AKAMAI 제품 설명서

Secure Internet Access ThreatAvert

중요한 네트워크 자산의 보호 및 가입자에게 영향을 주는 멀웨어 탐지

서비스 제공업체는 가입자의 만족도에 직접적인 영향을 주는 네트워크 보안을 통해 브랜드 가치를 끌어올릴 수 있다는 점을 잘 알고 있습니다. 대부분의 위협은 DNS에 의존해 작동하며, 중요한 DNS 인프라를 대상으로 한 새로운 위협도 등장했습니다. 이제 서비스 제공업체는 네트워크 리소스와 가입자를 보호하는 방식을 재고해야만 합니다. 더구나, 모든 것이 연결된 오늘날의 세계에서 위협은 점점 더 활발해지며 다양해지고 있습니다.

Akamai Secure Internet Access ThreatAvert는 실시간으로 DNS 룩업을 확인하여 악성 활동을 탐지하고 차단합니다. Secure Internet Access ThreatAvert는 네트워크 중단 또는 지연을 야기하거나, 가입자 경험에 악영향을 미치거나, 기타 네트워크 보호 방법을 무력화하는 다음과 같은 위협을 대상으로 합니다.

- DNS 기반 DDoS: 막대한 용량의 쿼리로 리졸버의 마비 초래
- 봇 멀웨어: 중요한 개인 데이터를 훔치거나 소비자의 디바이스를 훼손
- DNS 터널: DNS 내에 다른 프로토콜을 전송해 서비스를 도용

Secure Internet Access ThreatAvert는 Akamai 동적 위협 피드가 장착된 Akamai의 대표적인 CacheServe DNS 리졸버를 기반으로 합니다. CacheServe는 안정성을 대표하는 업계 표준입니다. 다년간에 걸친 성능 최적화에 대한 투자와 꾸준히 개선된 다양한 소프트웨어 기능으로 DNS 트래픽이 폭증하는 상황에서도 탁월한 복구 성능과 가용성을 보장합니다. Akamai 위협 인텔리전스는 Akamai Data Science 팀에서 개발했습니다. Akamai Data Science는 매일 전 세계에서 실시간으로 스트리밍되는 천억 개 이상의 DNS 쿼리를 처리합니다.

DNS **서버에서 담당하는** DNS **보안**

DNS 쿼리는 악성 활동을 나타내는 주요 지표라고 할 수 있습니다. 명령 및 제어 서버, 멀웨어 다운로드, 유출 사이트 등 악성 리소스의 주소를 확인하는 작업은 대부분의 악성 활동을 활성화하는 첫 단계이기 때문입니다. DNS 리졸버는 서비스 제공업체 네트워크의 모든 쿼리를 다루므로 위협에 대응하기 위한 인텔리전스를 내장하기에 가장 적절한 위치입니다. 수신되는 쿼리를 동적 위협 목록의 항목과 비교하는 방법으로 악성활동을 감지할 수 있습니다.

Secure Internet Access ThreatAvert는 DNS 제어 영역에서 확장할 수 있습니다. 이 경우, 데이터 영역 트래픽과 함께 확장되는 전용 패킷 처리 솔루션보다 비용, 운영상의 작업, 네트워크에 미치는 영향 등을 큰 폭으로 줄일 수 있습니다.

ThreatAvert는 구성이 간소하고, 효율성이 뛰어나며, 네트워크 트래픽으로 지연 시간을 늘리지도 않습니다. 또한, 네트워크를 기반으로 하므로 모든 디바이스를 지원하고 클라이언트와 호스트에 보안 소프트웨어를 설치하거나 업데이트할 필요도 없습니다.

기업이 누릴 수 있는 혜택

- 디바이스 종류에 상관없이 수백만 명의 가입자로 확장 가능한 경량 솔루션
- 최고의 데이터 과학을 통해 탁월한 심층 분석과 폭넓은 위협 범위를 지원
- 지속적으로 업데이트되는 위협 피드를 통해 공격 유형 변화에 따른 방어 유지
- 가독성이 우수한 실시간 보고서에서 빠르게 확인 가능한 위협 상태 표시 및 세부 정보 연결
- 위협 및 텔레메트리 데이터의 효율적인 수집 및 확장형 관리

Akamai

우수한 정확도, 심층적 보호, 다양한 위협에 대한 대처 능력

멀웨어 개발자는 꾸준한 혁신을 통해 작업에서 ROI를 극대화하고자 노력합니다. 결국, 대부분의 위협은 탐지를 회피하기 위해 정교하게 설계되고 살아남기 위해 빠르게 변화하기 마련입니다. 공격면 또한 놀라울 정도로 다양한 사물 인터넷까지 확대되었으며, 이에 따라 공격자가 목표를 달성하기 위해 사용하는 방식 역시 다양해지고 있습니다.

Akamai Data Science 팀은 세밀해지고 다양화되는 위협 환경을 제대로 파악하며 실시간으로 스트리밍되는 DNS 쿼리를 분석하기 위해 주요 시스템을 개발, 구현 및 통합했습니다. 평판 목록, 허니팟, 기타 써드파티 소스에서 가져온 위협 데이터도 이 과정에 통합 적용되었습니다. 폭넓은 대응 위협 범위와 심층적 수준, 정확도, 그리고 민첩성은 다음과 같은 투자로 인해 가능했습니다.

