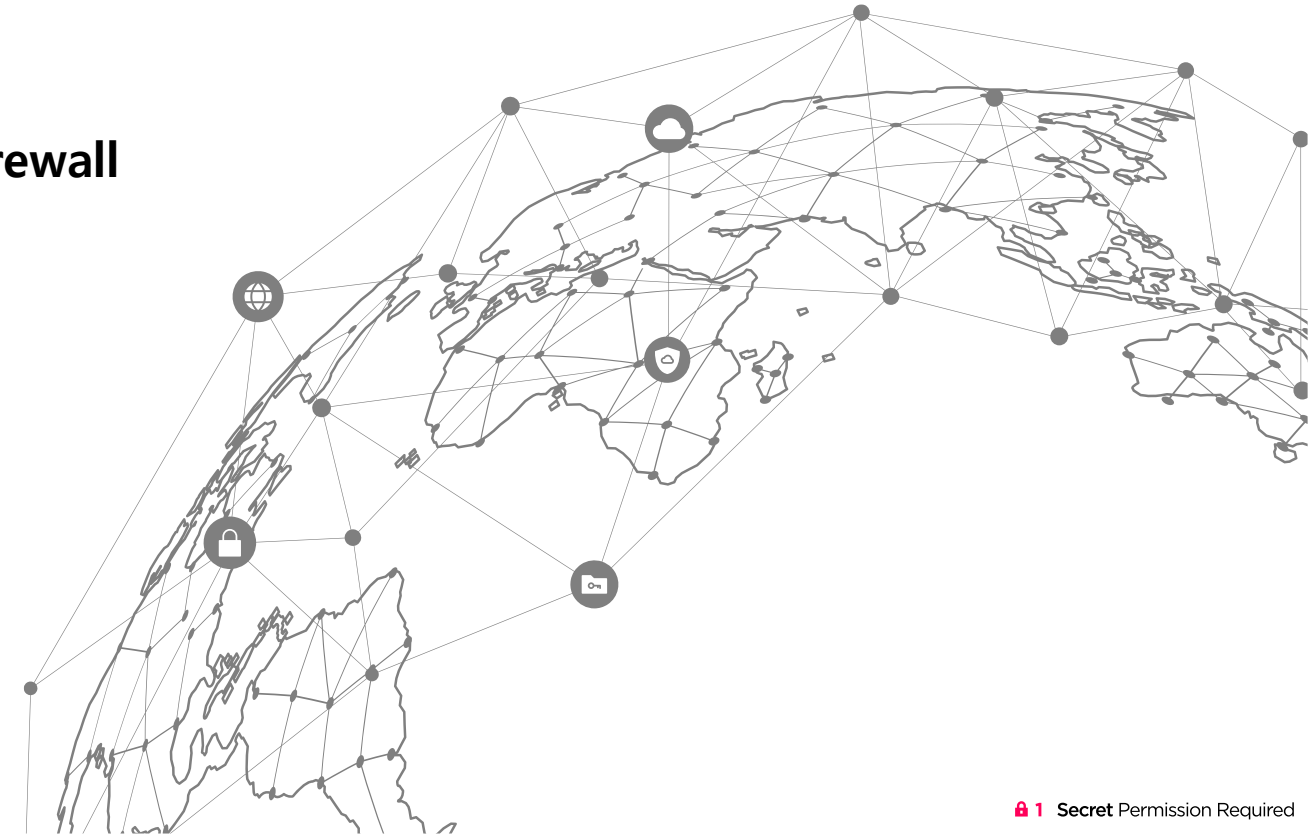
Penta SECURITY

WAPPLES

Intelligent and Comprehensive Web Application Firewall

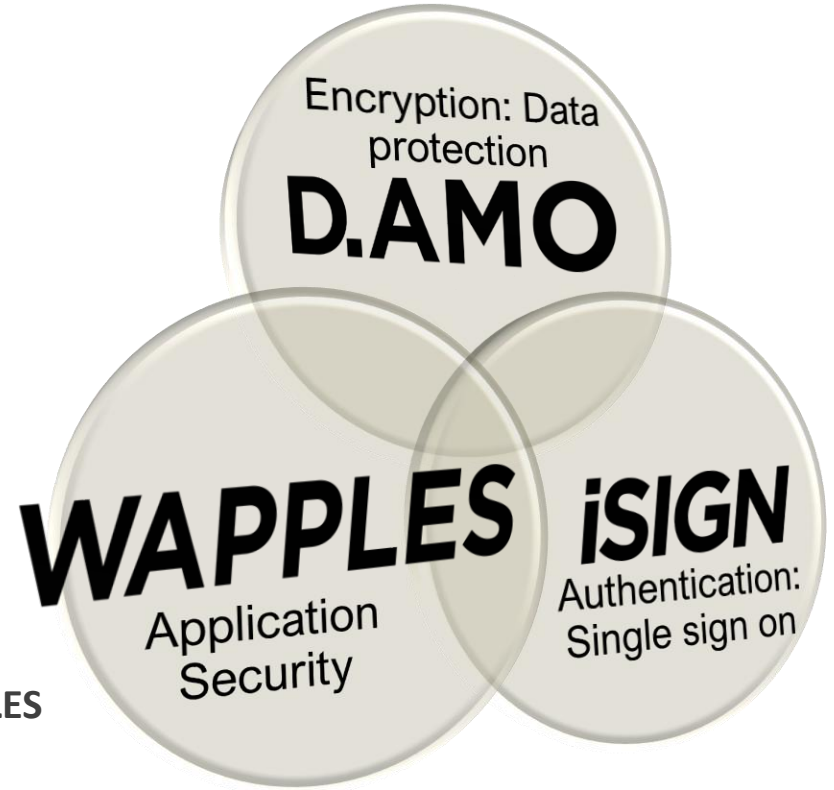


2025

Global Business

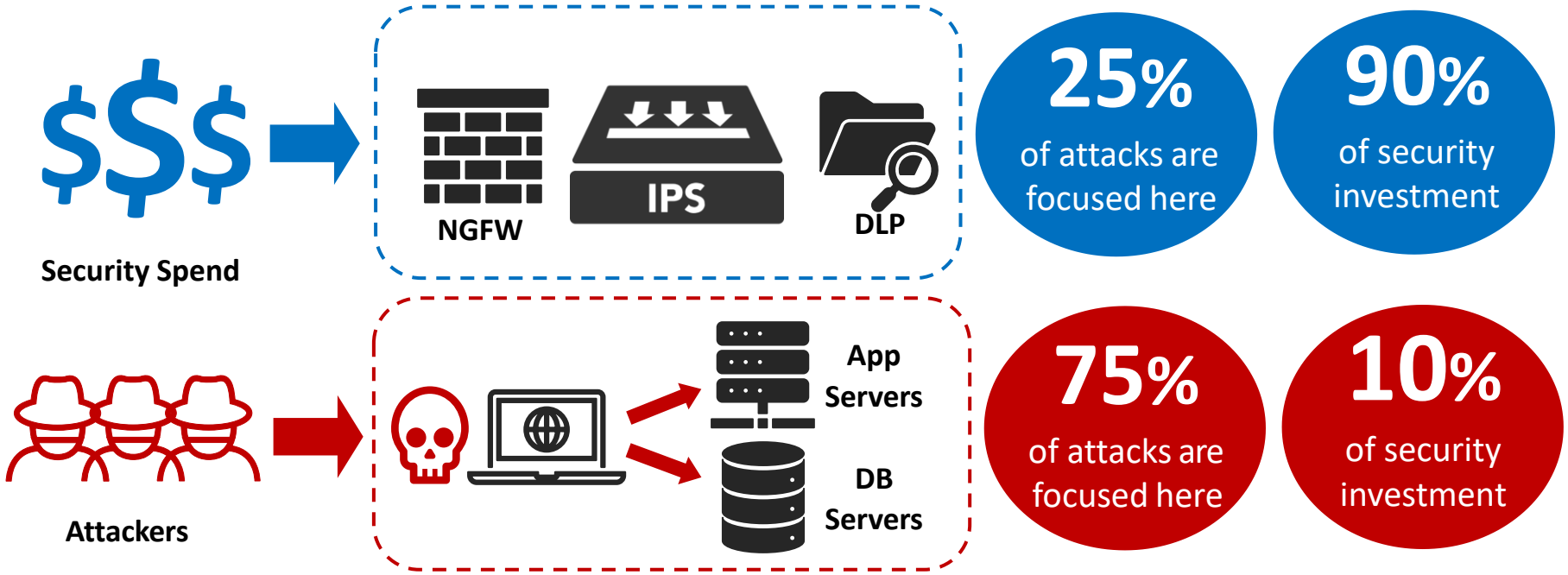
Company overview

Company	**PENTA SECURITY INC.**
Founded	July 1997
Founder / CEO	Seokwoo Lee / Tae Gyun Kim
Staff	250 employees (150 in R&D and tech support)
Headquarters	Seoul, Republic of Korea
Overseas Branch	Japan(Tokyo), Singapore, Vietnam(Hanoi)
Products	Data Encryption Platform **D'Amo**
	The Logical Web Application and API Protection (WAAP) **WAPPLES**
	Secure Identity and Access Management **iSIGN+**
	Cloud Security Platform **Cloudbric**



Security shadow

NGFW, IPS/IDS, and DLP are the most considered cybersecurity solutions for enterprises.
However, they cannot deal with layer 7 attacks in which **75%** of attacks are focused.



Web vulnerability

No.1

Hacking action vector leading to a data breach in 2018[1]

