F1security

Web Security Platform

SaaS-based universal service for MSSP

Whitepaper Ver 1.0

We are not just vendors that make products. We are a consulting firm.

www.f1security.co.kr/english

Contents

Web Growth and Security

Importance of Web Security

- Websites are the most frequently attacked target

- Websites are the system with the most information leakages

- Web is the most popular service for Internet users

Problems faced by Managed Security Service Providers

- Difficulty in Acquiring Web Security Professionals

- Difficulty in integrated management of web security solution, increase in operating cost

- Difficulty in Deploying it in a Cloud Environment

Suggestions for the solution

- Continuous professional service through outsourcing

- Improve operational efficiency and reduce costs through integrated management of web security solutions

- Utilization of SaaS-based solutions and maintain customer service levels

F1security Web Security Platform Background

- Established Information Security Consulting Division

- Established R & D Center and Malware Analysis Response Team

- Microservice architecture, combination of machine learning and artificial intelligence

Web Growth and Security

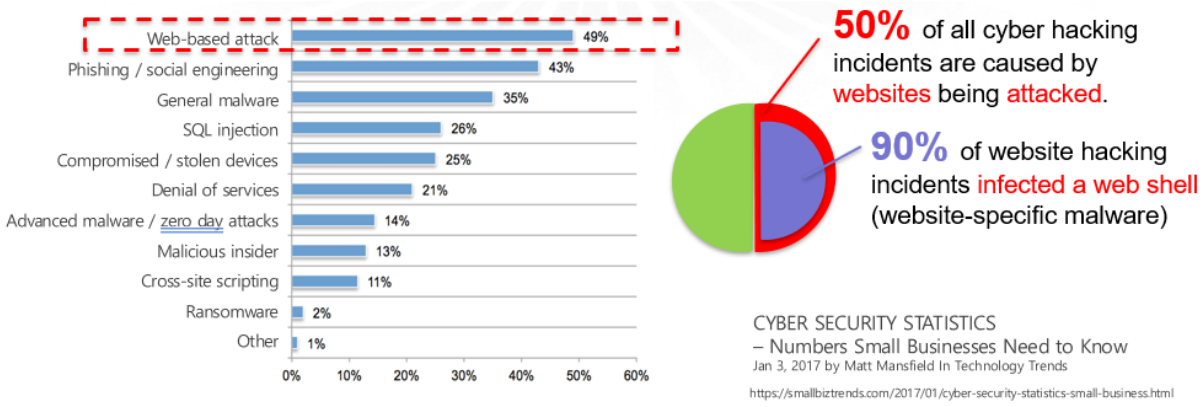
With the emergence of the World Wide Web in 1989, the private sector's participation in the Internet, which was previously used primarily for education or public purposes, was rapidly expanding, bringing both quantitative and qualitative expansions in terms of content and users. Later, with the introduction of mosaic web browsers in 1993 and the emergence of the web search service Yahoo in 1994, the number of web users exploded on the Internet. In addition, with the introduction of Apple's smartphones in 2007, web access via mobile grew rapidly, and in 2018, 52% of global web traffic came from mobile devices.

As of 2018, the world's number of websites is 1.24 billion (16% of the world's 7.5 billion people), and the number of online visits for social media and information gathering was the second largest online activity after email. Worldwide retail e-commerce sales are expected to grow steadily over the last few years, reaching $ 4.4 trillion by 2021. As such, the Internet and the web are rapidly spreading in our daily lives, giving life changes and benefits that are hard to find in the history of human history.

However, websites aimed at providing external web services are open to the Internet 24 hours a day, 365 days a year, and became top priority targets for hackers because they store important online data of companies and individuals. In fact, website targeted hacking incidents are constantly occurring every year. Recently, more than 160 million customer data were leaked from US bank Capital One, which was also caused by a hacking of a Web site, and Capital One analyzed that it would cost about $ 150 million to resolve the hacking incident.

Importance of Web Security

Of all the various hacking paths, web site attack is accounted for the half of the entire attacks, the most targeted system for the hackers. In addition, 90% of the hackers who have successfully hacked websites install a Webshell, a malicious code specifically designed for targeted website.



Since Web sites are the most favorable targets for hackers, causing the most security incidents with massive damages to the customers, they should be the priority for the protection in terms of information security.

Problems faced by Managed Security Service Providers

Operators who provide Management Security Service can install and operate various web security solutions to protect customers' websites. However, a paradigm shift is needed to solve the difficulties of integrated management, increase system implementation costs, and difficulty in securing experts.

- Difficulty in Acquiring Web Security Professionals

Web security is not only solved by the introduction of security solution, but also requires operation management along the cycle of prevention, detection and response. In other words, preventive processes for proactively diagnosing and removing vulnerabilities of customer web sites, security solutions such as web firewalls, detection processes for monitoring hacking signs, and web shells installed through hacking are analyzed for deletion / isolation and incurring additional damages. Responsive processes should be organically interoperable and managed.

The important point here is that each process requires a high level of expertise in information security, so it is necessary to have a suitable staff. So how can MSSP secure these web security experts? And how can you continuously upgrade the expertise of the workforce you secured? On the other hand, is it the only strategy of choice to employ all process-specific web security experts within the MSSP organization?

- Difficulty in integrated management of web security solution, increase in operating cost

Although MSSP can provide security services by implementing security solutions to protect customers' web sites from hacking, there are similar products in web security solution categories which takes a lot of time to evaluate and facing the challenges of managing and operating them individually. In other words, web application vulnerability diagnosis scanners, web application firewalls, and web shell detection solutions provided by different developers are operated in different central management systems.

This increases the complexity of the MSSP service provider's service infrastructure and increases costs such as infrastructure system construction and maintenance, thereby deteriorating profitability. Is there any way to manage various web security solution categories through a single integrated central management system?

