AKAMAI 제품 설명서

Secure Internet Access Enterprise 클라우드 기반 DNS 방화벽

기업은 직접 인터넷 접속, SaaS(Software as a Service) 애플리케이션, 클라우드 서비스, 재택근무 정책, IoT(Internet of Things)를 도입함에 따라 공격표면이 급격히 증가하고 새로운 보안 과제에 직면하게 됩니다. 멀웨어, 랜섬웨어, 피싱, 데이터 유출 등 최신 보안 위협으로부터 기업과 사용자를 보호하는 일은 점점 어려워지고 있습니다. 한정된 리소스를 사용해 보안 컨트롤 포인트 문제를 해결하고 기존에 사용 중인 온프레미스 보안 솔루션과의 갭(gap)도 관리해야 합니다.

Akamai Secure Internet Access Enterprise는 클라우드 기반의 DNS(Domain Name System) 방화벽입니다. 기존에 사용 중인 보안 솔루션과 관련된 복잡성이나 관리 오버헤드 없이 언제 어디서나 사용자와 디바이스가 인터넷에 안전하게 접속할 수 있도록 지원하는 솔루션입니다. 전 세계 인터넷 및 DNS 트래픽에 대한 인사이트와 다수의 멀웨어 탐지 엔진을 기반으로 실시간 위협 인텔리전스를 제공합니다.

Secure Internet Access Enterprise

Secure Internet Access Enterprise는 Akamai Connected Cloud와 Akamai의 통신사급 리커시브 DNS 서비스를 기반으로 합니다. 빠르게 설정하고 쉽게 배포할 수 있는 클라우드 기반의 DNS 방화벽으로서 하드웨어를 설치하거나 유지 관리할 필요가 없습니다.

Secure Internet Access Enterprise는 실시간 Akamai 클라우드 보안 인텔리전스를 활용해 멀웨어, 랜섬웨어, 피싱, 저처리량 DNS 기반 데이터 유출과 같은 표적 위협을 선제적으로 식별하고 차단합니다.

보안팀은 Akamai의 포털을 통해 사용자들이 인터넷에 접속하는 위치에 상관 없이 통합 보안 정책과 제한적 사용 정책(AUP)을 몇 분 안에 일괄적으로 생성, 배포, 적용할 수 있습니다.

기업이 누릴 수 있는 혜택

- 몇 분 안에 전 세계적으로 설정 및 배포가 가능하고 별도의 하드웨어가 필요하지 않아 사용자 불편을 초래하지 않으면서 신속하게 확장할 수 있는 클라우드 기반의 DNS 방화벽을 통해 웹 보안을 클라우드로 이동시킵니다.
- 최신 위협 인텔리전스를 기반으로 멀웨어 및 랜섬웨어 드롭 사이트, 피싱 사이트, 멀웨어 명령 및 제어(C2) 서버에 대한 요청을 선제적으로 차단하여 보안 체계를 강화하고 저처리량 DNS 데이터 유출을 파악합니다.
- 카테고리 또는 리스크 점수를 기준으로 애플리케이션을 식별하고 차단해 섀도 IT 및 승인되지 않은 애플리케이션의 사용을 제어합니다.
- 오탐 및 다른 보안 제품의 알림 건수를 줄이고, 장소에 상관 없이 보안 정책 및 업데이트를 신속히 관리하고, 모든 지역의 사용자를 보호하여, 보안 관리 시간과 복잡성을 최소화합니다.

Akamai

작동 방식

Secure Internet Access Enterprise는 성능에 영향을 주지 않으면서 보안을 제공하고 몇 분 안에 활성화돼 복잡성을 줄일 수 있는 클라우드 기반의 보안 서비스입니다. IPsec 터널, 경량 클라이언트, Akamai의 매니지드 DNS 포워더, 기존 DNS 리졸버 수정 등 다양한 방법을 사용해 리커시브 DNS 트래픽을 Secure Internet Access Enterprise로 리디렉션하는 것만으로 보호 효과를 얻을 수 있습니다.