42% of

All websites have at least one severe vulnerability[2]

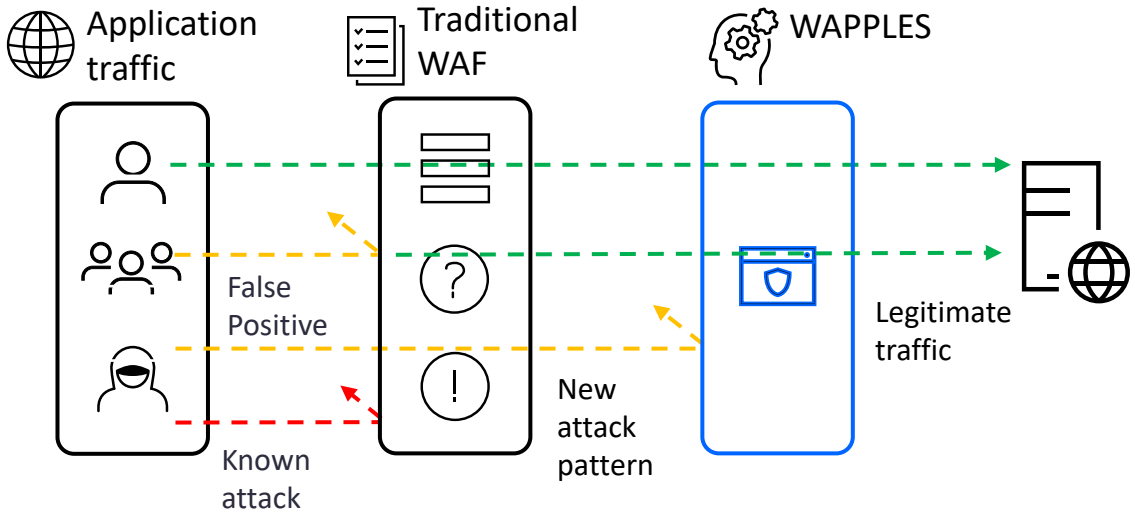
Web applications are the front end of most businesses and easily accessible without a special connection. Once breached, not only the company's resources but thousands and millions of users.

For hackers, web applications are therefore an easy and profitable target.

Traditional signature-based web application firewalls (WAFs) are designed to combat known threats; they cannot detect zero-day attacks that exploit modified or unknown attack patterns.

Sources: 1. Verizon “2019 Data Breach Investigations Report”, 2. Acunetix “Web Application Vulnerability Report 2017”

Intelligent COCEP detection engine



Logic-based Detection Engine: COCEP™

- COCEP™ uses a set 40 pre-defined rules
- Request & Response **code parsing**,

  not **'Pattern-Matching'**
- Guarantee higher accuracy & lower false rate
- Protect from zero-day attack, including OWASP Top 10
- With virtual patching, it fixes vulnerabilities without delay

URL Recognition	• Analyze the HTTP Construction • Analyze whether the request is to the protected webservers or not
Protocol Validation and Data Splitting	• Check whether the request is standard HTTP or not • Split the incoming HTTP data
In-depth Web Traffic Analysis	• Send the split data to the parser of each rule • Performs in-depth analysis according to the detection location of each rule
Countermeasures	• Responds countermeasure against attacks ✓ Detection only ✓ Page Redirection ✓ Error Code Return ✓ Disconnection
Logging	• Records the Detection Log in DB

3rd Party evaluation – Penetration test

Test scope

A penetration test by WizlynxGroup revealed that all 1,739 known malicious payloads such as SQL Injections, Cross-Site Scripting, and more were 100% detected and blocked by WAPPLES' COCEP engine.

