Akamai가 VPN을 제거하고 제로 트러스트 보안 모델을 구현하는 방법

배경

퍼블릭 인터넷과 SaaS 애플리케이션이 널리 사용되고 공격면이 계속 변화하는 상황에서 위치에 따라 애플리케이션 접속을 허용하는 방법은 점차 비효율적인 방법이 되어가고 있습니다. 접속에 대한 요구사항과 데이터 집약적인 현실 또한 네트워크 인프라에 전례 없는 수준의 압박을 가하고 있습니다. 특히 직원들은 장소에 상관 없이 기업 애플리케이션에 빠르고 안정적으로 접속하고 싶어하고 완전한 모빌리티를 기대하고 있기 때문에 기존 솔루션으로는 이런 변화에 대응할 수 없습니다. 기업은 끊임 없이 변화하는 오늘날의 IT 및 비즈니스 환경과 변화하는 요구사항에 맞춰 진화해야 합니다.

비즈니스 상황

Akamai IT 팀은 보안 및 접속에 대해 네트워크 중심으로 접근하는 방식은 기업 자산을 보호하기에 부족하다고 판단했습니다. 기존 VPN은 민감한 데이터에 대한 무단 원격 접속으로 인해 리스크가 증가하고 인증된 디바이스가 기업 네트워크의 모든 애플리케이션에 접속하는 등 보안상의 단점이 존재합니다. 원격 접속에 대한 이러한 접근 방식은 불필요한 보안 리스크를 발생시킵니다. VPN을 통해 일반적으로 개별 사용자가 다른 모든 사용자들이 접속할 수 있는 애플리케이션에 접속하기 때문입니다.

Akamai에서는 전통적인 기업 VPN을 제거하고 경계 기반의 보안 모델에서 벗어난 제로 트러스트 보안 전략을 채택하기로 결정했습니다. Akamai의 기업용 애플리케이션과 데이터를 보호하고 기업 네트워크의 측면 이동(lateral movement)을 방지하며 사용자 경험을 개선하기 위해서였습니다.

Akamai의 기업용 애플리케이션과 데이터를 보호하고 기업 네트워크의 측면 이동(lateral movement)을 방지하며 사용자 경험을 개선하기 위해서였습니다.

Akamai의 제로 트러스트 전환의 핵심 원칙은 다음과 같습니다.

- 인터넷이 기업 네트워크로 사용되는 경계 없는 환경으로의 전환
- 모든 사무실이 Wi-Fi 핫스팟으로 변화
- ID는 물론 위치, 시간대 등의 환경적 요인과 클라이언트 인증서 또는 디바이스의 기업 보안 정책 준수 등의 디바이스 시그널을 기반으로 상황에 따라 동적으로 애플리케이션 접속 권한 부여

Akamai IT 팀은 제로 트러스트 원칙에 맞춰 모든 시스템이나 사용자를 기본적으로 신뢰하지 않도록 보안 가이드라인을 업데이트했습니다. 모빌리티, 보안 강화, 유연한 접속, 가상화를 지원하는 동시에 클라우드의 간소함을 활용하고 비용 효율적인 기술을 찾는 것이 이 접근 방식의 핵심이었습니다.

도전과제

- **분산된 인력**
  정규직, 계약직, 파트너 등 전 세계에 분산된 다양한 형태의 Akamai 직원들이 애플리케이션에 원활하게 접속할 수 있도록 해야 했습니다.
- **모바일 디바이스**
  기업용 애플리케이션에 접속하는 디바이스가 증가하고 디바이스 종류 역시 다양해지고 있었습니다.
- **인수합병**
  새로 인수합병한 기업의 직원들에게 기업용 애플리케이션 접속을 제공하면서 복잡성이 커지고 비용이 증가했습니다.
- **다양한 애플리케이션**
  애플리케이션 종류(온프레미스, IaaS, SaaS)에 상관 없이 공격으로 인한 비즈니스 중단 및 데이터 손실을 막는 것이 중요했습니다.
- **헬프데스크 티켓**
  Akamai의 IT 인력이 내부 애플리케이션에 대한 원격, 계약직, 파트너 접속과 관련된 문제 해결에 사용하는 시간이 증가하고 있었습니다.
- **아키텍처 관리**
  디바이스의 다양성과 라스트 마일 링크의 수·크기 증가로 인해 네트워크 복잡성과 비용이 증가했고 관리 요구사항이 많아졌으며 애플리케이션 성능에 부정적인 영향을 미쳤습니다.
- **지연 시간**
  기존 아키텍처 및 VPN 접속으로 인해 애플리케이션 접속 속도와 일관성이 떨어졌습니다.

