

WAF as a Service & 보안관제서비스 Web Shield



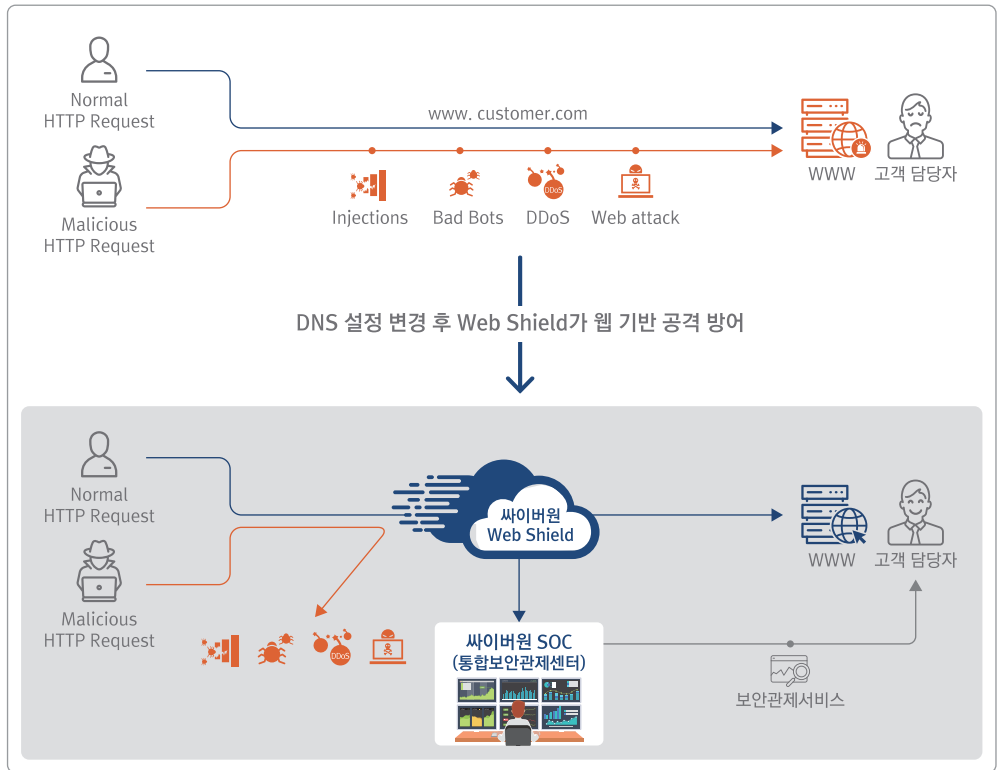
필요성

웹 공격으로부터 웹 서비스를 안전하게 보호할 수 있는 보안 전략

- ☑ 지능화되고 있는 웹 공격 방어를 위한 기술적 보안조치 필요
- ☑ 웹 공격에 대한 가시성 확보 및 신속한 대응체계 마련 요구
- ☑ 웹 서비스 보호를 위한 자체적인 보안 운영 및 관리, 비용 부담 증가

서비스 개념

스타트업 및 중소기업이 웹 공격으로부터 웹 보호 체계를 갖출 수 있도록 지원하는 클라우드 기반의 SECaaS형 WAF 보안관제서비스



사이버원 Web Shield 주요 기능 (WAF)

웹 공격 방어	DDoS 공격 방어	웹 통신 암호화
<ul style="list-style-type: none"> · OWASP 10대 취약점 방어 · 웹을 통한 정보 유출, 부정접근 방지 · 웹 사이트 위 · 변조 방지 	<ul style="list-style-type: none"> · 서버 자원 고갈 공격 방어 · 애플리케이션 공격 방어 · 멀티백터 공격 방어 	<ul style="list-style-type: none"> · SSL(Secure Socket Layer)제공 · 인증서 발급, 적용, 갱신 자동화 · 브라우저와 웹서버간 통신 보호

주요 특징



WAF as a Service

- 구축 및 운영 관리 불필요
- 사용 트래픽만큼 비용 지불
- 유지 보수 비용 부담 없음



Managed Security Service

- 숙련된 보안 전문가 집단
- 체계적인 보안관제 및 대응
- 실시간 원격관제 서비스

주요 서비스



24 x 365 실시간
웹 사이트 위협 모니터링



웹 사이트 침해 위협
이벤트 알림(e-Mail 및 SMS)



보안관제
월 정기 보고서



최신 공격 및 긴급 취약점
대응 패턴 업데이트



전용 모니터링 대시보드 제공
(종합 위협현황, 웹트래픽, 방문자 수)



최신 보안이슈 및
보안정보 제공

기대 효과



안전한 웹 사이트

웹 공격 방어를 위한 기술적 보안 수단 마련



보안 운영 및 관리 강화

상시 모니터링 및 대응체계 수립



기업 가치 보호

웹 공격으로 인한 경제적 손실과
대외 이미지 실추 방지



비용 부담 해소

총소요 비용 절감 측면의
경제적 보안관리