Vulnerability Type	Blocked Payloads	Block Rate
SQL Injection	599 / 599	**100 %**
Cross-Site Scripting (XSS)	600 / 600	**100 %**
Path Traversal	20 / 20	**100 %**
OS Command Injection	519 / 519	**100 %**

"The only vulnerabilities left unpatched are vulnerabilities that, for their nature, can be hardly detected by a WAF"

wizlynx group

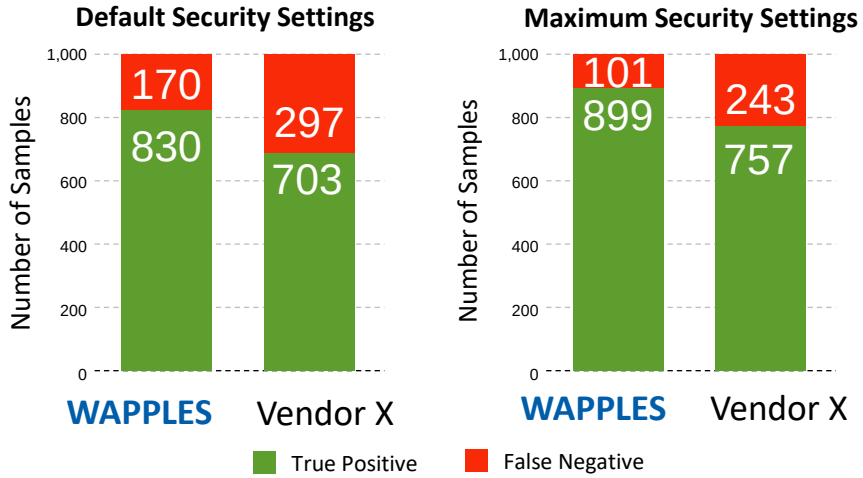
wizlynx group is one of the few globally accredited CREST Penetration Testing service providers, employing CREST registered Penetration Testers. This highly recognized certification is proof to customers that wizlynx maintains the highest quality of technical capabilities, policies, processes, and procedures.

3rd Party evaluation – Competing WAF

Test scope

Tests by Tolly using 1,000 attack samples showed that Penta Security provided more effectiveness both at default and maximum settings, delivering higher performance and greater functionality than Vendor X.

WAF Effectiveness with Default and Maximum-Security Policies



Note: WAPPLES used PCI/DSS policy for Maximum security configuration. Vendor X Maximum security consisted of enabling all signatures on the system. Green denotes that no data was compromised by the WAF, while red denotes that the attack was successful.

