Cloudbric WAF+
CASE STUDY

Cloudbric WAF+ (Web Application Firewall Plus)

Cloudbric 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.

Penta SECURITY

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

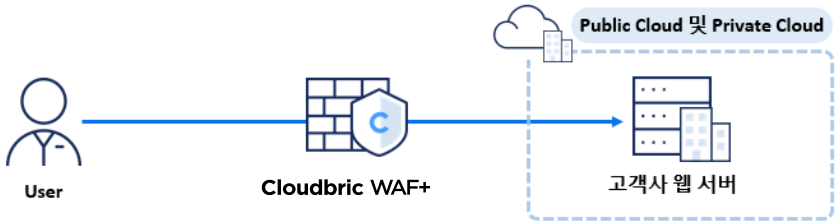
공격은 언제 어디서든 다양하게 변화하고 있다. 비즈니스 보호를 위해 다양한 보안 서비스들이 존재하지만, 서비스에 따라 공격에 대한 탐지와 차단의 성능은 천차만별이다. 이러한 차이가 나는 요인은 다양한데 그 중 가장 대표적인 요인은 공격에 대한 정보 수집과 대응 방식에 따른 차이가 있기 때문이다. Cloudbric WAF+는 새로운 공격이 등장할 때마다 별도의 업데이트 없이 위협을 즉시 탐지/분석하는 특허 논리기반 탐지엔진과 AI 기술을 이용해 트래픽의 특성을 학습하는 자체 개발 AI 엔진으로 공격에 대한 정보를 수집한다. 그리고 데이터 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

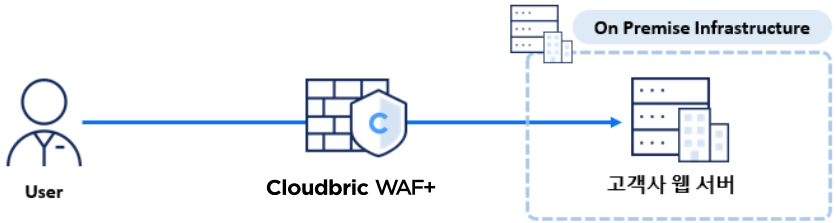
Cloudbric WAF+는 기업과 조직들의 필요사항을 충족시킬 수 있도록 다양한 환경에서 도입이 가능하다. 이러한 환경은 퍼블릭 클라우드 (AWS, Azure, Linode 등), 프라이빗 클라우드 (VMware, Xen 등), 그리고 온프레미스 환경 (물리 환경)으로 구분되며, 이러한 환경 내에서 Cloudbric WAF+는 SaaS (Software as a Service) 형태 또는 구축형 형태로 도입할 수 있다.

SaaS로 Cloudbric WAF+ 도입

[Public Cloud & Private Cloud]

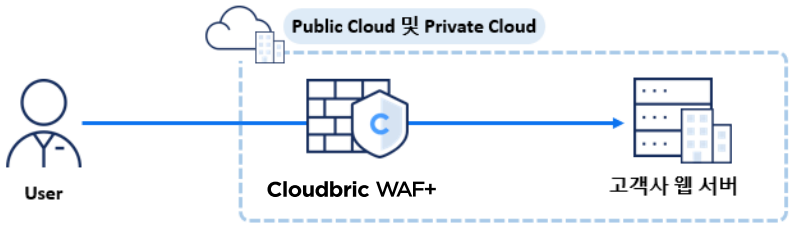


[On Premise]

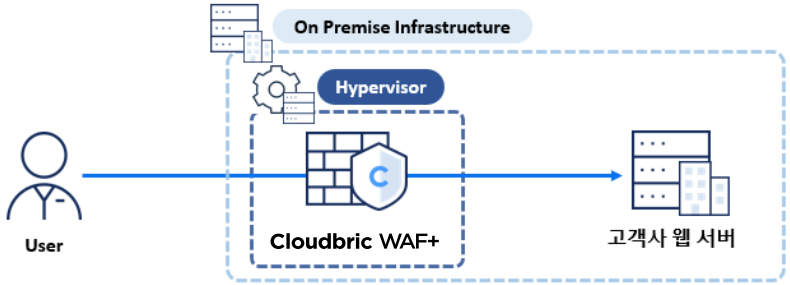


구축형으로 Cloudbric WAF+ 도입

[Public Cloud & Private Cloud]



