IMPERVA®

ThreatRadar: 웹 애플리케이션 위협 인텔리전스

데이터시트

온라인 비즈니스가 영향을 받기 전에 위협 차단

사이버 범죄자들은 인터넷을 접하는 웹 애플리케이션의 취약점을 악용하여 기존 보안 통제 체계를 우회하여 계정을 갈취하고 IT 인프라의 측면을 노리고 비즈니스 크리티컬 데이터 및 애플리케이션에 액세스할 수 있는 초기 공격 벡터로 활용합니다. 공격자들의 능력은 갈수록 향상하고, 목표는 다각화되며, 방식은 더욱 은밀해지고 있습니다.

끊임 없이 진화하는 웹 기반 공격에 대비할 수 있는 고급 경고 시스템은 발전된 형태의 사이버 범죄에 대비하기 위한 필수 요소입니다. 이에 따라 신뢰할 수 있는 크라우드 소싱 기반의 플랫폼과 동종업계 종사자 커뮤니티로부터 도출된 위협 인텔리전스의 중요성이 그 어느 때보다도 높아지고 있습니다. Imperva ThreatRadar는 업계 1위를 달리는[1] SecureSphere WAF(Web Application Firewall)를 다음과 같은 보호 기능으로 보강해 주는 고급 위협 인텔리전스 피드입니다.

- **Reputation Service:** 소스의 최신 실시간 평판에 기초하여 트래픽 필터링 수행
- **Community Defense:** Imperva 사용자들로부터 크라우드 소싱받은 독창적인 위협 인텔리전스 제공
- **Bot Protection:** 봇넷 클라이언트 및 애플리케이션 DDoS 공격 감지
- **Account Takeover Protection:** 웹 사이트 사용자 계정을 공격 및 갈취 시도로부터 보호
- **Fraud Prevention:** 업계 최고의 파트너 사기 방지 솔루션 설치 간소화

Imperva ThreatRadar는 업계 1위를 달리는[1] SecureSphere WAF(Web Application Firewall)를 보호 기능으로 보강해 주는 고급 위협 인텔리전스 피드입니다.

[1] Gartner Magic Quadrant WAF(Web Application Firewall) 부문, 2015년 7월 15일

Imperva ThreatRadar 서브스크립션 서비스

- Reputation Service
- Community Defence
- Bot Protection
- Account Takeover

위협 인텔리전스를 활용하여 악의적인 사용자 및 자동 공격 차단

크라우드 소싱 방식의 위협 인텔리전스로 새로운 공격 벡터 식별

ThreatRadar는 데이터 및 애플리케이션 보안 분야의 세계적인 전문가들로 구성된 Imperva ADC(Application Defense Center)의 조사로 탄생한 위협 인텔리전스에 SecureSphere WAF 고객들의 실시간 위협 데이터를 통합한 제품입니다.

악의적인 소스에 대한 손쉬운 감지 및 차단

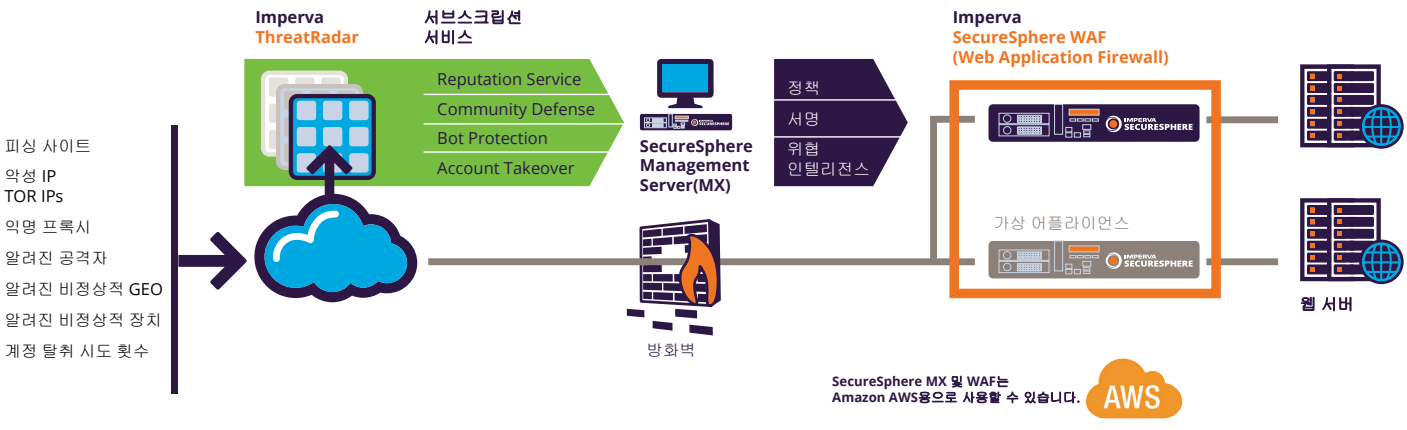
타사 보안 제공업체와 전 세계에 설치된 SecureSphere WAF의 데이터를 모두 통합한 ThreatRadar는 알려진 악의적인 소스를 조기에 감지하고 포괄적으로 방어합니다.