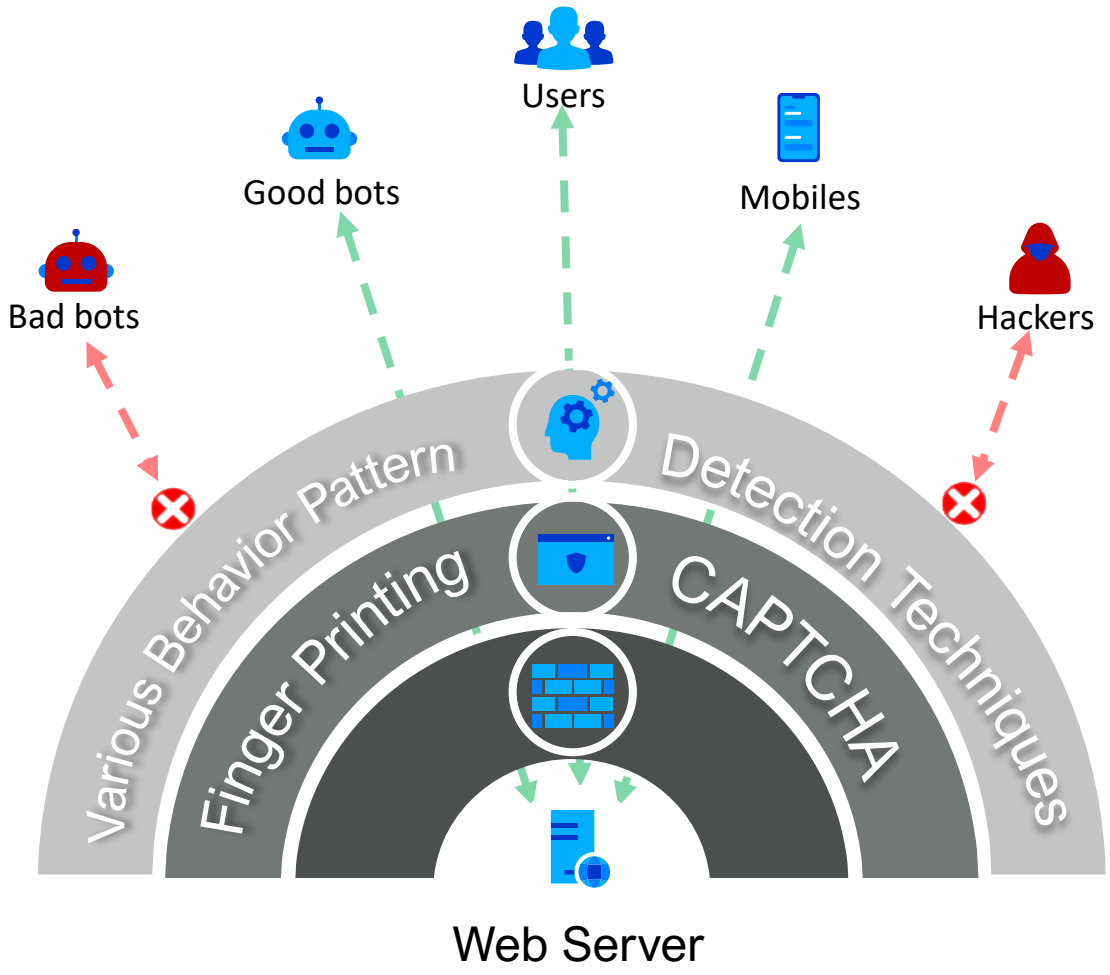
WAF Effectiveness – False Positive Rate.

Vender	Product Configuration	
	Default	Max. Security
WAPPLES	0%	4%
Vendor X	24%	29%

Note: Collection of 100 valid traffic items used for testing. Delivered via same mechanism as detection tests.

The Tolly Group is positioned to certify vendor solutions and thereby provide evidence that their products meet or exceed marketing claims. This proof-of-performance and/or features/functions lets customers know they can buy with confidence. Furthermore, custom testing enables vendors to verify a specific feature or function or commission a comprehensive evaluation.