[On Premise]



Cloudbric WAF+
CASE STUDY

산업

[소프트웨어]
웹 애플리케이션/소프트웨어 제공

회사정보

보험사를 대상으로 클라우드를 통해 실행되는
다양한 웹 애플리케이션 및 소프트웨어 제공

이용 플랜 정보

Shared 5Mbps
[최대 대역폭: 5Mbps]

서비스 환경 내 개인정보 및 데이터 보안 강화

The Challenge

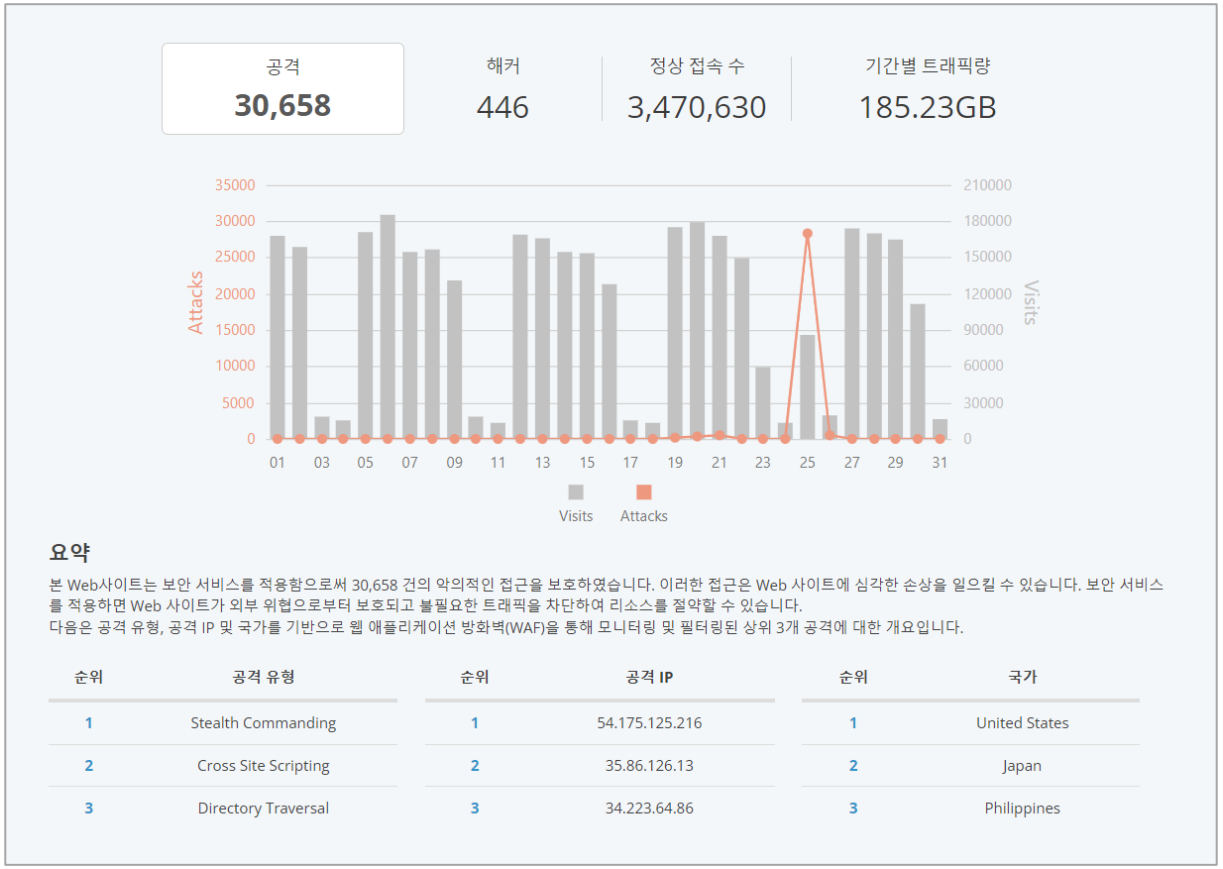
O사는 보험사를 대상으로 기업 정책 관리, 비용 청구, 제품 구성 등 다양한 클라우드 기반 솔루션을 제공하는 소프트웨어 제공사이다. O사의 솔루션들은 복잡한 핵심 시스템을 자동화하거나 단순화하여 요구되는 각종 리소스나 업그레이드에 대한 비용 절감에 도움을 주기 때문에 많은 보험사들이 O사의 솔루션들을 이용 중에 있다. 하지만 보험사들이 고객들의 민감한 개인정보를 다량 보유한 만큼 데이터 탈취 공격의 타겟이 되는 경우가 많을 수밖에 없다. 때문에 O사는 당사의 웹사이트뿐만 아닌 당사의 고객사 (보험사)의 웹사이트도 함께 보호할 수 있는 강력하고 포괄적인 데이터 보안 서비스를 필요로 하였다.

