

# WEBFRONT-K KS

Web Application and API Protection



# WEBFRONT-K

POILINK WEBFRONT-K has evolved into a web application and API protection (WAAP) from the legacy web application firewall.

As the use of APIs in application development has become a common way, attacks targeting API vulnerabilities are increasing. In addition, WAAP is essential because existing WAF alone cannot effectively protect sensitive information through your web applications and APIs.

WEBFRONT-K is a WAAP that responds to new web attacks by applying intelligent detection technology including user behavior-based detection, boasting the best performance on the in-house developed platform.



### Korea's best-performance WAF/ WAAP

Optimized Web/API Security Platform



### Convenient and improved management

GUI-based management console and web security log analysis/reports



### OWASP TOP 10 / API TOP 10 response

Various detection skills



### Latest protocols and SSL visibility

TLS 1.3, HTTP/2, hardware-based SSL offloading



### Automation of application operation

Full REST-API and ANSIBLE



### Save CAPEX

Expanding license-based performance without equipment change

## Applied core technology for API security

WAAP is an evolved web application firewall that performs WAF, DDoS protection, bot management, and API security.

API security is based on the security of web applications. Therefore, a certain level of API security is possible with functions like a response to attacks (e.g. Buffer overflow, Injection and XSS) on web applications, prevention of sensitive information leakage, a permission list, a block list, access log control and blocking credential stuffing.

However, in order to respond to OWASP vulnerabilities, which is the most important in application security, the following technologies must be equipped in WEBFRONT-K.

<p><b>Mutual TLS (mTLS)</b></p>	<p><b>Cloaking identification information</b></p> <p>GET/account [redacted] /My data</p>	<p><b>API token authentication and integrity test</b></p> <p>JWT 101 10110 10</p>
<p><b>Limiting the thresholds of each API and methods</b></p>	<p><b>JSON response cloaking</b></p>	<p><b>JSON request field test</b></p>

## Differentiated design for high-performance

We design and develop hardware and software for optimized web security.



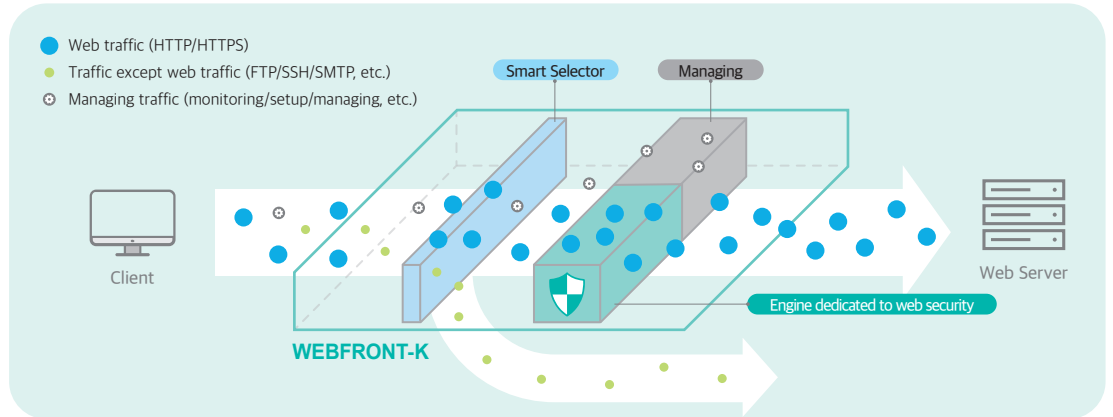
### Selective Traffic Processing

- ✓ Applying Smart Selector™, proprietary technology, to an equipment port
- ✓ Delivering web traffic (HTTP & HTTPS) selectively on 'dedicated web security engine'



