

Oct. 2021

Unified Web Security Service (UWSS)

Our web Security solution Protects 4M websites a day

T: +82-70-4640-3031

gpartners@f1security.co.kr

www.f1security.co.kr



Table of Content

Unified Web Security Service

F1-UWSS

I Web Security Needs

II Web Security Issues

III The emergence of Unified Web Security Service

IV Features of Unified Web Security Service

V Key Contents of Unified Web Security Service

VI Reference

Unified Web Security Service

F1-UWSS

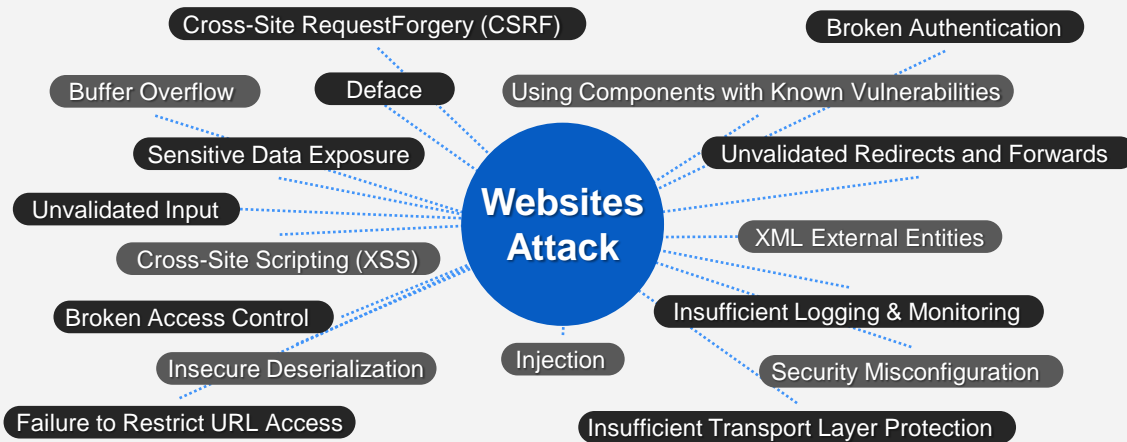
1 . Web Security Needs

Web hacking is making the cyber world too noisy

80% of all cyber hacking incidents are caused by **websites** being **attacked**



↑70% of ransomware attacks are **distributed via websites**



Wannacry (ransomware) infected **300,000 PCs in 150 countries** on May 12, 2017

One in 13 of the world's websites is **malicious**

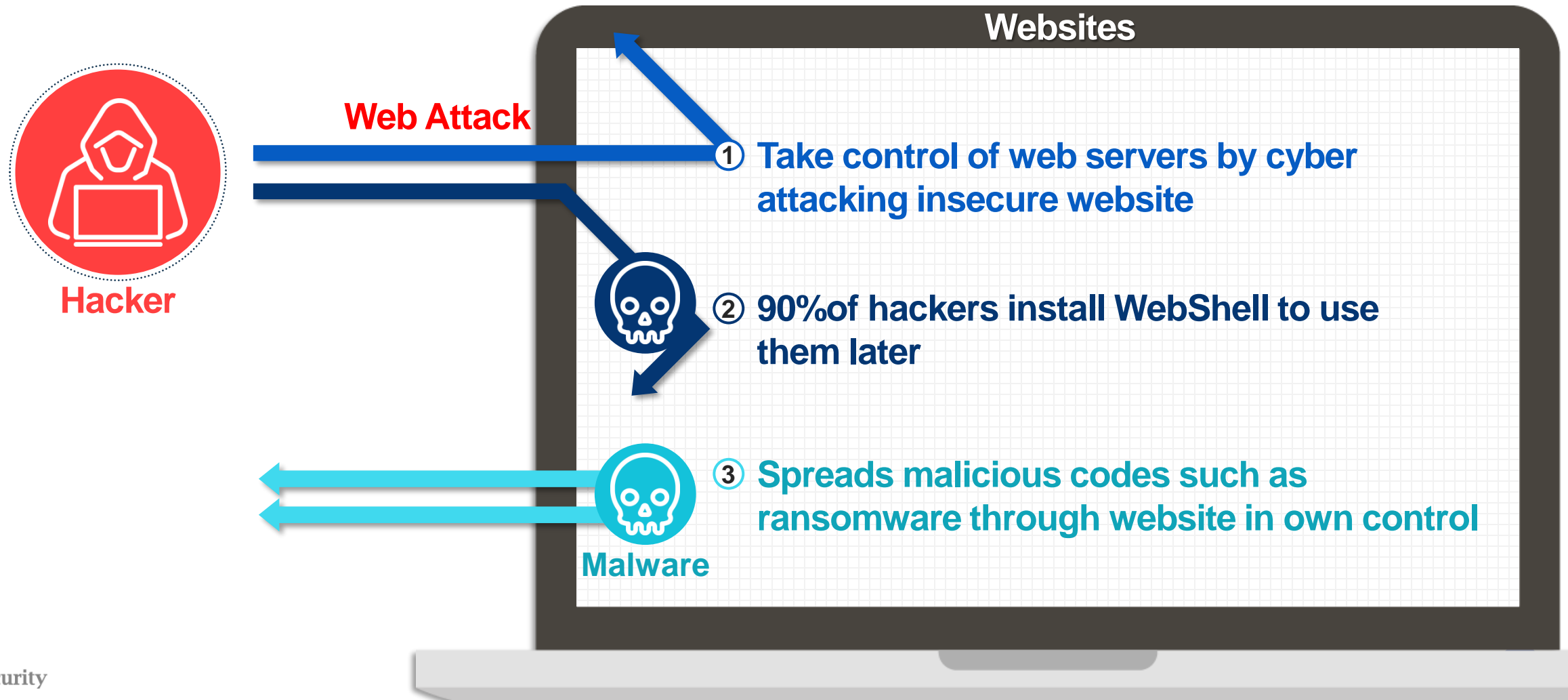
※ Source: Security News(<https://www.boannews.com/media/view.asp?idx=55170>)
Computer World(<http://www.comworld.co.kr/news/articleView.html?idxno=49509>)