Bot & APIs protection



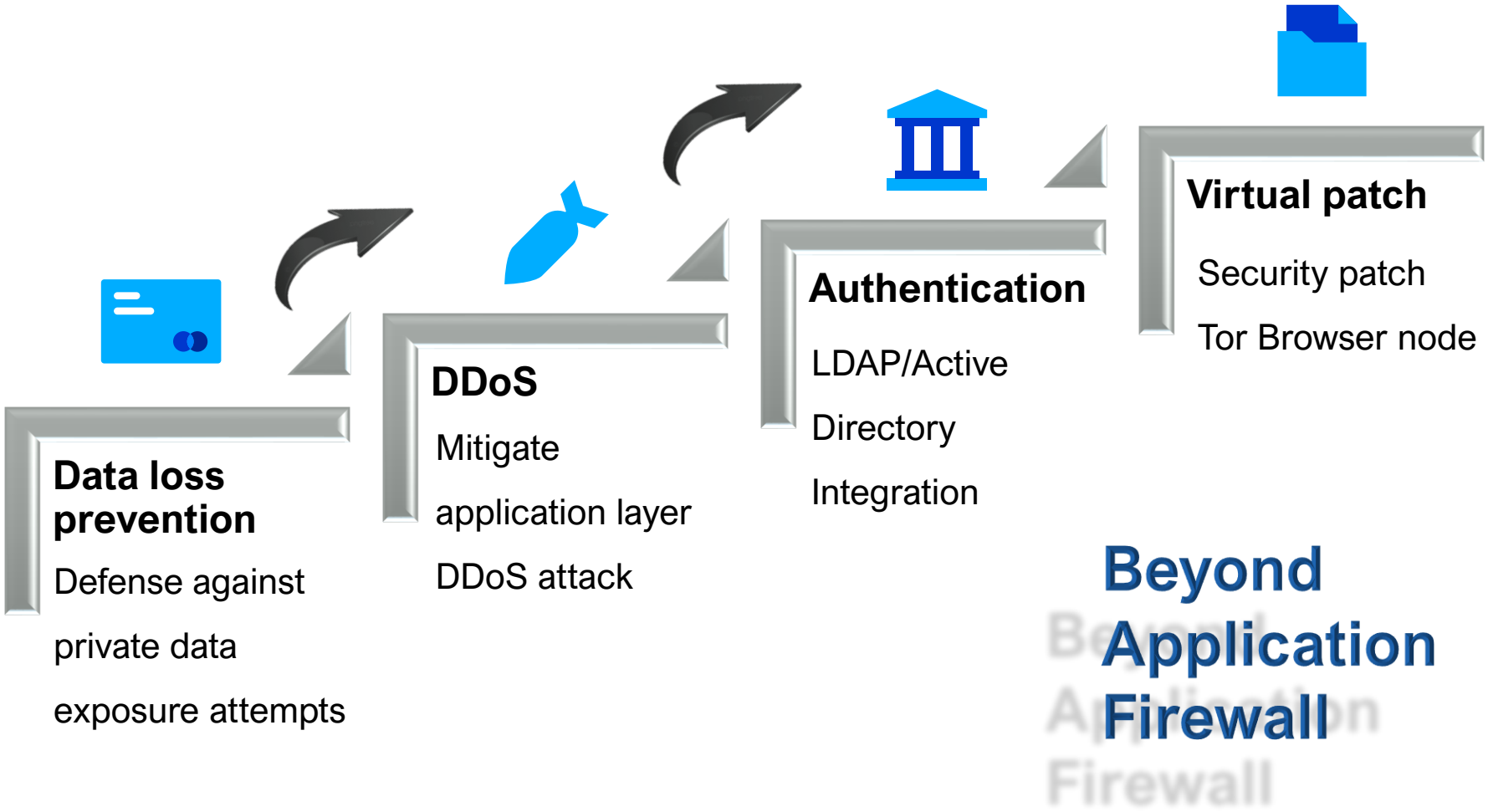
Bot Protection

- Blocking suspicious and bad bot access
- Protect bots using fingerprinting and CAPTCHA
- Plus, various behavior pattern detection abilities

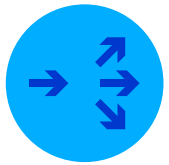
APIs & Mobiles Protection

- Mitigate threats coming through APIs
- With a dedicated API parser from COCEP engine
- Protect from XML/Jason/YAML attacks.