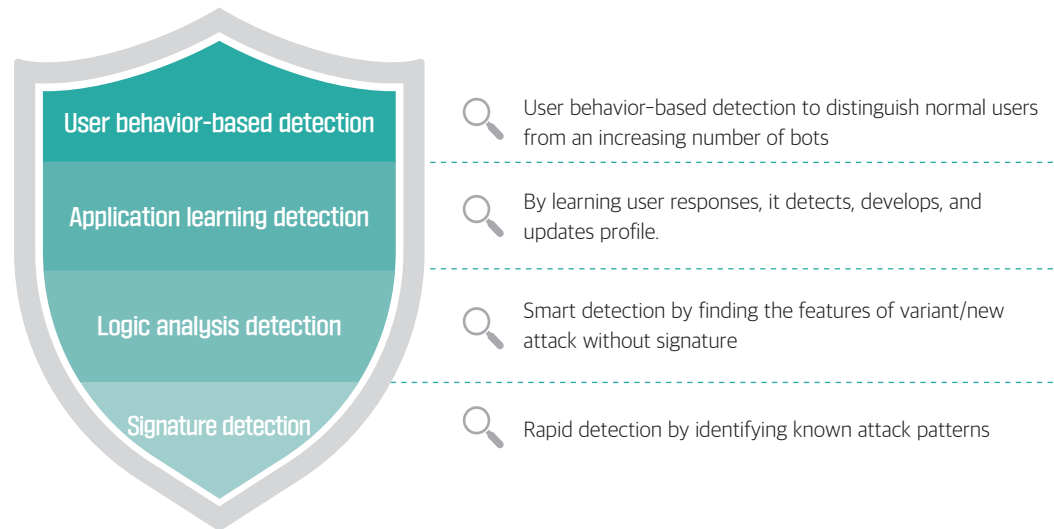
### Core load balancing packet process

- ✓ Performing a load balancing to avoid bottleneck of a certain CPU core when web traffic is detected
- ✓ Providing high-performance web security by effective CPU usage (patent registered)



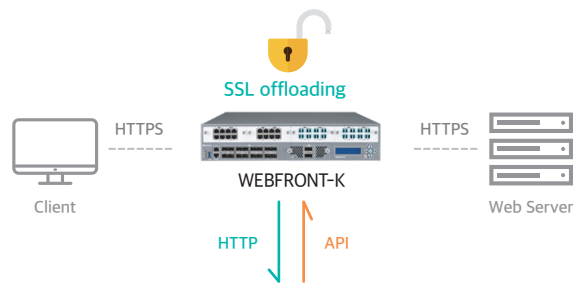
## Various detection technologies

Applying CAPTCHA and JavaScript action-based authentication to control improper bot activities

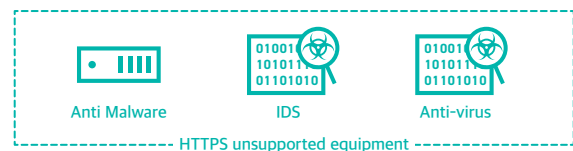


## SSL decryption mirroring

WEBFRONT-K delivers decrypted traffic to threat analysis equipment and blocks it if it's identified as abnormal traffic

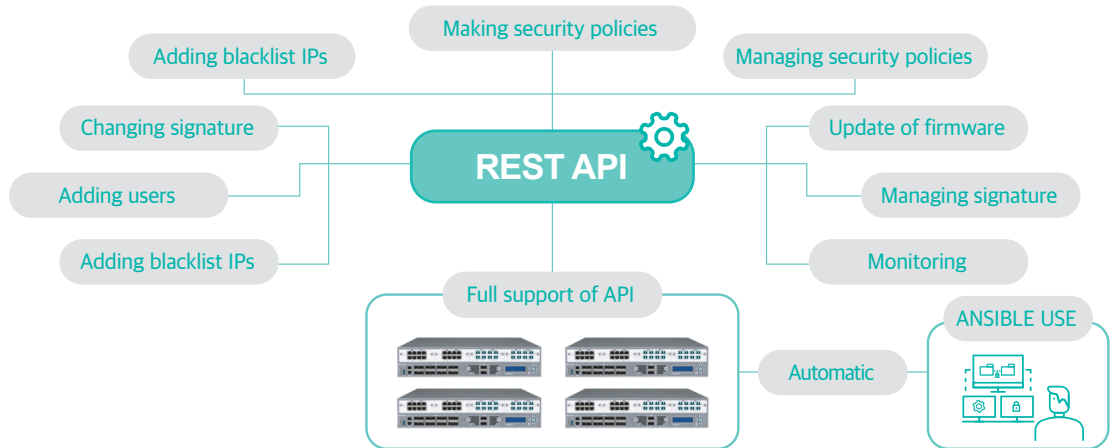


- ✓ Internet Content Adaptation Protocol (ICAP)
- ✓ SSL/TLS Decryption Mirroring
- ✓ API integration
- ✓ No need of separate SSL decryption equipment
- ✓ Latest TLS 1.3 and HTTP/2



## Supports Full REST API

Multiple WAF/WAAP can be easily managed and integrated. It provides various management function through REST API and supports ANSIBLE.



## Security analysis and statistics management

WEBFRONT Analyzer is an analysis solution which monitors multiple WEBFRONT-K from a remote site. Analyzer monitors the state of equipment by analyzing log data received from WEBFRONT-K. It informs attack events to users and makes various statistics reports.



## Managed Security Service and security consulting

(Optional, Domestic only)

PIOLINK Security Service offers systematic, professional services about vulnerability analysis, hacking simulation, new policies, equipment operation, etc. which are needed for the build-up of WAF/WAAP.



## Cloud web application WAF

# WEBFRONT-KS

WEBFRONT-KS is the cloud delivered web application and API protection(WAAP), expanding WAF capabilities to four core features: WAF, DDoS protection, bot management and API protection.