솔루션

Akamai IT 팀은 VPN을 제거하고 Enterprise Application Access(EAA)를 도입하기로 결정했습니다. EAA는 클라우드 기반의 접속 솔루션입니다. 방화벽 뒷편의 애플리케이션에 대한 다이얼 아웃 전용 접속을 통해 기업 네트워크를 안전하게 보호합니다. Akamai 기술을 통해 애플리케이션이 호스팅되는 위치(온프레미스, IaaS, SaaS)에 상관 없이 오직 애플리케이션 수준의 자격, ID, 인증, 권한 확인을 기반으로 애플리케이션 접속이 이루어집니다. Akamai는 애플리케이션별 접속 및 제어에 EAA를 사용한 결과, IT·보안 팀을 포함한 전체 직원의 민첩성과 편의성이 향상되었고 사용자 경험이 개선되었습니다.

애플리케이션이 호스팅되는 위치(온프레미스, IaaS, SaaS)에 상관 없이 오직 각 애플리케이션 수준의 자격, ID, 인증, 권한 확인을 기반으로 접속이 이루어집니다.

Akamai IT 팀은 보안을 강화하기 위해 Akamai의 웹 애플리케이션 방화벽인 Kona Site Defender를 EAA와 함께 사용하여 예전에는 '신뢰'했던 호스트를 통한 SQL 인젝션 공격 및 기타 내부자 위협으로부터 내부 애플리케이션을 보호하고 있습니다. 또한 이를 통해 리스크를 줄이고 Akamai의 전반적인 보안 수준도 강화했습니다. Akamai IT 팀은 EAA를 Akamai의 성능 최적화 엔진인 Ion과 함께 사용한 결과, 디바이스, 네트워크, 지리적 위치에 상관 없이 최종 사용자에게 우수한 웹 애플리케이션 경험을 제공할 수 있었습니다.

Akamai의 접근 방식은 일반적으로 애플리케이션 접속 보안과 관련된 비용과 복잡성을 감소시켰습니다. 기업 네트워크에 원격으로 접속하는 다양한 엔드포인트의 접속을 통제하거나 제한하는 대신 IT 팀에서 사용자에게 실제로 필요한 애플리케이션에 대한 접속만 모니터링하고 제어할 수 있는 솔루션이 Akamai에게 더 합리적인 선택이었습니다. VPN과 기업 네트워크 대신 제로 트러스트 접근 방식을 사용하여 모든 트래픽(사용자, 디바이스, 위치, 애플리케이션 등)에 대한 가시성과 컨텍스트를 확보해 리스크를 크게 줄였을 뿐만 아니라 기업 애플리케이션 배포 프로세스도 간소화했습니다.

동적 접속 결정을 위한 디바이스 포스쳐(posture) 역시 Akamai가 제로 트러스트 모델로 전환할 때 중요한 요소입니다. 디바이스 포스쳐는 추가 컨텍스트와 시그널을 제공해 동적 애플리케이션 접속 결정을 뒷받침하고 기존 인증, 권한 확인, 접속 제어 룰, 리포팅 기능을 보완하고 향상합니다.

제로 트러스트를 향한 Akamai의 노력

2000년대

네트워크 및 애플리케이션 제어

- 모두를 위한 클라이언트 인증서
- 네트워크 dot1x - 2FA
- 통합 인증 – SAML
- 내부 무선 없음
- 배스천 관리 호스트
- 아웃바운드 인터넷 없음(디폴트)

2011년

기존 Akamai 솔루션 사용

- Akamai IT 팀에서 만든 솔루션을 통해 외부에서 사용할 수 있는 애플리케이션(인바운드 프록시)
- Global Traffic Management (인텔리전트 트래픽 매니저)
- Site Shield (애플리케이션 오리진에 직접 접속하지 못하도록 제한)

2016년

사용자 비밀번호 제거

- 2FA에서 인증 및 푸시 MFA 로 발전
- 비밀번호 대부분 제거
- Enterprise Application Access(써드파티 접속)

