Site Shield

웹 인프라를 숨기고 취약점을 감소시켜 오리진 보안을 강화하는 솔루션!

Akamai
Intelligent Security Starts at the Edge

온라인 혁신이 빠르게 진행되고 접속 성능이 크게 개선되면서 웹사이트와 클라우드 기반 애플리케이션에 대한 공격의 규모, 강도, 종류 역시 급증하고 있습니다. Site Shield는 클라우드 기반 보안을 강화할 수 있는 추가적인 방어 레이어입니다.

웹사이트와 애플리케이션을 보호하려면 클라우드 상에서 공격을 차단해야 하고 공격자가 애플리케이션 인프라에 직접 접근할 수 없도록 막아야 합니다.

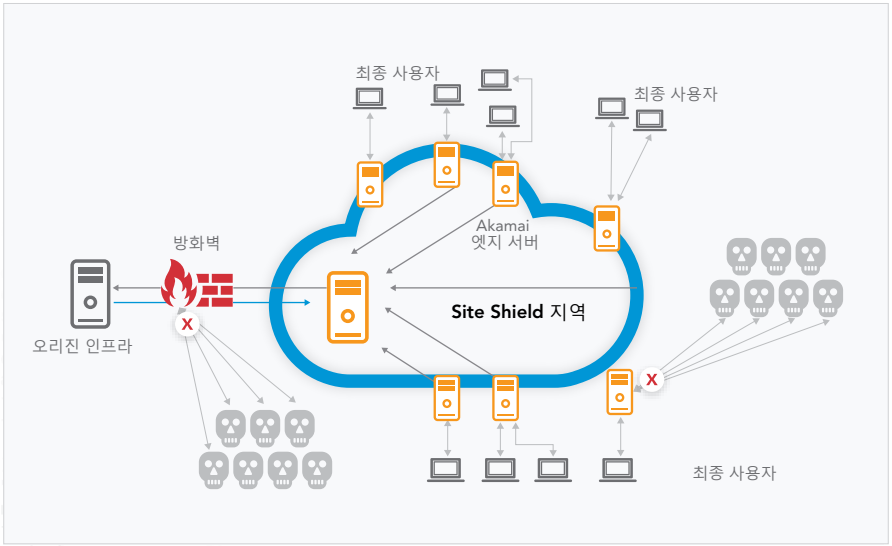
기능

Site Shield는 공격자가 클라우드 기반 보안 기능을 우회하고 애플리케이션 오리진을 직접 공격하지 못하도록 차단하는 추가적인 보안 레이어를 제공합니다. 웹사이트와 애플리케이션을 퍼블릭 인터넷으로부터 숨기고 클라이언트가 오리진에 직접 접속하지 못하도록 제한합니다. 전 세계에 분산된 Akamai Intelligent Edge Platform™에서 제공하는 최신 클라우드 보안 기술과 기존의 네트워크 인프라를 보완하는 역할을 하며 오리진 인프라를 직접 공격하는 네트워크 및 애플리케이션 레이어 위협 리스크를 완화하도록 설계되었습니다.

기업이 누릴 수 있는 혜택

- 애플리케이션 오리진에 직접 접속하지 못하도록 제한하여 **사이트 보안 강화 및 리스크 최소화**
- 다른 Akamai 엣지 보안 솔루션의 효율성을 높이는 **추가적인 보안 레이어 제공**
- 오리진의 글로벌 접속을 통합하여 **인프라 비용 절감**

> Akamai는 저희 사이트의 가용성을 보장하고 사용자들에게 가장 쾌적한 경험을 전송합니다.
>
> **— 스티븐 쉴링거(Stephen Schillinger),**
> 미국 이민국(U.S. Citizen and Immigration Services)
> 웹 서비스 부서 책임자



작동 방식

Site Shield는 Akamai 소스 주소 리스트를 제공하는데 이 주소를 통해서만 애플리케이션 오리진과 통신할 수 있습니다. 기업은 Site Shield 서버를 화이트리스트에 추가하고 네트워크 방화벽을 통해서 또는 인터넷 서비스 사업자(ISP)와 연계하여 표준 HTTP 및 HTTPS 포트(80 및 443)로 들어오는 모든 접속을 차단할 수 있습니다. Site Shield는 다른 Akamai 엣지 보안 솔루션과 함께 배포하도록 설계되었습니다. Site Shield는 웹 트래픽을 Akamai Intelligent Edge Platform으로 전달하여 클라이언트가 오리진에 직접 접속하지 못하도록 제한하고 Kona Site Defender, Web Application Protector, Bot Manager 등의 엣지 보안 솔루션은 트래픽을 검사하고 보안 위협을 차단합니다. API를 사용하면 DevOps 프로세스와 간편하게 통합되어 보안 설정을 자동으로 업데이트할 수 있습니다.

추가적인 장점

Site Shield는 오리진에서 애플리케이션 접속 문제가 발생하지 않도록 지원합니다. 몇 대의 Akamai 서버를 통해서만 오리진에 접속할 수 있기 때문에 오리진까지 도달하는 접속 건수가 감소합니다. 이를 통해 성능을 개선하고 오리진 인프라에 미치는 영향을 줄일 수 있습니다.

> “Akamai 덕분에 국방부 웹사이트에서 과거에는 불가능했던 일을 고려할 수 있게 됐습니다. 우리는 더 이상 분산 용량에 대해 걱정하지 않아도 되고 DoS 공격의 영향에 대응하는 데 걸리는 시간도 줄었습니다.
>
> **— 테리 데이비스(Terry Davis),**
> 미 국방부(Office of the Secretary of Defense) 퍼블릭 웹 프로그램 매니저

Akamai Experience the Edge