It has user behavior-based security detection technologies (same technology used in WEBFRONT-K, dedicated hardware) as well as the function of CAPTCHA and JavaScript action-based authentication to control improper bot activities.



User behavior-based detection



Load balancing



REST API & ANSIBLE



Security Operation Center



Easy installation

## Various Cloud environments



### Private Cloud

Supporting VMware, Xen, KVM, OpenStack, etc.



### Public Cloud

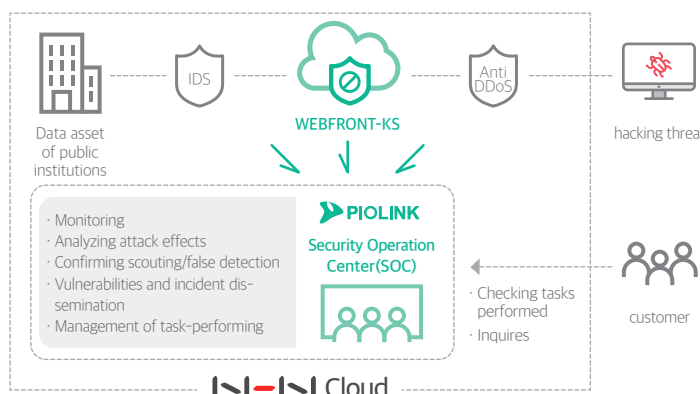
Supporting Amazon Web Service, NHN Cloud, MS Azure, etc.



### Cloud for public institutions

- Cloud for public institutions obtaining Cloud security certificate
- Providing Korea's first WAF and security operation services to Cloud for public institutions
- Outstanding WAAP operation and managed security services through excellent PIOLINK teams

## Cloud web security and SOC (Case of NHN Cloud)



### Managed Service





- Professional engineers with WAAP operation and offering security operation services
- Providing Cloud for public institutions




### Self Service

- Building and operating WAAP by users

# Specification

## WEBFRONT-K (Appliance WAAP)

WEBFRONT	K1800		K3200		K3200R		K4600	
								
Ethernet Ports (Total)	22		22		22		22	
· 40 GbE Fiber (QSFP+)	-		-		-		-	
· 10 GbE Fiber (SFP+)	2		2		2		2	
· 1 GbE Fiber (SFP)	8		8		8		8	
· 1 GbE Copper	12		12		12		12	
Bypass Ports · Type1 : 2 pairs Fiber · Type2 : 2 pairs Copper	Choose type 1 or 2		Module type (up to 4)		Module type (up to 4)		Module type (up to 4)	
Memory (RAM)	8 GB	16 GB	16 GB	32 GB	16 GB	32 GB	32 GB	64 GB
Storage Log (SSD)	480 GB	1 TB	1 TB	2 TB	1 TB	2 TB	1 TB	2 TB
Storage OS (SSD)	240 GB		240 GB		240 GB		240 GB	
CPU	1 x 2-core		1 x 4-core		1 x 6-core		1 x 12-core	
Power Consumption	88 W		98 W		117 W		115 W	
Power Input	100-240VAC, 50-60 Hz (universal voltage) / Dual Power (hot-swappable)							
Dimension (WxDxH)	428 x 458 x 44 mm		428 x 458 x 88 mm		428 x 458 x 88 mm		428 x 458 x 88 mm	
Weight	8.1 kg		9.3 kg		9.3 kg		9.3 kg	
Throughput License	1 Gbps, 2 Gbps		5 Gbps, 7 Gbps		5 Gbps, 7 Gbps		10 Gbps, 13 Gbps	
Concurrent Session	4,000,000		8,000,000		8,000,000		16,000,000	
CPS / TPS	50,000 / 100,000		140,000 / 210,000		140,000 / 210,000		270,000 / 450,000	

WEBFRONT	K5600		K5800		K8600	
						
Ethernet Ports (Total)	16 or 18 or 24		16 or 18 or 24		20	
· 40 GbE Fiber (QSFP+)	2 (optional)		2 (optional)		4	
· 10 GbE Fiber (SFP+)	16, 8 (optional)		16, 8 (optional)		16	
· 1 GbE Fiber (SFP)	-		-		-	
· 1 GbE Copper	8 (optional)		8 (optional)		-	
Bypass Ports · Type1 : 2 pairs Fiber · Type2 : 2 pairs Copper	Module type (up to 4)		Module type (up to 4)		Fixed type 1, Optional type 1 only	
Memory (RAM)	32 GB	64 GB	64 GB		128 GB	
Storage Log (SSD)	1 TB	2 TB	2 TB		2 TB	4 TB
Storage OS (SSD)	240 GB		240 GB		1 TB	2 TB
CPU	1 x 12-core		1 x 16-core		1 x 16-core	
Power Consumption	146 W		144 W		416.1 W	
Power Input	100-240VAC, 50-60 Hz (universal voltage) / Dual Power (hot-swappable)					
Dimension (WxDxH)	428 x 508 x 88 mm		428 x 508 x 88 mm		428 x 731 x 88 mm	
Weight	10.1 kg		10.1 kg		17.5 kg	
Throughput License	16 Gbps, 20 Gbps		25 Gbps, 40 Gbps		40 Gbps	
Concurrent Session	16,000,000		20,000,000		20,000,000	
CPS / TPS	400,000 / 900,000		400,000 / 1,000,000		400,000 / 1,400,000	

