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

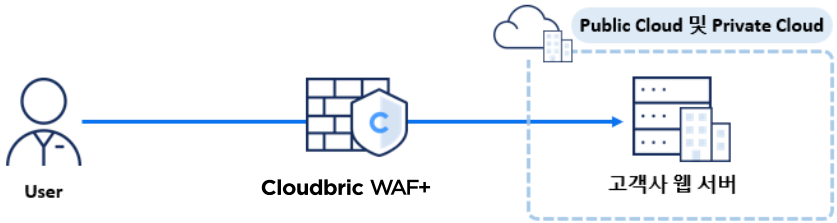
공격은 언제 어디서든 다양하게 변화하고 있다. 비즈니스 보호를 위해 다양한 보안 서비스들이 존재하지만, 서비스에 따라 공격에 대한 탐지와 차단의 성능은 천차만별이다. 이러한 차이가 나는 요인은 다양한데 그 중 가장 대표적인 요인은 공격에 대한 정보 수집과 대응 방식에 따른 차이가 있기 때문이다. Cloudbric WAF+는 새로운 공격이 등장할 때마다 별도의 업데이트 없이 위협을 즉시 탐지/분석하는 특허 논리기반 탐지엔진과 AI 기술을 이용해 트래픽의 특성을 학습하는 자체 개발 AI 엔진으로 공격에 대한 정보를 수집한다. 그리고 데이터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

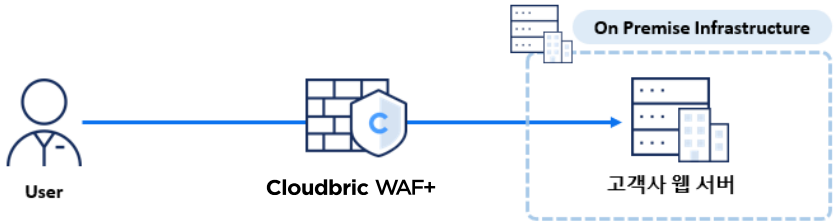
Cloudbric WAF+는 기업과 조직들의 필요사항을 충족시킬 수 있도록 다양한 환경에서 도입이 가능하다. 이러한 환경은 퍼블릭 클라우드 (AWS, Azure, Linode 등), 프라이빗 클라우드 (VMware, Xen 등), 그리고 온프레미스 환경 (물리 환경)으로 구분되며, 이러한 환경 내에서 Cloudbric WAF+는 SaaS (Software as a Service) 형태 또는 구축형 형태로 도입할 수 있다.

SaaS로 Cloudbric WAF+ 도입

[Public Cloud & Private Cloud]

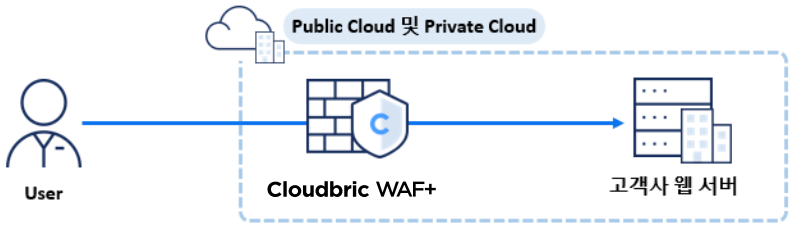


[On Premise]

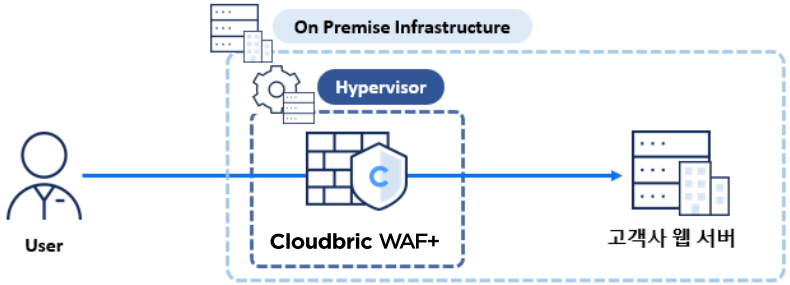


구축형으로 Cloudbric WAF+ 도입

[Public Cloud & Private Cloud]



[On Premise]



Cloudbric WAF+
CASE STUDY

산업

[엔터테인먼트]
게임 및 애니메이션 관련 컨텐츠 제작 및 유통

회사정보

일본 게임 제작 및 일본 애니메이션 관련 DVD와 블루레이를 제작하며
이러한 콘텐츠들과 관련된 사이트 운영

이용 플랜 정보

Shared 100Mbps
[최대 대역폭: 100Mbps]

사이트 보호와 부정 액세스의 효과적인 방어를 위한 대책

The Challenge

일본은 다양한 문화 사업을 보유하고 있지만, 그 중에서도 게임 및 애니메이션 분야는 세계에서 인정받으며 높은 인기를 누리고 있다. M사는 다양한 디바이스의 게임 제작 및 애니메이션 관련 DVD와 블루레이를 제작하는 회사이다. M사에서 제작한 게임 및 DVD 그리고 블루레이는 전세계에서 수출되며 이들이 보유한 미디어 콘텐츠는 세계적으로 유명한 콘텐츠 역시 여럿 포함하고 있다. 애니메이션이나 게임과 같은 미디어 콘텐츠들은 사람들의 관심을 많이 받기 때문에 다양한 공격에 노출되어 있다. 특히, 미디어 콘텐츠 제작사의 특성상 M사는 다소 짧은 간격으로 여러 게임 및 애니메이션을 출시하고 있었고, 이에 따라 각 게임과 애니메이션에 필요한 다양한 서비스 사이트 역시 짧은 간격으로 만들고 있었다. 때문에 다양한 서비스 사이트에 대한 취약점 파악이나 관리에 대한 어려움이 존재할 수밖에 없었다.

