

Security

WAF(Web Application Firewall)



**웹 취약점과 공격으로부터
웹 애플리케이션을
보호하는 서비스**

WAF는 웹 사이트의 트래픽을 모니터링하여
웹 애플리케이션을 안전하게 보호하는 서비스입니다.
웹 사이트의 취약점을 노리는 HTTP, HTTPS 기반
보안 위협을 신속하게 탐지하고 분석합니다.



강력한 탐지/차단

고객이 등록한 웹페이지의 HTTP, HTTPS 트래픽을 모니터링하여, 해커의 공격 시도를 실시간으로 탐지합니다. SQL Injection, Cross-Site Scripting(XSS), Web Scan 등 공격을 분류하고, 웹 보안에 필요한 다양한 방어기능을 제공하여 신종 웹 공격 유형에 즉각적으로 대처합니다.



안정적인 웹 서비스 운영 지원

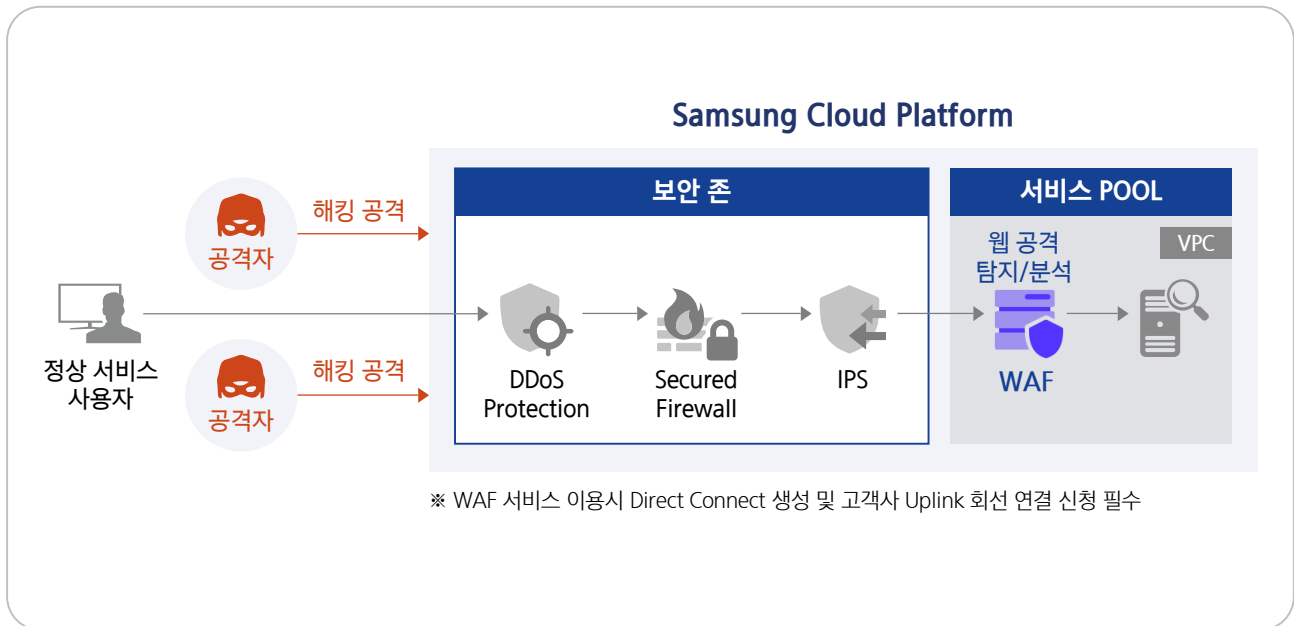
방화벽 시그니처 패턴 및 펌웨어 업데이트를 통해 신규 보안 위협에 대응합니다. OWASP(Open Web Application Security Project) 상위 10대 공격, 국정원 8대 취약점 공격, Zero-Day 공격 등 신종 웹 위협과 Bad Bot 등 해커의 공격 시도를 탐지하여 효율적이고 안정적인 웹 서비스를 운영할 수 있도록 지원합니다.



편리한 보안 관리

고객사가 직관적인 GUI를 통해 보안 정책을 직접 설정·운영할 수 있으며, 정책 구성이 어렵거나 추가 지원이 필요한 경우 전문인력이 지원합니다.

서비스 구성도



주요 기능

- 침입 탐지/분석 정보 제공
 - 웹 방화벽 이벤트를 통한 공격 분류(Injection, XSS, File Include, File Up/Download, Web Scan 등)
 - 최신 공격 패턴 탐지(Apache Struts 취약점 등)
- 침입 대응
 - 등록된 URL 대상 공격 시도 IP 정보 제공

SAMSUNG SDS

 www.samsungsds.com / cloud.samsungsds.com
 contact.sds@samsung.com / scp_sales@samsung.com
 youtube.com/samsungsds

