

Cloudbrix WAF+
CASE STUDY

Cloudbrix WAF+ (Web Application Firewall Plus)

Cloudbrix WAF+ 서비스는 클라우드 기반의 보안 서비스 (SECaaS, Software as a Service)로서 웹 애플리케이션 방화벽 서비스인 WAF(Web Application Firewall) 서비스를 포함하여 비즈니스 웹 보안에 필수적인 5가지 서비스를 하나의 플랫폼에서 제공합니다.

Cloudbric WAF+

Cloudbric WAF+는 클라우드를 기반으로 한 WAF, SSL/TLS 인증서 무료 제공, DDoS Protection, Malicious IP, Bot Control 기능을 하나의 플랫폼에서 제공하는 통합 웹 애플리케이션 보안 서비스다. 직관적인 인터페이스를 제공하는 Cloudbric WAF+ Console의 대시보드를 통해 위협을 즉각 확인할 수 있고, 보안 현황 리포트를 제공받을 수 있다. Cloudbric WAF+는 20년 이상의 경험을 보유한 보안 전문가들의 기술 지원과 모니터링, 그리고 취약점에 대한 즉각적이고 지속적인 업데이트를 통하여 높은 수준의 보안을 유지하고 있다. Cloudbric WAF+는 에이전트나 모듈을 별도로 설치할 필요 없이 보호 대상의 DNS 정보 변경만으로 강력한 웹 보안 도입을 가능하게 하였다.



공격에 대한 정보 수집과 대응 방식

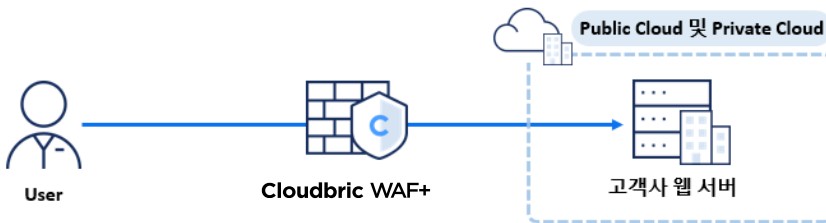
공격은 언제 어디서든 다양하게 변화하고 있다. 비즈니스 보호를 위해 다양한 보안 서비스들이 존재하지만, 서비스에 따라 공격에 대한 탐지와 차단 성능은 천차만별이다. 이러한 차이가 나는 요인은 다양한데 그 중 가장 대표적인 요인은 공격에 대한 정보 수집과 대응 방식에 따른 차이가 있기 때문이다. Cloudbric WAF+는 새로운 공격이 등장할 때마다 별도의 업데이트 없이 위협을 즉시 탐지/분석하는 특허 논리기반 탐지엔진과 AI 기술을 이용해 트래픽의 특성을 학습하는 자체 개발 AI 엔진으로 공격에 대한 정보를 수집한다. 그리고 데이터 의미/구조를 파악해 숨겨지거나 변경된 새로운 공격 패턴을 정확하게 감지해 차단한다. 이러한 기능들을 통한 정보 수집 및 대응 방식의 따른 확실한 방어 성능의 차이는 Cloudbric WAF+를 통해 경험할 수 있다.

Cloudbric WAF+ 도입형태

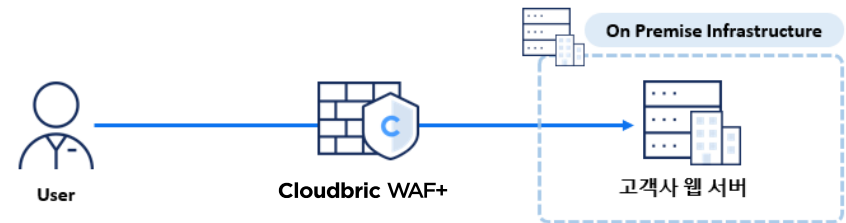
Cloudbric WAF+는 기업과 조직들의 필요사항을 충족시킬 수 있도록 다양한 환경에서 도입이 가능하다. 이러한 환경은 퍼블릭 클라우드 (AWS, Azure, Linode 등), 프라이빗 클라우드 (VMware, Xen 등), 그리고 온프레미스 환경 (물리 환경)으로 구분되며, 이러한 환경 내에서 Cloudbric WAF+는 SaaS (Software as a Service) 형태 또는 구축형 형태로 도입할 수 있다.