Unified Web Security Service

F1-UWSS

II. Web Security Issues

Web hacking cannot be solved with a single security product



Freedom from Web Security issues is not free

● Market Status

There are so many kinds of **security solutions**



Web security solutions require **specialized knowledge to use**



Many web security solutions on the market, but **not for SMEs**

※ SME: Small and medium enterprise



● Problem

Make customer choice **difficult** and increase system **complexity**



Many companies **do not have Information security experts**



Security solution is **too expensive to majority of SMEs**



Unified Web Security Service

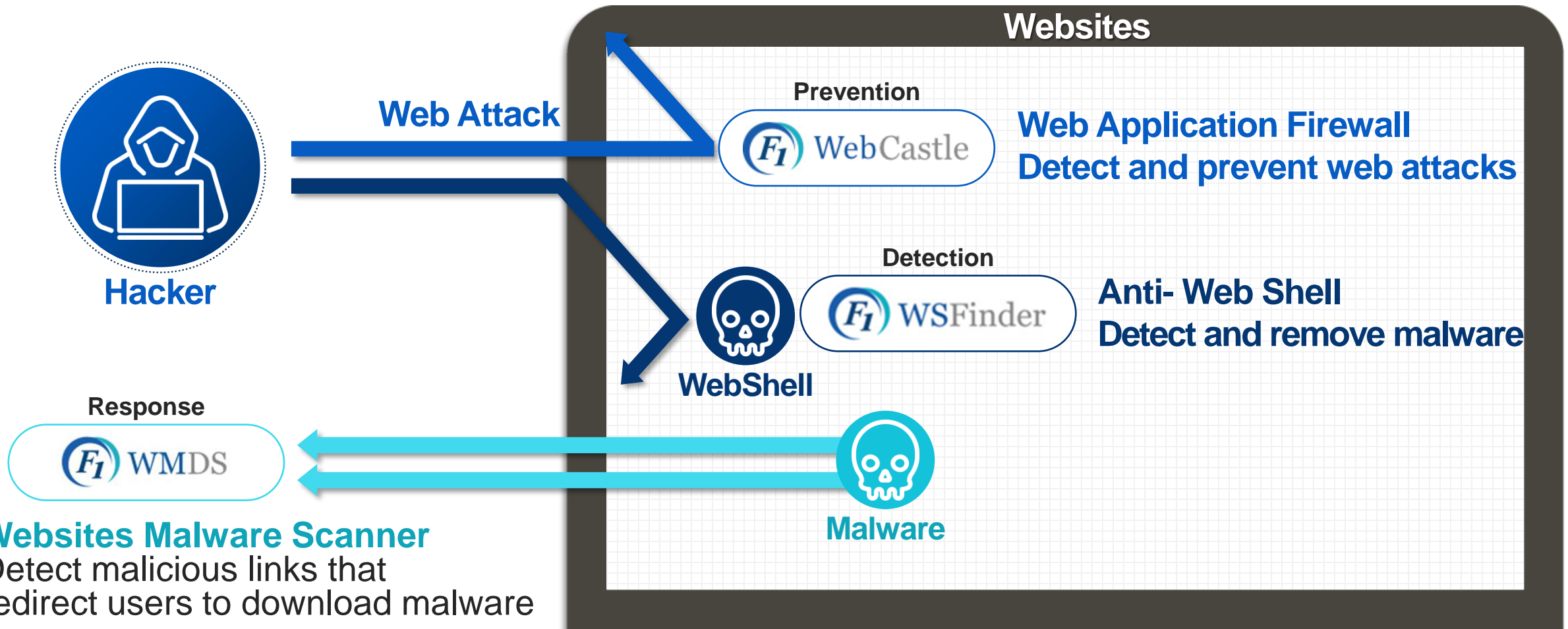
F1-UWSS



III . The emergence of Unified Web Security Service

III. The emergence of Unified Web Security Service

We develop a solution to prevent, detect and respond to web hacking



III. The emergence of Unified Web Security Service

We provide all-in-one web security solution with one platform

Conceptual expansion and refinement



F1Security

UWSS: Unified Web Security Service

All-In-One

FORTINET

UTM



Firewall

IDPS

Anti-virus

* UTM: Unified Threat Management,
IDPS: Intrusion Detect Prevent System



WebCastle



WSFinder



WMDS



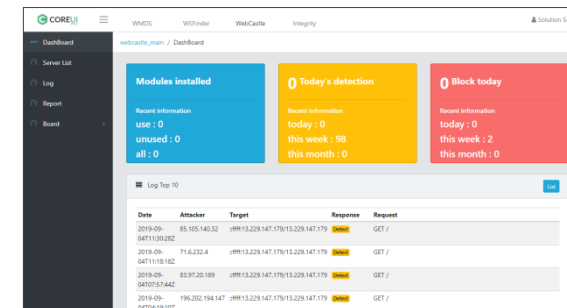
WFDetector

Packaging Products



Centralized management

- ❖ Web Application firewall
- ❖ Anti-WebShell detection
- ❖ Website Malware scanner
- ❖ Website Forgery Detection etc.