## WEBFRONT-KS (Software WAAP, Performance License)

WEBFRONT	KS100	KS500	KS1000	KS2000	KS6000
Throughput	100 Mbps	500 Mbps	1 Gbps	2 Gbps	6 Gbps

\* Up to KS2000 is provided in public cloud, and KS6000 is only provided in private cloud environment.

### Min. requirements for WEBFRONT-KS

CPU Core	2	4	8	16	16
Memory	4 GB	8 GB	16 GB	32 GB	32 GB
HDD	40 GB				
Hypervisor	QEMU/KVM, VMware, OpenStack, Xen				

## Key functions

Request check	<ul style="list-style-type: none"> <li>Whitelist and blacklist</li> <li>Requested user definition filter</li> <li>Access control</li> <li>URL regular expression</li> <li>Request URL cloaking</li> <li>Check evasion</li> <li>Buffer overflow</li> <li>Shellcode</li> <li>Request form check</li> <li>Cookie protection</li> <li>Web attack program</li> </ul>	<ul style="list-style-type: none"> <li>SQL injection</li> <li>Logical operation SQL injection</li> <li>Cross site scripting (XSS)</li> <li>Include injection</li> <li>Personal information inflow</li> <li>Download check</li> <li>Blocking banned words</li> <li>Upload check</li> <li>Smuggling</li> <li>Web application DoS</li> <li>Excessive request control</li> </ul>
Response check	<ul style="list-style-type: none"> <li>Responded user definition filter</li> <li>Error code cloaking</li> <li>Response URL cloaking</li> <li>Server data cloaking</li> <li>Code cloaking</li> </ul>	<ul style="list-style-type: none"> <li>Response type</li> <li>Personal information leakage (outflow)</li> <li>Directory listing</li> <li>Credential stuffing</li> <li>Web falsification prevention</li> </ul>
Learning	<ul style="list-style-type: none"> <li>Access control learning</li> <li>Form field learning</li> </ul>	<ul style="list-style-type: none"> <li>URL structure learning</li> </ul>
Cloaking	<ul style="list-style-type: none"> <li>URL encoding</li> <li>Improper error handling</li> </ul>	<ul style="list-style-type: none"> <li>Server data spy</li> </ul>
Response	<ul style="list-style-type: none"> <li>CAPTCHA</li> <li>JavaScript authentication</li> </ul>	<ul style="list-style-type: none"> <li>User definition page [by attack/ by application/ user definition]</li> </ul>

## Additional functions

Traffic load balancing	<ul style="list-style-type: none"> <li>Traffic load balancing on the multiple web servers that operate the same web applications</li> <li>Reducing investment costs with no need of separate load balancer (ADC, L4/L7 Switch) installation</li> </ul>
Caching	<ul style="list-style-type: none"> <li>Storing the content often requested by users instead of a server by designating it</li> <li>As responding on behalf of a server, reducing traffic directly sent to the server and able to provide services faster</li> </ul>
Compression	<ul style="list-style-type: none"> <li>Sending important content files including images to users after compressing them</li> </ul>
QoS	<ul style="list-style-type: none"> <li>Setting the threshold for usage-request traffic bandwidth to prevent excessive traffic towards a server</li> <li>Blocking DDoS, protecting servers and maintaining the effective networks</li> </ul>



PIOLINK is specialized in network and security.

We ensure the industry's best application availability and performance and own unrivaled technologies and leadership in this intelligent, advanced IT environment by offering the build-up of Cloud infrastructure, the easy management of networks and data protection.

Our flagship products are Application Delivery Controller (ADC) having Korea's No.1 market share, Web Application Firewall (WAF/WAAP), Cloud Managed Networking and Hyper Converged Infrastructure and services, Managed Security Service (MSS or MSSProvider) and Security Consulting.



[www.PIOLINK.com](http://www.PIOLINK.com)

- 
- The content of this document is subject to change to improve on the performance and functions of a product, correcting print errors, etc.
  - The image described here can be different from that of a real product.
  - The name of a company, a product and a service specified here is the trademark or service label of the company.
  - A product can be purchased from official partners and checked with the company's Sales Department or on its Website.