Over 1,700 customers
27 years of providing integrated cybersecurity

Cloud X WAF

Proactive Cloud Web Application Firewall for Advanced Threat Defense

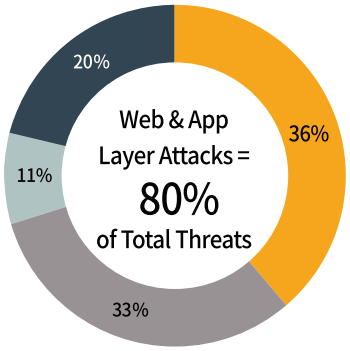
- Reduced False Positives and Processing Time
- TLS/SSL Protocol Compatibility
- Personal Data Leakage Prevention
- Detailed Rule-based Policies
- Anti Web DDoS/DoS Protection
- Automatic Self-Diagnosis

SOOSAN INT

As web services grow, so do the threats targeting them. Conventional network security solutions – such as IPS, IDS and Firewalls – often fail to detect exploits targeting vulnerabilities in the web applications that power modern web services, thereby creating opportunities for malicious actors

「Rising Security Threats on Web Applications & Cloud」

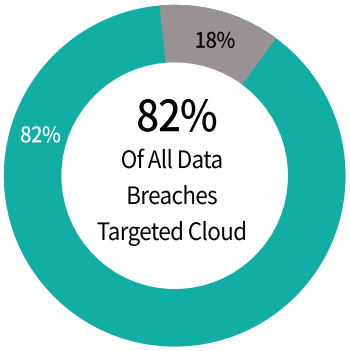
Cyberattack Trends by Type



- App vulnerability attacks
- Web-based attacks
- Scanning attacks
- Others

Source : Asec, Cyberattack Trend Data, 2023

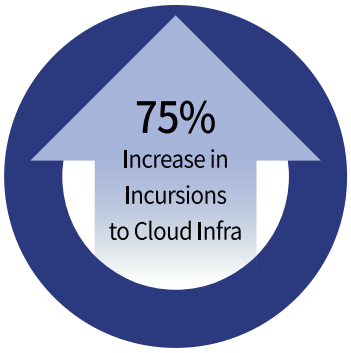
Cloud Threat Reports ①



- Cloud data breaches
- Others

Source : IBM Data Breach Report, 2023

Cloud Threat Reports ②



“ Cloud Under Siege ”

Source : CrowdStrike Global Threat Report, 2023

eCloudx WAF defends against the increasing attacks on cloud environments and protects the servers by analyzing the unique characteristics of each web application and traffic pattern.

Solution Overview

eCloudX WAF is a cloud-based Web Application Firewall. Our own Real-Time White URL technology drastically reduced false positives and processing time. It enables a safe and uninterrupted web service operation by proactive protection against malicious attacks and establishment of secure network environment.

Score-based threat analysis
Web Attack Filtering

White URL Real-time
Web Attack Protection

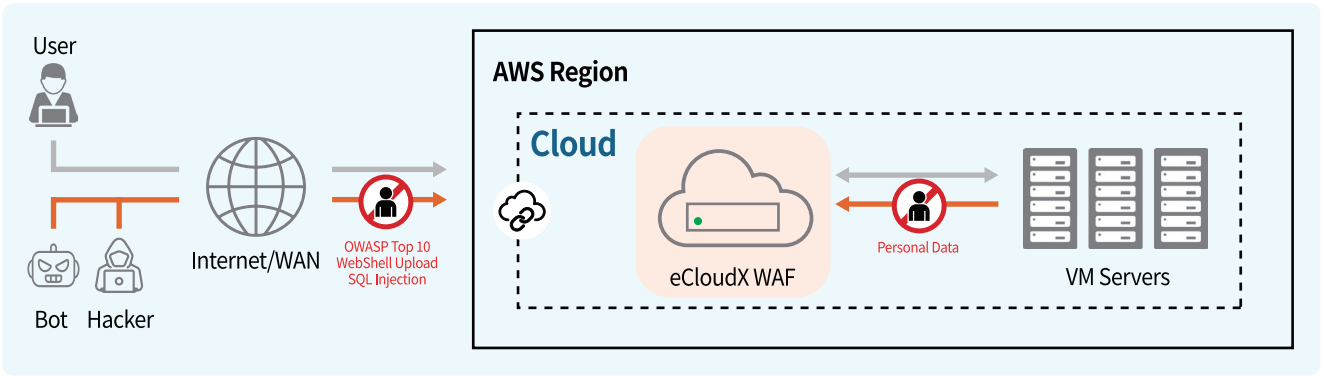
Supports URL-based
Policy & Exception Setting