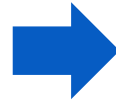


III. The emergence of Unified Web Security Service

Give our customers **the freedom of web security**

● Problem

Make customer choice **difficult** and increase system **complexity**



Many companies **do not have Information security experts**



Security solution is **too expensive to majority of SMEs**



● Solution

Packaging the Security Products Needed for Web Security



Intuitive web-based UI user experience in one platform



Reasonable pricing with software and cloud-based system



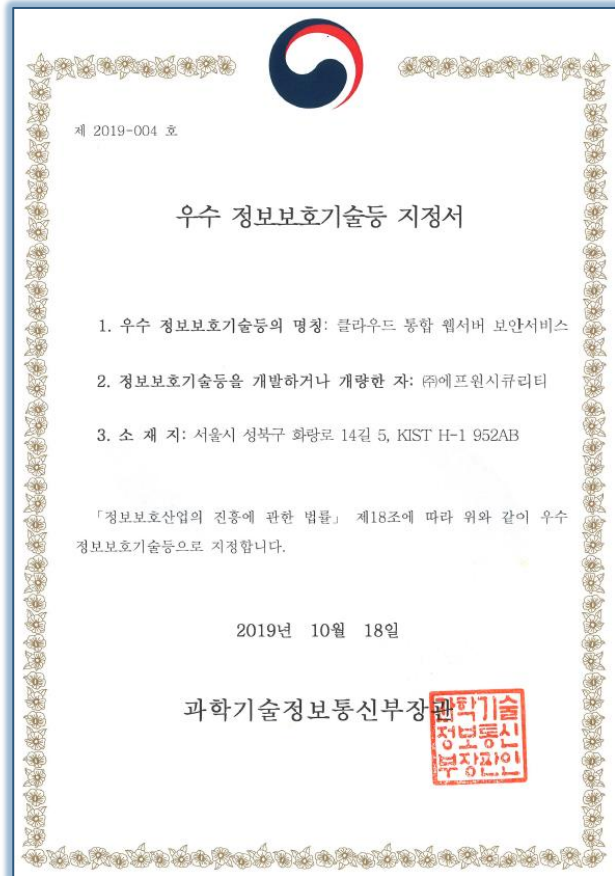
Unified Web Security Service

F1-UWSS

IV. Features of Unified Web Security Service

IV. Features of Unified Web Security Service

Excellent information security product and technology designated by the Ministry of Science and ICT of Korea



과학기술정보통신부
Ministry of Science and ICT
www.msit.go.kr

보도자료 I-KOREA 40
4차산업혁명의 큰길로 대한민국이 달려갑니다. 사할 중심의 4차산업혁명 실현

보도일시	2019. 10. 18.(금) 조간(온라인 10.17. 12:00)부터 보도해 주시기 바랍니다.		
배포일시	2019. 10. 17.(목) 09:00	담당부서	정보보호산업과
담당과장	정은수(044-202-6440)	담당자	정영관 주무관(044-202-6442)
관련기관	한국인터넷진흥원 보안기술확산팀 오주형(061-820-1249)		

과기정통부, 신기술(5G 빅데이터 인공지능 클라우드) 기반 '2019년 우수 정보보호 기술 제품' 5건 지정
- 판로개척·기술개발(R&D) 연계 지원을 통한 지속적 혁신성장 지원 -

- 과기정통부(장관 최기영, 이하 '과기정통부')는 (주)라인컴퍼니, (주)삼오씨엔에스, (주)스파이스웨어, (주)에프원시큐리티, (주)와이키키소프트가 개발한 정보보호 신기술을 '2019년 우수 정보보호 기술·제품'으로 지정(유효기간 2년)한다고 밝혔다.
- 올해로 2회째인 우수 정보보호 기술 등의 지정제도는 기술경쟁력 있는 정보보호 벤처기업의 신기술을 발굴하여 홍보, 해외진출, 연구개발(R&D) 등을 지원하는 제도로 정보보호 산업 육성에 기여하고 있다.
- 산·학·연 전문가와 벤처사 등으로 구성된 우수 정보보호 기술 심사위원회에서 지정신청기술에 대한 신규성, 독창성, 사업가능성 심사를 통해, 4차 산업혁명의 기반이 되는 5세대(5G) 이동통신, 빅데이터, 인공지능(AI), 클라우드 관련 우수 정보보호 기술·제품 5건이 지정되었다.

- 올해 지정된 우수 정보보호 기술·제품은 ▲5G 모바일 환경에서의 앱 보안솔루션인 '리엡(라인컴퍼니)', ▲머신러닝 분석기법을 활용하여 개인정보 침해사고를 탐지·예측하는 솔루션인 '파르고스(삼오씨엔에스)', ▲클라우드 환경에서 데이터 암호·복호화가 가능한 '스파이스웨어(스파이스웨어)', ▲인공지능 기반으로 웹 악성코드를 탐지하는 '클라우드 통합 웹서버 보안서비스(에프원시큐리티)', ▲생체인식과 이상징후 탐지기술을 결합하여 비밀번호 입력이 필요 없는 '와이덴터티 2.0(와이키키소프트)'이다.
- 이번에 지정된 기술·제품에 대한 자세한 정보는 과기정통부 누리집(www.msit.go.kr) 및 한국인터넷진흥원 누리집(www.kisa.or.kr)을 통해 10월 18일(금) 공고될 예정이다.
- 지정된 기술·제품에게는 과기정통부 장관 명의로 '우수 정보보호 기술·제품' 지정마크가 부여될 예정이며, 과기정통부와 한국인터넷진흥원이 정보보호 기업 육성을 위해 추진하는 해외진출, 제품개발 등 사업에 지원하는 경우 가점을 받게 된다.
- 과기정통부 오용수 정보보호정책관은 "정부 및 공공기관 발주자 대상 우수 정보보호 기술·제품 설명회와 지원사업 확대 등을 통해 우수한 신기술을 보유한 정보보호 벤처기업이 지속적으로 성장할 수 있도록 지원해 나갈 계획이다."라고 밝혔다.