SaaS로 Cloudbric WAF+ 도입

[Public Cloud & Private Cloud]

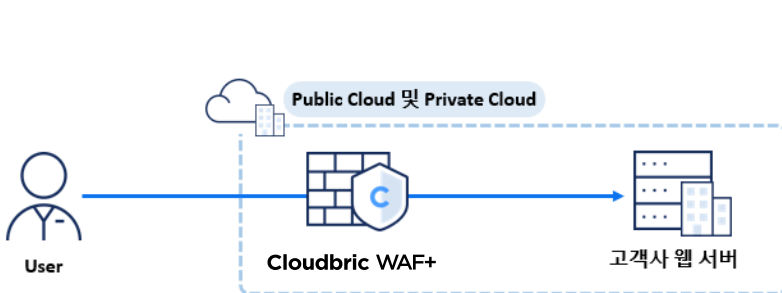


[On Premise]

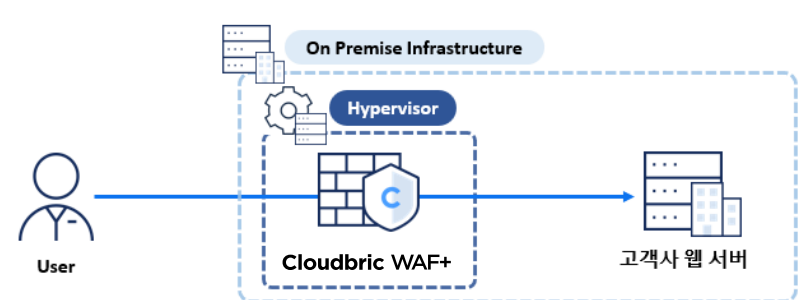


구축형으로 Cloudbric WAF+ 도입

[Public Cloud & Private Cloud]



[On Premise]



원활한 보안 서비스 이용을 위한 서비스 이전

The Challenge

일본 방송사의 출판사 편집부인 N사는 원예 및 식물을 주제로한 잡지를 출간함과 함께 동명의 사이트를 운영하고 있다. 해당 잡지는 N사의 월간지들 중 하나이며 동명의 사이트에서는 도감, 사진, 일지, 커뮤니티 등 다양한 서비스를 제공하고 있다. N사는 기존에 타 벤더사의 설치형 WAF를 이용 중에 있었다. 하지만 부정 액세스 IP 차단에 필요한 IP 리스트를 등록하고 나면 서버용 소프트웨어를 재가동 해야 하는데, 이때 소프트웨어를 재가동 하면 오히려 웹 페이지에 에러가 발생하며 사이트 운영에 지장을 주는 문제점을 확인하게 되었다. 때문에 N사는 운영에 영향을 주지 않으면서도 필요한 수준의 보안을 제공해줄 수 있는 새로운 보안 서비스로 이전하기로 결정하였다.

The Solution

N사는 Cloudblic WAF+를 도입하기 이전, 기존 서비스에서 문제가 되었던 에러의 발생 없이 Cloudblic WAF+가 안정적으로 서버 운영이 가능한 서비스인지에 대한 사전 확인 과정을 요청하였다. 당사는 Cloudblic WAF+의 탐지모드로 작동하는 무상평가 기간동안 여러가지 테스트를 통해 기존 WAF 서비스에서 나타난 에러 관련 문제를 해소할 수 있을 지를 점검하였고, 공격에 대한 탐지 능력을 확인할 수 있었다. N사는 Cloudblic WAF+에서 제공하는 무상 평가 기간 동안 해당 서비스에 대해 만족스러운 수준의 보안 서비스라 평가하였고, 이에 따라 Cloudblic WAF+ 서비스를 SaaS의 형태로 정식으로 도입하게 되었다.