TCP Session Transparency
Up-to-date Vulnerability DB

Customizable &
Automated Report Generation

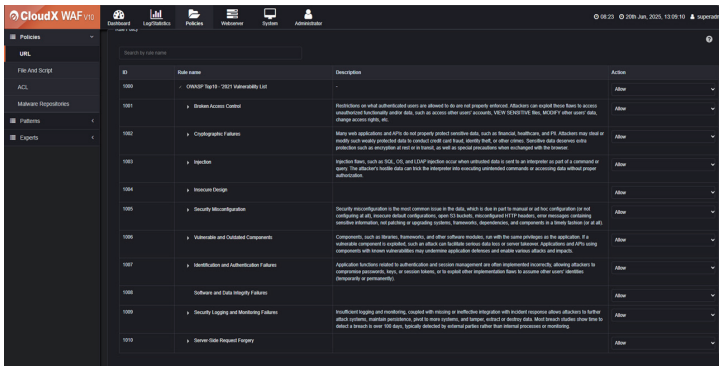
3rd Party Network Devices
High Compatibility

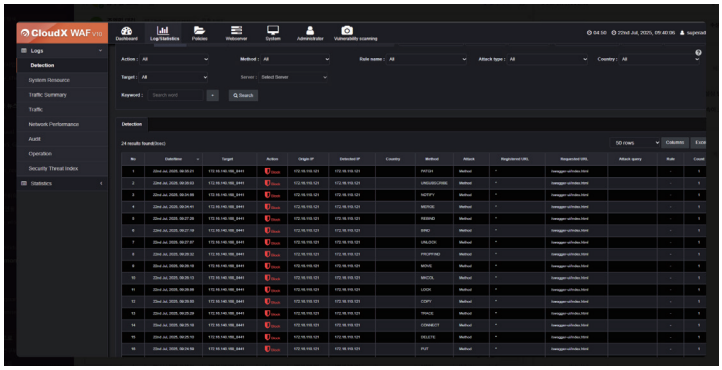
Solution Deployment



- Supports the latest Linux kernel and OpenSSL for maximum stability and security
- Performs web traffic monitoring and TLS/SSL decryption/re-encryption
- Server health check and load balancing support
- Supports cost-efficient operation through auto scaling
- Ensures continuous web service in case of fail-over through HA(Active-Standby) and Bypass
- CDN integration support

Solution Highlights





Web-based Threat Protection

- A range of threat detection algorithms including pattern and threshold
- OWASP Top 10 Vulnerabilities protection
- Latest Anti-web DDoS/DoS attack protection

Protection Without Downtime

- Real-time White URL technology reduces false-positives and processing time
- Quick response to threats during pattern learning period
- Provides alerts for SSL certificate expiration before validity ends

Automated Tools & Bot Control

- Automated web scraping prevention
- Malicious bot prevention
- Offers CAPTCHA authentication functionality

Dashboard and Monitoring

- Live visualization of web attacks
- Real-time system diagnostics and web traffic monitoring

Detailed Rule-based Policies

- Role-based admin access control
- Website URL, parameter, IP protection
- Malicious file upload/download prevention
- Personal data leakage prevention

Built for Integration

- Offers REST API
- Supports SIEM, SOAR integration
- Provides TLS/SSL visibility to 3rd party solutions

Cloud X WAF

We Secure your network with our 27 years of experience recognized by more than 1,700 customers

Solution Specification

Scalable Options for Your Traffic Needs

AMI Type Cloud Solution

eCloudX WAF	AWS instance type	Throuhput	vCPU	Memory	Storage	NIC
AWS AMI	t3.large	100Mbps	2 Core	8 GB	40 GB	2 nic
	t3.xlarge	200Mbps	4 Core	16 GB	40 GB	2 nic
	t3.2xlarge	500Mbps	8 Core	32 Gb	40 GB	2 nic

* For license inquiries, please contact gcbt@soosan.co.kr

SOOSAN INT

SOOSAN INT Co., Ltd. | +82 02-541-0843 | gcbt@soosan.co.kr
SOOSAN Bldg., 13, Bamgogae-ro 5-gil Gangnam-gu, Seoul, Republic of Korea | https://www.soosanint.com