[붙임] 2019년 우수 정보보호 기술·제품 지정 개요

※ Excellent information security products and technologies are described in the "Information Security Industry Promotion Act."

IV. Features of Unified Web Security Service

Detection and analysis of malicious code distribution on 4 million website

Business Summary

Business item

Malware Analysis & Distribution Detection
Treatment support business

ordering organization

KISA

Business Period

2017.1.1 ~

Abstract

Detect malwares, Prevent distribution through web and respond early

Description

MCF (Malicious Code Finder) Operation Business For all Korea website a day (4M Websites/day)

Malware distribution response Activity through web			
Response report of media report	Report of Issue response	Response report of mass detection	Periodic Report (Stat's, Trends)
dissemination Detection	deletion Treatment	malware Analysis	Foreign dissemination site command control server Block
System automatic detection Outside detection C-TAS, Google, MS, etc Webhard, Free SW detect Forgery	Treat stop by site Treat distribution site Send treat guide letter Investigae CS(Customer Satisfaction)	Analyse malicious scripts Compose distribution structure Analyse malware Create detection pattern Check command control server	Block foreign distribution site Block foreign information leakage site Block foreign command control site
Update check domain - Domestic domain selection - Check domestic domain connection Webhard, free SW - Update checking object information	System malfunction Mgt. - 2017 new introduced system stabilization - First reporting, recover in 1hour	Human Mgt. - Affair capability analysis capability reinforcement - Stable personnel offering - Manage affair satisfaction & encouragement	Project Mgt. / Support - Security management - Schedule production item Mgt. - Education and counseling

IV. Features of Unified Web Security Service

Yearly 5,000 websites vulnerability checking and treatment support

Business Summary

Business item

web vulnerability diagnosis and
web security tool supplement business

ordering organization

KISA

Business Period

2017.1.1 ~

Abstract

Perform web vulnerability diagnosis,
web shell detection, web firewall supplement