위협 데이터의 효과 개선 및 보안 운영 워크로드 감소

SecureSphere WAF 고객은 사용자 평판, 봇넷, 계정 탈취 시도 횟수 및 취약점을 찾기 위해 애플리케이션을 정찰하는 해커 행위에 대한 자동 경고를 발령하고 웹 요청을 차단하여 악의적인 웹 트래픽과 관련된 보안 운영 워크로드를 대폭 감소할 수 있습니다.

최신 공격 소스에 대한 자동화된 지속적 피드

ThreatRadar는 거의 실시간으로 복수의 공격 피드를 자동으로 제공합니다. 보안 피드로 최근 SQLi(SQL 인젝션), XSS(교차 사이트 스크립팅), DDoS 및 기타 웹 공격을 수행한 소스를 식별합니다.



알려진 악성 소스

- 알려진 비정상적 공격자가 공격의 90%를 차지합니다
- 악성 봇이 트래픽의 60%를 차지합니다
- 훔친 자격 증명을 사용한 공격이 웹 공격의 50%를 차지합니다

출처: Imperva 및 Verizon DBIR

명백하고 관련성 높은 경고 및 보고서를 통하여 능률적으로 포렌식 분석 수행

ThreatRadar는 보안 이벤트 분석 시 절대로 추정하지 않습니다. 사용자 반응과 지리적 위치 데이터로 추가적인 맥락 정보를 파악할 수 있으며, 이를 통해 정밀한 사고 대응과 운영 워크로드 최소화가 가능해집니다.

ThreatRadar Reputation Service

ThreatRadar Reputation Service는 다음과 같은 알려진 악의적인 소스에 대한 실시간 위협 인텔리전스를 SecureSphere WAF에 보강합니다.

- 악의적인 IP 주소: 다른 웹 사이트를 반복적으로 공격한 이력이 있는 소스
- 익명 프록시: 실제 위치를 은폐하기 위해 공격자들이 사용하는 프록시 서버
- TOR 네트워크: TOR(The Onion Router)를 사용하여 공격 소스를 은폐하는 해커들
- IP 위치 추적: 공격 발원지 파악 및 접근 차단
- 피싱 URL: 피싱 공격에 사용되는 허위 사이트(URL)
- 코멘트 스패머: 알려진 코멘트 스패머의 IP 주소

ThreatRadar Community Defense

ThreatRadar Community Defense는 전 세계에 설치된 SecureSphere WAF의 전체적인 인사이트를 활용하여 각 SecureSphere WAF에 크라우드 소싱된 위협 인텔리전스를 거의 실시간으로 제공합니다. 특허 출원 중인 알고리즘을 적용하여 수집하는 실시간 공격 데이터로 공격 패턴, 정책 및 평판 데이터를 도출하고, Imperva WAF 고객이 경험하는 위협 인텔리전스를 거의 실시간으로 제공합니다.

ThreatRadar Reputation Service가 선도적인 외부 보안 공급업체의 보안 정보에 의존하는 반면, ThreatRadar Community Defense는 전 세계에 설치된 SecureSphere WAF로부터 집계한 실시간 공격 정보를 활용합니다.

ThreatRadar 클라우드로 익명 공격 데이터를 전송하도록 설정하는 SecureSphere WAF 고객들은 ThreatRadar Community Defense를 무료로 받을 수 있습니다.