Enhanced security



A Comprehensive WAF



Application Delivery

Application load balancing

Web socket protection / Sticky session

Easy to Deploy and Manage

Pre-defined security rule sets

Self-diagnostics features

SSL

SSL key encryption

SSL accelerator / SSL offloading

Rich Graphical Reporting

Intuitive web console UI

Comprehensive visualized logs and reporting

High Performance

A near-zero false positive rate

Excel in both security and performance

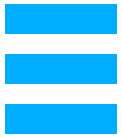
Affordable Pricing

Reasonable pricing policy with higher specification of product

Adaptable to all environments

Appliances

- 6 HW Models
- 300 Mbps to 10 Gbps
- Support for 10GE



VMs

- 4 VM Models
- 100 Mbps to 1 Gbps
- VMware, Hyper-V, Xen server, KVM

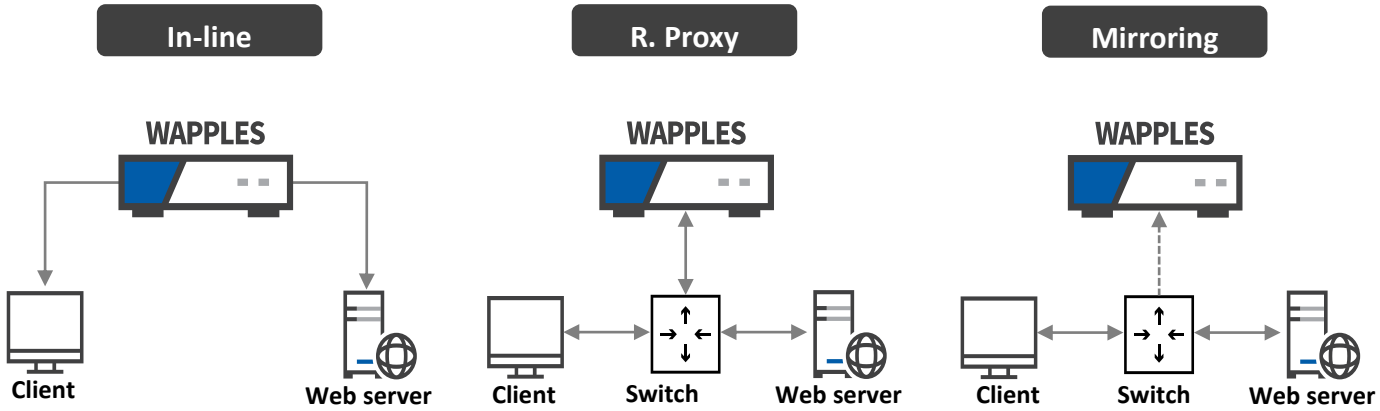
Public Cloud

- 4 VM Models
- BYOL and On-demand
- AWS, Azure, Google, Alibaba Cloud

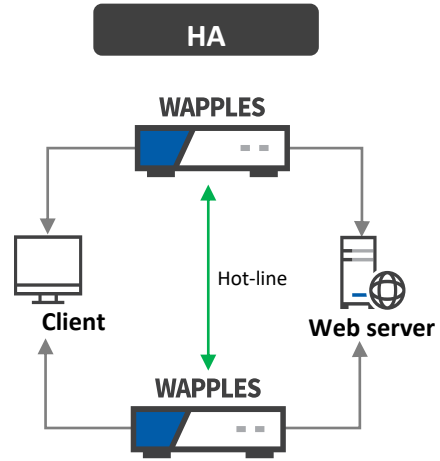
SaaS

- Subscription Based
- Traffic and no. of domains based

Deployment Option & HA Configuration



- Supports Inline, R- Proxy and Mirroring modes deployed without modifying the existing network environment



- A cluster of two WAPPLES devices can be configured in Active-Active/ Active-Standby
- High Availability provides synchronization of security policies and logs between devices

Product specifications

WAPPLES Appliance

Class	Value	Performance			High-end	
Model	W-160	W-1600	W-2600	W-4600	W-5600	W-12000
Throughput	300Mbps	1Gbps	2Gbps	4Gbps	6Gbps	10Gbps
RAM	8GB	16GB	32GB	48GB	96GB	192GB
Form Factor	1U	1U	2U	2U	2U	2U
Default NIC bypass port	CU	CU	CU or Fiber	CU or Fiber	CU or Fiber	CU or Fiber

WAPPLES SA

Class	Value	Performance		High-end	
Model	SA-50	SA-100	SA-500	SA-1000	SA-5000
Throughput	300Mbps	1Gbps	4Gbps	6Gbps	10Gbps
RAM	4GB	8GB	16GB	32GB	64GB

*Supported Hypervisors: Vmware, Hyper-V, Xen Server, Linux KVM
*Cloud support: AWS, Microsoft Azure, Google Cloud, Alibaba Cloud

Penta SECURITY

TRUST FOR OPEN SOCIETY

KOREA www.pentasecurity.co.kr

GLOBAL www.pentasecurity.com

JAPAN www.pentasecurity.co.jp

Cyber Security Awards Application Security 2020

IoT-based Smart Security Innovation Award 2020

Mwmber of the International Transport Forum CPB (~ 2020)

TU-Automotive Awards Best Auto Cybersecurity Product/Service 2019

Cybersecurity Excellence Awards Winner 2018

Hot Company in Web Application Security for 2016

SC Magazine Europe Best SME Solution

ICSA Labs Certified WAF

The First and Only CCEAL4 Certified WAF

PCI-DSS Compliance

Listed in Gartner®, 2023 Market Guide for Cloud Web Application and API Protection