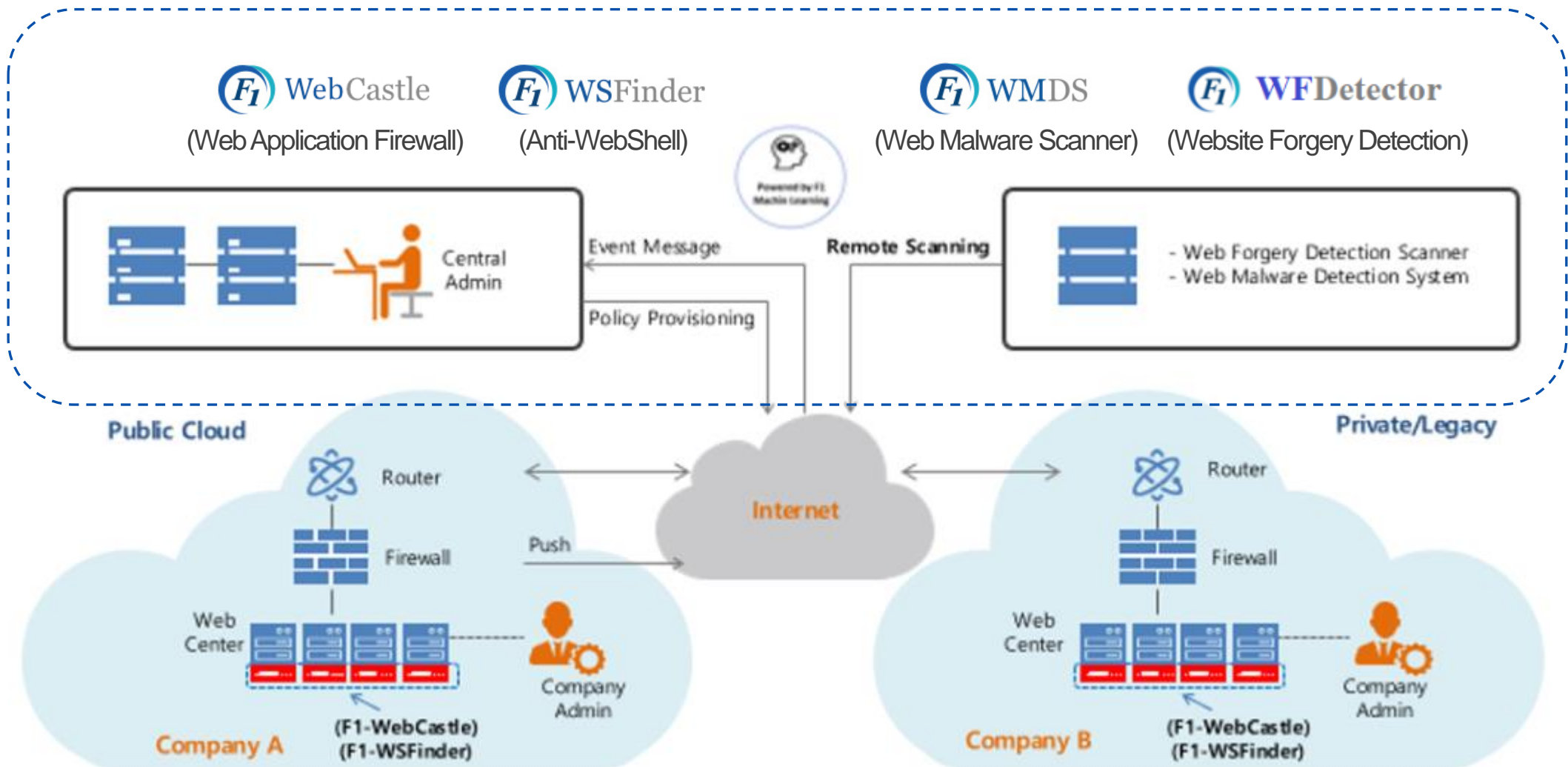
Description

Yearly 5,000 websites vulnerability checking Web security support business of SMB

The screenshot shows the KISA (Korea Internet & Security Agency) security service interface. The header includes the KISA logo and 'KISA 보호나라 & K+CERT'. The main content area is titled '보안서비스' (Security Service) and features a navigation menu with options like '웹 취약점 점검' (Web Vulnerability Check), '사이버대피소' (Cyber Shelter), 'PC 원격점검' (PC Remote Check), and 'DNS 싱크로' (DNS Sync). The main content area displays '웹 취약점 점검' (Web Vulnerability Check) with a '주의' (Warning) icon and a date '2017.03.10. 22:59'. Overlaid on the screenshot are three circular callouts: a dark blue circle labeled 'web vulnerability diagnosis', a blue circle labeled 'WHISTL web shell detection', and a light blue circle labeled 'Castle web firewall'.

IV. Features of Unified Web Security Service

Host-based Software + Cloud Central Management System + SECaaS



IV. Features of Unified Web Security Service

UWSS provides various values to customers as a differentiator

values	Differentiation factor	Similar products
Integration service	Provides a comprehensive web security solution that can be integrated and managed ※ Customized service according to customer choice	Purchase of individual products, Convenience is reduced by managing each individual product
Server construction cost reduction	Provides an integrated central management platform in the cloud ※ Customer Server Construction / Operation Cost Zero	Management server purchase and construction, operation cost is required
Immediate installation operation	Available immediately after downloading / installing Agent software	SECaaS (Proxy method) requires time to change / apply DNS
Monthly spending	Reasonable monthly subscription	Provided just on-premise configuration, Only some individual products are provided as monthly subscriptions
Operation management efficiency	Integrated operation management through a single management website ※ Contract / management of multiple products through a single window (work efficiency)	Provide individual product management system
User convenience	Increased security management convenience such as integrated dashboard and integrated report	Not provided, individual product dashboard / report
Disability Web access guarantee	No impact on customer web access due to platform or agent failure	SECaaS (Proxy method) also stops accessing customer websites in case of service infrastructure failure
Hacking Secure platform	Since the cloud platform does not bypass and store any web traffic, information leakage does not occur even if the platform is hacked.	SECaaS (Proxy method) analyzes / stores all web traffic bypass in the service infrastructure (possible), Traffic information can be leaked in case of infrastructure failure