The Result

N사는 Cloudblic WAF+ 도입을 통해 고객 서비스가 끊기지 않는 보안 환경을 유지할 수 있게 되었고 10분 단위의 도메인에 대한 접속 장애를 판단하는 Domain Health Check 기능과 5분 단위의 WAF 기능에 대한 장애를 판단하는 Server Health Check 기능을 통해 기존 보안 서비스 이용과 관련한 불편함을 해소할 수 있었다. 또한 Cloudblic WAF+를 이용하며 공격에 대한 위협 분석 레포트를 통해 서버에 일어나는 갖가지 위협들에 대한 가시화가 가능해지며 각종 위협에 대한 인지와 대응을 마련할 수 있게 되었다.

Conclusion

웹 보안 서비스는 업종/규모와 상관없이 비즈니스 자산을 가지고 있다면 보호를 위해서 고려가 아닌 필수적으로 이용해야만 한다. 하지만 많은 고객들이 어떤 기준으로 선택해야 하는지 등의 많은 어려움이 있기 때문에 도입을 망설이고 있다. 비즈니스 자산을 노리는 사이버 공격은 어떤 형태로 공격을 해올지 모르기 때문에 이에 대해 통합적인 대비책을 세우는 것이 중요하다. 더욱 철저하고 안전한 비즈니스 자산 보호를 위하여 웹 보안 서비스를 선택할 때는 아래와 같은 기준으로 비교 및 검토를 해야 한다.

서비스 도입 시 선정 기준

- 취약점 및 Zero-Day 공격으로 인한 피해가 일어나기 전, 사전에 탐지 및 차단이 가능한 대응 방식을 갖추고 있는가?
- 웹 방화벽 외에 비즈니스 자산을 보호 할 수 있는 추가적인 기능이 포함 되어 있는가?
- 비즈니스 자산 규모에 맞는 웹 보안 서비스 플랜을 선택할 수 있는가?
- 웹 보안 공격의 결과에 대해 가시화가 가능한 기능을 제공하는가?
- 빠른 서비스 도입과 24/365 실시간 응대 및 서포트가 가능한가?

Cloudblic WAF+ 도입효과

- Cloudblic WAF+는 별도의 업데이트 없이 새로운 공격에 대한 위협을 자동으로 탐지, 분석하는 논리기반 탐지엔진과 웹 트래픽의 특성을 학습하는 자체개발 AI엔진으로 보다 안전한 보안 서비스 운용이 가능하게 한다.
- Cloudblic WAF+는 보호 도메인의 개수와 트래픽 기준의 다양한 플랜으로 고객 비즈니스 규모와 환경에 맞게 효율적인 운영이 가능하게 한다.
- Cloudblic WAF+는 WAF (Web Application Firewall) 기능 이외에도 L3/L4, L7 DDoS 완화, SSL/TLS 인증서 제공, Malicious IP 차단, 악성 Bot 차단 등 비즈니스 웹 보안에 필수적인 기능들을 포함하고 있어 하나의 플랫폼에서 복잡하지 않고 일관된 정책으로 간편하게 관리 할 수 있도록 한다.
- Cloudblic WAF+는 전문가가 아니어도 직관적인 인터페이스를 제공하는 콘솔의 대시보드와 리포트를 통해 웹 위협을 확인할 수 있을 뿐만 아니라 리포트 생성도 가능하게 한다.
- Cloudblic WAF+는 DNS 변경만으로 빠르고 쉽게 도입이 가능하며 24/7 서포트 채널 운영 및 한/영/일 기술 문의 지원 및 오류 대응이 가능하다.

Cloudblic WAF+ 서비스는 고객의 비즈니스 자산을 유연하게 보호할 수 있도록 기본적인 웹 보안 서비스와 더불어 보안에 필수적인 다양한 기능을 제공하고 있기 때문에 다양한 비즈니스 요구사항에 대응이 가능하며 효율적인 비즈니스 보호에 탁월하다.