The Solution

M사가 가장 해소하고자 하였던 부분은 새로운 게임을 출시하면서 집중적으로 발생하는 부정 액세스 공격에 대해 방어함과 동시에 이러한 공격이 반복되지 않도록 하는 것이었다. M사는 당사에서 보유한 모든 서비스 사이트에 대해 직접 정보를 수집 및 분석하여 부정 액세스를 차단하는 일련의 과정을 수행할 수 없었기 때문에 이 과정이 모두 가능한 보안 서비스 도입을 필요로 하였다. M사는 Cloudbric WAF+를 SaaS 형태로 도입함으로써 공격에 대한 데이터 수집 및 분석과 공격에 대한 방어가 모두 가능하게 되었다.

The Result

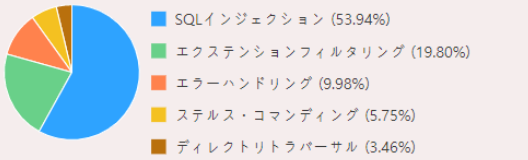
M사는 Cloudbric WAF+ 도입 후, Cloudbric WAF+ 서비스 콘솔의 직관적이고 가시성 높은 대시보드를 통해 외부 공격에 대한 분석데이터를 정확하게 확인할 수 있게 되었고, 분석된 데이터에 따라 공격에 대응할 수 있는 적절한 차단 조치를 설정할 수 있었다. 또한 Cloudbric Labs* 통해 정기적으로 수집 및 분석되는 위협 정보 데이터를 이용하여 Malicious IP를 차단하며 부정 액세스를 더욱 효과적으로 차단하며 이전에는 별다른 보호조치가 없이 공개되던 신규 웹사이트들이 이제는 철저한 보안 아래 공개 되고 있다.

* **Cloudbric Labs**는 클라우드브릭의 위협 데이터 시스템의 핵심으로 전 세계에서 수집한 Web 취약성과 리스크 정보를 보안 전문가가 분석한 결과를 제공하는 플랫폼이다. 사이버 공격자들이 과거에 행했거나 유사한 공격 수법과 패턴을 사전에 파악하여 이를 제거하거나 방어하는데 사용되는 지식 정보로써 다양한 채널로 수집된 위협 데이터를 블록체인 기반의 신뢰 가능한 정보로 제공한다.

ブロックされた攻撃の概要

遮断した攻撃に対し、その内訳と最も多かった攻撃に対し説明します。

攻撃の内訳 (%)



最も多く発生した上位5個の攻撃タイプを表示します。
当該期間中に発生したすべての攻撃タイプは「検知ログ」メニューで確認できます。

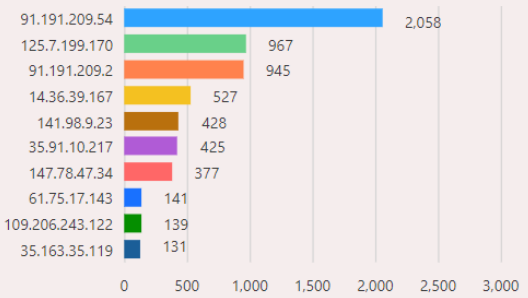
当該期間中に最も多く行われた攻撃タイプは、「SQLインジェクション」です。

SQLインジェクション攻撃は、Webアプリケーション内にSQLフレーズを挿入し、データを悪用/変更したり、管理者の検証をバイパスしたりします。 攻撃者はまず、Webアプリケーションからデータベースに送信されたパラメータを見つけます。 その後、攻撃者はそれらのパラメータに不正なSQLコマンドを挿入し、不正なクエリをデータベースに送信します。

上位の攻撃元IPアドレス

Webサーバに悪意のある攻撃をしかけた上位の攻撃元IPアドレスを表示します。悪意のある訪問者だと思われるIPアドレスの場合は、ブラックリストに登録してください。

攻撃頻度が最も多かった攻撃元IP



攻撃頻度が最も多かった上位10個の攻撃元IPを表示します。
当該期間中に発生したすべての攻撃元IPは「検知ログ」メニューで確認できます。
発生件数が同じIPがある場合、IPは10個まで表示されます。

当該期間中における最も危険な攻撃元IP

弊社のWAFは世界中で発生した攻撃の分析を行なっています。次は、当該期間中にWAFによって遮断された危険度が高いIPリストです。これらのIPをブロックIPリストに登録することを推奨します。

	IP	攻撃発信国
1	109.237.98.53	ロシア
2	185.83.146.154	トルコ
3	185.241.208.25	モルドバ

M사의 도메인에 발생한 위협 데이터를 수집, 분석, 및 차단한 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
© Penta Security Inc.
Official Website. www.pentasecurity.co.kr
Cloudbric Service Website. www.cloudbric.co.kr
Contact. cloudbiz@pentasecurity.com