ThreatRadar Bot Protection

ThreatRadar Bot Protection Service는 SecureSphere WAF를 활용하여 수신 트래픽 중 실제 사용자 트래픽과 봇에서 기인한 트래픽, '정상적인' 봇과 '비정상적인' 봇을 구분하고, 브라우저 유형으로 트래픽을 분류합니다.

DDoS 공격, 코멘트 스팸 인젝션, 웹 사이트 콘텐츠 스크레이핑 등을 수행하는 악성 봇은 전체 웹 사이트 공격의 95% 이상을 차지합니다. 전체 웹 사이트 트래픽의 최대 30%를 차지하는 무단 봇의 접근을 차단함으로써 웹 사이트 성능과 보안을 향상시킬 수 있습니다.

Imperva SecureSphere 사이버 보안

Imperva SecureSphere는 SecureSphere 웹, 데이터베이스 및 파일 보안을 포함하는 포괄적인 통합 보안 플랫폼입니다. 막대한 규모의 조직의 데이터센터 보안 수요에 부응할 수 있도록 확장할 수 있으며, 진화하는 위협에 대비하여 제품의 최첨단 보호 기능을 유지하기 위해 밤낮을 가리지 않고 최선을 다하는 세계적인 수준의 보안 리서치 조직 Imperva Application Defense Center가 든든하게 뒷받침합니다.

ThreatRadar Account Takeover Protection

범죄자들은 맬웨어 및 피싱 공격을 통해 훔친 자격 증명을 사용하여 고객 계정에 무단으로 접근하고, 현금을 이체하고, 사기성 거래를 수행하고, 기업의 평판을 훼손합니다. ThreatRadar Account Takeover Protection은 자격 증명/장치 위협 인텔리전스를 활용하여 SecureSphere WAF에서 무단 접근을 감지하고 완화할 수 있도록 해 줍니다.

자격 증명 인텔리전스: 감지 및 완화

- 훔친 자격 증명 활용
- 취약한 암호를 사용한 사전 대입 공격(Dictionary Attack)
- 권한 있는 계정에 대한 기본 암호 공격

장치 인텔리전스: 감지 및 완화

- 리스크가 높은 장치로부터의 로그인
- TOR/프록시에 의해 은폐된 장치에서 오는 트랜잭션
- 위치 정보 기반 고위험 위치—ISP, 위치 정보/IP 불일치
- 단일 계정에 접근하는 복수의 장치, 또는 단시간에 복수의 계정에 접근하는 단일 장치

ThreatRadar Fraud Prevention

기업은 Imperva SecureSphere WAF용 ThreatRadar Fraud Prevention 커넥터를 사용하여 업계 최고의 사기 방지 파트너들과 신속하게 통합함으로써 보호 대상 애플리케이션에 대한 완전한 시야를 확보할 수 있습니다.

SecureSphere WAF는 다음과 같은 사기 모니터링 솔루션과 통합하여 사기 정책에 대한 중앙 집중식 관리를 지원합니다.

- iovation ReputationManager 360
- ThreatMetrix TrustDefender ID

ThreatRadar 에디션

ThreatRadar는 Reputation Service, Community Defense 및 Botnet Protection이라는 세 가지 서브스크립션 기반 피드를 다음과 같은 두 가지 번들로 제공하여 기업이 쉽게 구매하고 경제적으로 구현할 수 있습니다.

ThreatRadar 커뮤니티 에디션

설치한 SecureSphere WAF의 실시간 공격 데이터를 Imperva의 글로벌 클라우드 ThreatRadar 리포지토리와 공유하도록 설정한 기업이 사용할 수 있는 번들입니다. 고객 데이터는 자동으로 익명 처리됩니다.

ThreatRadar 엔터프라이즈 에디션

설치한 SecureSphere WAF의 실시간 공격 데이터를 Imperva의 클라우드 ThreatRadar 리포지토리와 공유하지 않도록 설정한 기업에서 사용할 수 있는 번들입니다. 고객들은 전 세계에 설치된 SecureSphere WAF의 전체적인 인사이트를 확보하고 Imperva ADC의 위협 리서치를 활용할 수 있습니다.

DS-SECURESPHERE-THREATRADAR-A4-1015-rev2