Unified Web Security Service

F1-UWSS

V. Key Contents of Unified Web Security Service

V. Key Contents of Unified Web Security Service

Customers can select 3 service types according to environment and needs

		Basic	Pro	Premium
Target	Web server (quantity)	1	1	1
	Web domain (quantity)	1	1 ~ 4	1 ~ 10
Service Provided	WEBCastle (Web Application Firewall)	○	○	○
	WSFinder (Anti-WebShell)	n/a	○	○
	WFDetector (Web forgery detection)	○	○	○
	WMDS (Web Malware Distribution detection)	○ (Max 50 pages)	○ (Max 500 pages)	○ (Max 5,000 pages)
Technical Support	WebShell Analysis Support	n/a	n/a	○
	Web Malware Analysis Support	n/a	n/a	○
	Dedicated Technical Team Support	n/a	n/a	○
	Agent Installation Support	n/a	○	○
	Security Policy Setting Support	n/a	○	○
	Email Feedback	8 hours	4 hours	2 hours
	Phone Response	n/a	n/a	○

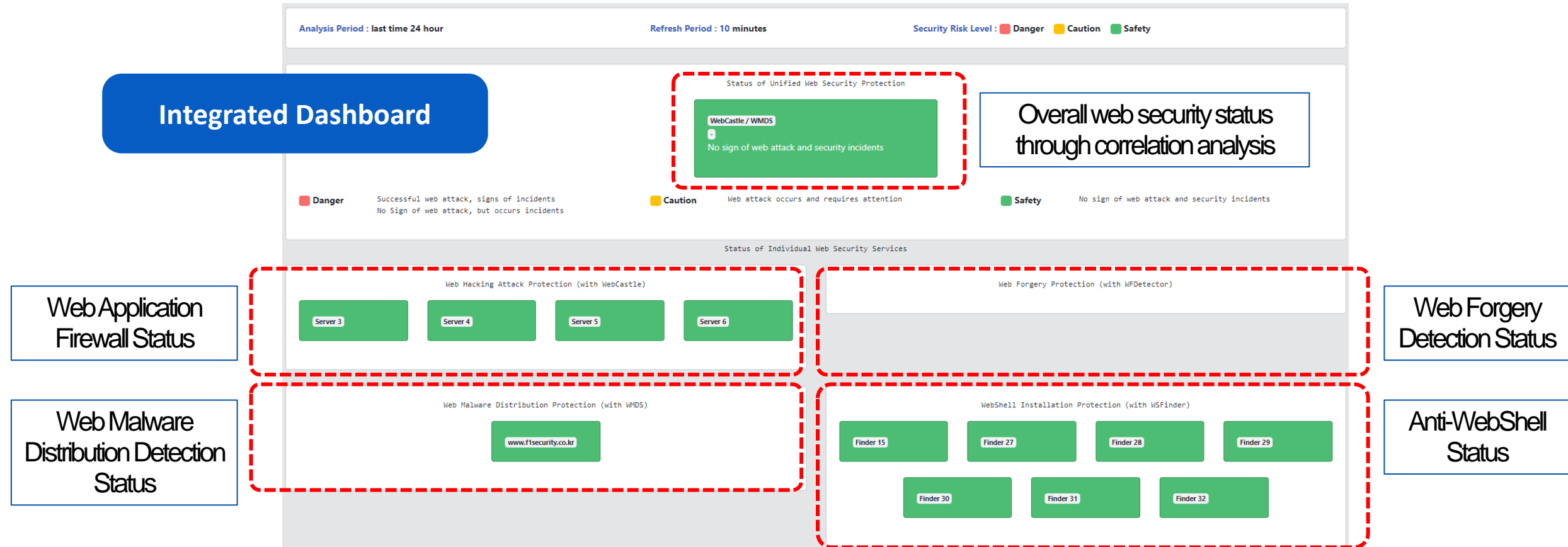
V. Key Contents of Unified Web Security Service