- Difficulties Deploying in a Cloud Environment

As cloud migration of on-premises systems is rapidly progressing, web security solutions provided as hardware-based dedicated appliance devices cannot be used in cloud environments unless server rack space is rented from cloud providers. In addition, solutions that simply port existing hardware-based products to software may raise questions about functionality and performance.

Is there any way to deploy and install an existing web security solution while maintaining its stability without being affected by cloud migration process?

Suggestions for the solution

- Continuous professional service through outsourcing

A Korean MSSP signed an outsourcing agreement for the provision of web security services with an external information security consulting firm with its own web security solution. The MSSP provides professional web security services to end customers without having to retain or retain web security experts within the company.

Specifically, an external contractor contracted outsourcing MSSP customer's web application vulnerability diagnosis and simulation hacking service, web firewall construction and operation support, web shell (web malware) detection system support, web shell code analysis and treatment, etc. It responds to accidents and detects web shell spreading. In other words, MSSP and external specialists are collaborating to service the entire process of prevention, detection and response of web security. This collaborative model enables MSSPs to successfully deliver highly specialized web security services to end customers even when their internal human resources are scarce.

F1security is a company that has grown to provide information security consulting services. F1security has been recognized for its credibility by obtaining the certificate of information protection service company that grants only strict preliminary examination by the Ministry of Science and ICT to Korea. This certification is held by only 2% of Korean security companies. Web vulnerability diagnosis and simulation hacking and response to web site / server infringement incidents reflect the know-how accumulated in the field in the development and research of security solutions to provide professional services and solutions for web security at the same time. At the time of writing, F1security is the only company in Korea that has the capability to perform, develop, build, and operate its own web security services and web security solutions (3 types) in-house.

- Increase operational efficiency and reduce costs through integrated management of solutions

To strengthen web security, multi-layered protection is required for multi-layers such as web servers, web middleware, web applications, and various solutions must be introduced. The introduction of individual vendor products from a variety of solutions can lead to poor work efficiency and increased costs during deployment and operation. In particular, as MSSPs serve a large number of end customers, the associated costs skyrocket.

A South Korean MSSP is seeking to increase operational efficiency and reduce costs by integrating web firewall, web shell detection and web shell scanning products from one vendor. In this case, it is possible to unify the contract window when the solution is introduced and the maintenance window after the construction, as well as the unification of the technical support window during the construction and operation.

An important factor in the integration of web security solutions is whether different products can be managed from one central management system. An integrated central management system should provide a dashboard for setting up and integrating solutions for solution administrators and users. Furthermore, if individual products such as web shell scanners and web firewalls are dynamically interconnected to provide security functions, web security is possible at a different level from the conventional solution.

- Using Software and SaaS-based solutions and maintain customer service levels

When deploying a web firewall to protect leased web servers from cloud providers, you have the following options: In the case of a VPC (Virtual Private Cloud) contract, a dedicated server rack is used so that a hardware-based appliance web firewall device can be installed on-premise as before. On the other hand, if you use Public Cloud, you can lease one more VM server, install web firewall software, install it as a proxy method, use SECaaS provider's web firewall service, or install a software-based web firewall directly on the web server. In this regard, the service model of the web firewall can be summarized as follows.

< Comparing Web Firewall Service Models >

	On-Premises		Cloud-Based		F1security Solutions
	Software	Hardware	Software(VM)	SECaaS	
Distribution types	Agent S/W	Appliance H/W	Virtual Machine + Agent S/W	DNS Proxy	Agent S/W
Distribution target	Vendor cloud	Physical shipping	Cloud Service Provider(CSP), Cloud environment	Vendor cloud	Vendor cloud
Installation place	Web server	network	Web server	-	Web server
Cloud Server installation	x	x	○	○	○
Central management	Requires separate server	Requires separate server	cloud	cloud	cloud
Deployment/ Maintenance Costs	Medium	High	Medium	Low	Low
Billing cycle	1 year	1 year	1 month	1 month	1 month
Main Contract Partner	customer - MSSP	customer - MSSP	customer - CSP	customer - SECaaS	customer - MSSP

If an end customer installs a web firewall directly through a cloud operator's marketplace or uses a SECaaS provider's web firewall service, MSSP's service will reduce the portion of the web firewall control service to end customers. On the other hand, for software-based web firewall products that are installed directly on a web server, MSSP can provide installation, configuration, monitoring, and response after a service agreement with an end customer, in the same public cloud environment as on-premises. It's a viable option for providing end customers with security services for the entire lifecycle of Web security for MSS.

F1security Web Security Platform Background

- Established Information Security Consulting Division

F1security was founded in 2012 as a company specializing in information security consulting and has developed its own web security solution to solve customer's difficulties, such as vulnerability diagnosis and incident response. In addition, the solution is continuously improved by reflecting consulting know-how and results.

- Established R & D Center and Malware Analysis Response Team

F1security operates a technical research institute that develops and maintains web security solutions. It also runs an Analysis and Response team that analyzes new / variant web malware and responds to incidents. As such, F1security has its own technology lab and analytical response teams, providing immediate, one-stop solution research, development, and analysis / response. In addition, the R & D Center and the Malware Analysis and Response Team have been recognized for their expertise and technology as they carry out the research assignment of the Korean government. The service is directly supported.

- Microservice architecture combines machine learning and artificial intelligence

F1security's web security solution is based on a microservices architecture that takes advantage of the platform's flexible architecture, allowing customers to quickly add value-added services that customers need, such as detecting personal information exposure through a Web site. In addition, by applying machine learning technology, the detection algorithm is advanced with artificial intelligence beyond pattern matching.