요청된 모든 도메인이 Akamai의 실시간 위협 인텔리전스를 기반으로 확인되고 확인된 악성 도메인에 대한 요청은 자동으로 차단됩니다. DNS를 1차 보안 레이어로 사용해 웹 접속이 이루어지기 전에 킬체인 초기 단계에서 위협을 선제적으로 차단합니다. 또한, DNS는 모든 포트 및 프로토콜에서 사용할 수 있도록 설계되었기 때문에 표준 웹 포트나 프로토콜을 사용하지 않는 멀웨어 역시 방어할 수 있습니다. 도메인 확인을 통해 사용자가 접속하려는 콘텐츠 종류를 확인하고 해당 콘텐츠가 기업의 제한적 사용 정책(AUP)을 위반할 경우 접속을 차단할 수 있습니다.

추가 보호를 위해 위험한 도메인을 클라우드 프록시로 전달해 URL을 검사할 수 있으며, 요청된 HTTP/S URL은 Akamai의 실시간 위협 인텔리전스를 통해 검사하고 악성 URL은 자동으로 차단합니다.

Secure Internet Access Enterprise는 방화벽, SIEM(Security Information and Event Management) 솔루션, 외부 위협 인텔리전스 피드를 비롯한 다른 보안 제품 및 보고 툴과 쉽게 통합되므로 보안 스택의 모든 계층에서 투자를 극대화할 수 있습니다.

또한 기업은 경량 Secure Internet Access Enterprise 클라이언트를 디바이스에 배포함으로써 네트워크 외부에서 사용되는 노트북이나 모바일 디바이스를 신속하고 간편하게 보호할 수 있습니다.

Akamai 클라우드 보안 인텔리전스

Secure Internet Access Enterprise는 보안 위협과 리스크에 대한 인텔리전스를 실시간으로 제공하는 클라우드 보안 인텔리전스를 기반으로 합니다.

Akamai의 위협 인텔리전스는 비즈니스에 영향을 미칠 수 있는 현재 위협과 관련 위협을 방어하고 보안팀의 조사가 필요한 오탐 알림 건수를 최소화하도록 설계되었습니다.

이 인텔리전스는 매일 글로벌 웹 트래픽의 최대 30%를 처리하고 11조 개의 DNS 쿼리를 전송하는 Akamai Connected Cloud에서 연중무휴 상시 수집된 데이터로부터 도출됩니다. Akamai 인텔리전스는 수백 개의 외부 위협 피드를 통해 강화되며, 통합된 데이터세트는 고급 행동 분석 기법, 머신 러닝, 독점 알고리즘을 사용하여 지속적으로 분석 및 관리됩니다. 새로운 보안 위협이 탐지될 때마다 즉각적으로 Secure Internet Access Enterprise 서비스에 추가되기 때문에 실시간 보안이 가능합니다.

Akamai Connected Cloud

Secure Internet Access Enterprise 서비스는 클라우드 컴퓨팅, 보안, 콘텐츠 전송을 위한 세계에서 가장 분산된 플랫폼인 Akamai Conntected Cloud에 구축되어 있습니다. Akamai Connected Cloud는 전 세계적으로 촘촘하게 분산되어 있으며 100% 가용성을 보장하는 서비스 수준 협약(SLA)을 제공하고 기업의 웹 보안에 대한 최적의 안정성을 보장합니다.

기업이 누릴 수 있는 혜택

VPN을 사용하지 않고, 보안 정책과 AUP를 실행하는 경량 Secure Internet Access Enterprise 클라이언트를 통해 네트워크 외부 디바이스의 리스크를 줄이고 보안을 개선합니다.

문제가 있거나 부적절한 도메인 및 콘텐츠 카테고리에 대한 접속을 차단해 컴플라이언스 및 AUP를 일관성 있고 신속하게 적용합니다.

Akamai Connected Cloud와 Akamai의 통신사급 DNS 플랫폼으로 복원력 및 안정성을 향상합니다

클라우드 기반 관리 포털

Secure Internet Access Enterprise의 설정 및 관리는 클라우드 기반의 Akamai Control Center 포털에서 가능하며 시간과 장소의 제약 없이 솔루션을 관리할 수 있습니다.