All-in-one web security service through cloud central management system

		Method	Main Contents
Web security service	Web Application Firewall	Software Agent	<ul style="list-style-type: none"> • OWASP Top 10 web application attack detection and blocking <ul style="list-style-type: none"> ※ Detection-only mode, blocking mode selectable • User-defined rules, handling IP / Domain exceptions, Parameter Block
	Anti-WebShell	Software Agent	<ul style="list-style-type: none"> • WebShell detection and quarantine (+3,500 detection patterns) <ul style="list-style-type: none"> ※ Regex, Hash, URL, SSDeep, obfuscation Algorithm • Real-time detection On / Off, manual inspection setting, white-list registration
	Detection of web malware distribution	Remote Scanning	<ul style="list-style-type: none"> • URL detection via malware and distribution sites (+175,500 detection patterns) • Periodic and manual inspection settings, Path Depth / Sub Page Link / Navigation Page settings
	Web page forgery detection	Software Agent, Remote Scanning	<ul style="list-style-type: none"> • Web forgery detection by agent or agent-less method <ul style="list-style-type: none"> ※ Supports precision detection using both methods
Central management system	Installation and setup	Cloud	<ul style="list-style-type: none"> • Agent download, registration, security policy setting and change
	Integration service		<ul style="list-style-type: none"> • Integrated dashboard and integrated report lookup
	Logging and notification		<ul style="list-style-type: none"> • Security event history logging and real-time email notifications such as detection, blocking, and quarantine
	my page		<ul style="list-style-type: none"> • Search, registration and change of user, service type, billing information, etc.

V. Key Contents of Unified Web Security Service

Provides an intuitive visualization of the overall web security status at a glance



V. Key Contents of Unified Web Security Service

Integrated reporting of service contract / usage status, security policy setting, detection and blocking history

F1-UWSS
Unified Web Security Service
Monthly Report

Confidentiality

Please select a year: Please select a month:

Username: 2020.02.01 ~ 2020.02.29

Integrated Report

Caution

This report is confidential with the user's asset information.
Please refer to the following notes for the report management.

1. never prohibits any outflows.
2. not reprinted or reprinted without permission.
3. forbidden to be viewed except by security officers and related personnel.

Contents

- 1. Overview 1
 - 1.1. General Information
 - 1.2. Service Contract Status
 - 1.3. Service System Status
 - 1.4. Web Security Status
 - 1.5. Web Security Configuration Status
- 2. Web Hacking Attack Detection & Blocking (WebCastle)
 - 2.1. Summary
 - 2.1.1. General Information
 - 2.1.2. WebCastle Status
 - 2.1.3. Total number of security events
 - 2.1.4. Web Server & WebCastle Status
 - 2.2. Monitoring Status
 - 2.2.1. Daily detection and blocking events by Total
 - 2.2.1.1. Daily detection (Total)
 - 2.2.1.2. Daily blocking (Total)
 - 2.2.2. Detection and blocking events per domain
 - 2.2.2.1. Total number per domain
 - 2.2.2.2. Top 10 events (Total)
- 3. WebShell Detection & Isolation (WS-Finder)
 - 3.1. Summary
 - 3.1.1. General Information
 - 3.1.2. WS-Finder Status
 - 3.1.3. Total number of security events
 - 3.1.4. Web Server & WS-Finder Status
 - 3.2. Monitoring Status
 - 3.2.1. Daily detection and isolation events by Total
 - 3.2.1.1. Daily detection (Total)
 - 3.2.2. Detection and isolation events per domain
 - 3.2.2.1. Total number per domain
 - 3.2.2.2. Top 10 events (Total)
 - 3.2.2.3. Top 10 events (Server 1)
 - 3.2.2.4. Top 10 events (Server 2)
 - 3.3. Management Status
 - 3.3.1. WebShell detection pattern
 - 3.3.1.1. Number of update
 - 3.3.1.2. Daily update
 - 3.3.1.3. Updated pattern description

2.2. Monitoring Status

2.2.1. Daily detection and blocking events by Total

2.2.1.1. Daily detection (Total)

2.2.1.2. Daily blocking (Total)

Confidential T: +82-70-4640-3031 gpartners@f1security.co.kr www.f1security.co.kr

Unified Web Security Service

F1-UWSS

VI. Reference

VI. Reference

F1Security's web security solution with many domestic usage records

6,600+ Web Application Firewall, **17,000+** Anti-WebShell
4,000,000+ Web Malware Distribution Detection



MSSP/CSP/ISP
(for end-customers)



Government
(for public service)



Enterprise
(for suppliers)



Thank you!

We can help make your website more secure

