost.com
Website: www.frost.com

DISCLAIMER

COPYRIGHT NOTICE