정책을 쉽고 빠르게 관리할 수 있고 전세계적으로 정책을 변경하는 데 몇 분밖에 걸리지 않기 때문에 지역에 상관없이 모든 사용자를 보호할 수 있습니다. 보안팀은 중요한 정책 이벤트에 대한 알림을 실시간 이메일로 받아볼 수 있고 보고서도 정기적으로 받을 수 있기 때문에 잠재적인 보안 위협이 발생했을 때 탐지하고 즉각적인 조치를 취할 수 있습니다. 실시간 대시보드는 트래픽, 위협, AUP 이벤트에 대한 정보를 제공합니다. 개별 활동에 대한 자세한 정보 역시 대시보드를 드릴다운해 확인할 수 있습니다. 이 세부 정보는 보안 인시던트를 분석하고 해결하는 데 유용한 리소스를 제공합니다.

모든 포털 기능은 API를 통해 접속 가능하고 데이터 로그는 SIEM으로 내보낼 수 있기 때문에 Secure Internet Access Enterprise는 다른 보안 솔루션 및 리포팅 툴과 효율적으로 간편하게 통합될 수 있습니다.

기능

보안
멀웨어, 랜섬웨어, 피싱 전송 도메인, URL 차단
악성 C2 요청 차단
DNS 기반의 데이터 유출 식별
요청된 HTTP 및 HTTPS URL를 검사하기 위해 위험한 도메인을 프록시로 전달
HTTP 및 HTTPS URL를 검사하기 위해 맞춤형 도메인 목록 생성
고객 트래픽 로그의 룩백 분석을 수행해 새로 발견된 위협을 식별하고 알림
맞춤형 허용/거부 목록 생성
추가적인 위협 인텔리전스 피드 통합
오류 페이지 사용자 지정
Akamai의 위협 데이터베이스 쿼리를 통해 악성 도메인 및 URL에 대한 인텔리전스 확보
외부 네트워크의 디바이스(Windows, macOS, iOS, Android, Chrome)에 보안 적용
AUP(Acceptable Use Policy)
그룹 기반 AUP 정책 생성
내부 및 외부 네트워크 사용자에 대한 AUP 위반 모니터링 및 차단
Google, Bing, YouTube에 SafeSearch 적용

클라우드 접속 보안 브로커(인라인)
섀도우 IT 애플리케이션 식별 및 차단
리스크 점수 또는 애플리케이션 그룹에 따라 애플리케이션 차단
SaaS 테넌트 적용
리포팅, 모니터링, 관리
IDP 및 Active Directory 통합
기업 전반의 모든 활동에 대한 가시성을 제공하는 맞춤형 대시보드
모든 위협 및 AUP 이벤트에 대한 상세 분석
모든 온보딩된 트래픽 요청, 위협, AUP 이벤트에 대한 전체 로깅 및 가시성
모든 로그 전송(로그는 30일 동안 유지되고 API를 통해 내보낼 수 있음)
API를 통해 지원되는 설정, 맞춤형 보안 목록, 이벤트
API를 통해 기타 보안 시스템(SIEM 등)과 통합
이메일로 실시간 보안 알림 전송
일별 또는 주별로 보고서를 이메일로 전송
관리 위임
Akamai Connected Cloud 플랫폼
리커시브 DNS에 대한 고객별 전용 IPv4 및 IPv6
100% 가용성을 보장하는 SLA
최적의 성능을 위한 Anycast DNS 라우팅
보안 강화를 위한 DNSSEC, DoH, DoT 실행
엔터프라이즈 디바이스 속성
인라인 속성(DNS 포워더 사용)
Security Connector를 사용하는 오프라인 속성
노트북 및 모바일 디바이스용 클라이언트 기반 속성(Windows, macOS, iOS, Android, Chrome)

Secure Internet Access Enterprise를 자세히 알아보고 무료 체험을 신청하려면 akamai.com/ko를 확인하시기 바랍니다.

| 2024년 01월 발행