The Solution

O사에게 있어 가장 중요한 목표는 고객사가 보유한 고객들의 개인정보들이 데이터 통신 환경 내에서 취약점이나 공격으로 인한 사고에 의해 유출되지 않도록 사전에 방지하는 것이었다. 특히 O사는 취약점이나 Zero-Day (알려지지 않은 공격)와 같은 공격에 대한 탐지와 사전 차단이 이루어지기를 원했다. O사는 Cloudbric WAF+가 새로운 공격에 대한 위험을 자동으로 탐지한 후 이러한 위험을 분석하고 공격 패턴을 감지하여 사전 차단하는 기능에 주목하였고, Cloudbric WAF+ 도입을 결정하게 되었다.

The Result

O사는 Cloudbric WAF+ 도입을 통해 새로운 웹 공격 패턴에 대해 미리 감지하여 사전에 이러한 공격들을 차단할 수 있었다. Cloudbric WAF+는 별도의 업데이트 없이도 논리 기반 탐지 엔진을 이용하여 새로운 공격을 자동 탐지하며 공격으로부터 사이트를 방어하였고 데이터에 대한 보안을 강화하였다. 또한 화이트리스트 기반의 악성 Bot 차단 기능을 통해 자동화 공격을 방어하였다.



요약

본 Web사이트는 보안 서비스를 적용함으로써 30,658 건의 악의적인 접근을 보호하였습니다. 이러한 접근은 Web 사이트에 심각한 손상을 일으킬 수 있습니다. 보안 서비스를 적용하면 Web 사이트가 외부 위협으로부터 보호되고 불필요한 트래픽을 차단하여 리소스를 절약할 수 있습니다.
다음은 공격 유형, 공격 IP 및 국가를 기반으로 웹 애플리케이션 방화벽(WAF)을 통해 모니터링 및 필터링된 상위 3개 공격에 대한 개요입니다.

순위	공격 유형	순위	공격 IP	순위	국가
1	Stealth Commanding	1	54.175.125.216	1	United States
2	Cross Site Scripting	2	35.86.126.13	2	Japan
3	Directory Traversal	3	34.223.64.86	3	Philippines

공격 패턴을 감지한 후 사전차단한 기록을 보여주는 리포트

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?

Cloudbric WAF+ 도입효과

- Cloudbric 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.
- Cloudbric WAF+는 보호 도메인의 개수와 트래픽 기준의 다양한 플랜으로 고객 비즈니스 규모와 환경에 맞게 효율적인 운영이 가능하게 한다.
- Cloudbric 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.
- Cloudbric WAF+는 전문가가 아니어도 직관적인 인터페이스를 제공하는 콘솔의 대시보드와 리포트를 통해 웹 위협을 확인할 수 있을 뿐만 아니라 리포트 생성도 가능하게 한다.
- Cloudbric WAF+는 DNS 변경만으로 빠르고 쉽게 도입이 가능하며 24/7 서포트 채널 운영 및 한/영/일 기술 문의 지원 및 오류 대응이 가능하다.

Cloudbric 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.

Penta SECURITY

서울특별시 영등포구 여의공원로 115(여의도동)8, 9층 07241

Official Website. www.pentasecurity.co.kr
Cloudbric Service Website. www.cloudbric.co.kr
Contact. cloudbiz@pentasecurity.com