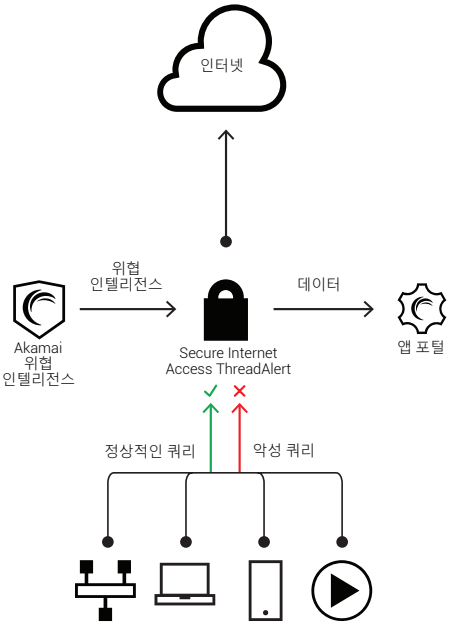
- DNS-DDoS와 같은 비정상적 동작을 빠르게 탐지하고, 이질적인 위협 간의 상관관계를 분석하고, 새로운 봇인 도메인 생성 알고리즘을 식별할 수 있는 알고리즘(특허 출원 중) 개발
- 특정 이름을 자동으로 허용하여 정상적 DNS 쿼리를 상시적으로 보호하기 위한 고급 기술 개발
- 다년간의 보안 관련 경력과 멀웨어 및 DNS 데이터에 대한 심층적 지식을 갖춘 연구 담당 인력 고용
- 실시간 데이터 스트림을 실시간으로 처리하기 위해 전 세계에 네트워크 및 데이터 센터 구축

정확도 정책을 통한 악성 트래픽 차단 및 정상 트래픽 보호

불필요한 DNS 트래픽을 관리하기 위해 Akamai 위협 인텔리전스 피드에 정확도 정책이 통합되었습니다. 다음과 같이 다양하고 심층적인 기능으로 악성 쿼리에 대응하고 정상 쿼리를 보호(응답)하기 위한 세분화 필터링을 지원합니다.

- 수신되는 쿼리 또는 내보내는 응답에 정확도 정책을 적용할 수 있습니다.
- IP, QTYPE, FQDN 또는 기타 다양한 쿼리 파라미터를 기반으로 필터 또는 속도 제한을 설정할 수 있습니다
- 필터 또는 속도 제한에 QTYPE AND FQDN, IP AND FQDN 등의 논리 연산자와 함께 다수의 쿼리 파라미터를 사용할 수 있습니다.
- 필터 또는 속도 제한을 Akamai 위협 인텔리전스 동적 위협 목록이나 운영자가 제공한 목록의 항목과 비교할 수 있습니다.
- 정책 및 위협 목록을 MATCH against BLOCKLIST, NOT on ALLOWLIST 등과 결합해 활용할 수 있습니다.
- drop, synthesize answer, answerwith truncate, NXD, NOERROR 등 다양한 정책 작업으로 쿼리의 처리 방식을 결정합니다.
- 여러 정책을 서로 결합하고 중첩해 보다 강력한 기능을 발휘합니다.

정확도 정책은 서비스 제공업체 네트워크에 국한된 문제를 해결하기 위해 수동으로 구성할 수도 있습니다.



Akamai 전문가들이 처리하는 대용량 데이터 스트림을 참고하면 특정 영역에 국한된 공격뿐만 아니라 인터넷 전체의 각종 악성 활동까지 종합적으로 파악할 수 있습니다.

확장성이 뛰어난 데이터 관리, 다기능 텔레메트리 및 보고 기능

Secure Internet Access ThreatAvert는 세계 최대 네트워크에서 검증된 오픈 솔루션 기반 데이터 관리 아키텍처를 통합하여 웹 규모와 속도면에서 운영 우수성을 제공합니다. 네트워크 전반의 Secure Internet Access ThreatAvert 시스템에서 실시간으로 스트리밍된 데이터가 집계되어 보고(아래 설명 참조) 및 기타 시스템에서 활용됩니다. 또한 안정적인 아키텍처를 토대로 무중단 가용성이 보장되고 이는 곧 무중단 고객 경험을 뒷받침합니다. Splunk, Hadoop 등과 같은 빅 데이터 시스템을 여는 선택적 커넥터 또는 특수 제작된 애플리케이션을 사용하면 운영, 보안, 비즈니스에 관해 더 깊은 인사이트를 얻을 수 있습니다.

차단된 DNS 쿼리, 저장된 최대 DNS 대역폭, 네트워크의 주요 멀웨어, 감염된 가입자, 위협 인텔리전스 업데이트 등을 다루는 Secure Internet Access ThreatAvert 보고서의 Executive Dashboard를 통해 보안 체계를 신속하게 평가할 수 있습니다. 또한 Security Dashboard에서는 DDoS와 멀웨어를 자세히 보여주는 그래프를 확인할 수 있습니다. 단 한 번의 클릭으로 멀웨어 및 감염된 클라이언트의 세부 정보도 연속적으로 계층화해 보여줍니다. 몇 분 안에 생성할 수 있는 맞춤형 대시보드와 보고서는 고유한 운영상의 요구를 충족시키기 위해 보안 데이터를 사용자 정의 형식으로 보여줄 수 있습니다. 운영 담당자는 태그 기반 보고서를 사용하여 자체 Secure Internet Access ThreatAvert 토폴로지의 뷰를 각자의 특수한 요구 사항에 알맞게 구성할 수 있습니다.