2017년

Akamai 엔터프라이즈 보안 솔루션 도입

- EAA로 자체 Akamai IT 솔루션 제거
- Enterprise Threat Protector(DNS 기반 위협 방어)

현재

제로 트러스트

- EAA 및 ETP 클라이언트를 수천 명의 내부 사용자에게 성공적으로 배포
- EAA와 Ion(성능 최적화)을 수백 개의 애플리케이션에 활성화
- EAA에 디바이스 포스쳐 기능 활성화
- Kona Site Defender (웹 애플리케이션 방화벽)
- Bot Manager(봇 방어)

제로 트러스트 보안 모델로 전환할 때 얻을 수 있는 비즈니스 혜택

- 전체 기업 네트워크 접속이 아닌 필요한 애플리케이션에만 접속을 제공하여 리스크 최소화
- VPN 트래픽을 중앙 데이터센터로 백홀하는 등 기존 기술과 관련된 네트워크 복잡성 제거
- Akamai와 써드파티 직원의 접속을 간소화함으로써 생산성 제고
- 새로 인수합병한 기업의 직원에게 접속 권한을 제공할 때 발생하는 IT 어플라이언스 및 프로세스 오버헤드의 감소
- 워크로드, 네트워크, 사용자, 디바이스에 대한 자동화, 오케스트레이션, 가시성, 분석을 지원하여 데이터 보호
- 빠르고 안정적인 애플리케이션 전송을 통해 모바일을 포함한 여러 디바이스의 사용자 경험 향상
- IT 리소스의 효율적인 할당을 통한 비용 절감과 하드웨어 및 소프트웨어의 업데이트, 관리, 유지에 소요되는 시간을 줄여 전략적 요구사항에 더 많은 시간을 투자
- 애플리케이션 접속과 관련된 헬프데스크 요청 감소

제로 트러스트 보안 모델로의 전환에 대한 자세한 내용을 확인하려면 **akamai.com/zerotrust**를 방문하시기 바랍니다. 보안 모델 전환에 대한 구체적인 계획은 **Akamai 전문가에게 문의** 하시기 바랍니다.

Enterprise Defender란?

Enterprise Defender는 Akamai Intelligent Edge Platform을 기반으로 모든 기업용 애플리케이션과 사용자를 안전하게 보호합니다. 성능 저하 없이 보안을 최적화하고 복잡성을 감소시킵니다. 기업이 제어하는 애플리케이션에 안전하게 접속할 수 있도록 하고 기업이 제어하지 않는 애플리케이션에 사용자가 접속할 때 발생하는 리스크를 경감시킵니다.

Enterprise Defender의 주요 기능은 다음과 같습니다. 사용자별, 월별로 사용이 가능한 편의성이 높은 서비스입니다.

멀웨어 방어: Akamai의 Secure Internet Gateway(SIG)는 멀웨어, 랜섬웨어, 피싱, DNS 데이터 유출, 정교한 제로데이 공격 등 다양한 표적 위협을 선제적으로 탐지, 차단, 방어합니다.

안전한 애플리케이션 접속: Akamai는 권한이 부여된 사용자 및 디바이스가 전체 네트워크가 아닌, 필요한 기업 애플리케이션에만 접속하도록 허용합니다.

Web Application Firewall: Akamai는 가장 규모가 크고 정교한 DDoS 및 웹 애플리케이션 공격으로부터 중요한 웹 애플리케이션을 안전하게 보호합니다.

Enterprise Defender는 멀웨어 차단, 탄력적인 애플리케이션 접속, 보안, 가속을 하나로 결합한 사용 편의성이 높은 보안 서비스입니다.

애플리케이션 가속: Akamai는 비용 효율적인 방식으로 애플리케이션을 빠르고 안정적이며 안전하게 전송합니다. 사용자, 클라우드, 온프레미스 워크로드와 더 가까운 엣지에 애플리케이션 전송 기능을 배치하여 전 세계 모든 곳에 애플리케이션을 제공할 수 있습니다.

Akamai

Akamai는 전 세계 주요 기업들에게 안전하고 쾌적한 디지털 경험을 제공합니다. Akamai의 Intelligent Edge Platform은 기업과 클라우드 등 모든 곳으로 확장하고 있고 고객의 비즈니스가 빠르고, 스마트하며, 안전하게 운영될 수 있도록 지원합니다. 대표적인 글로벌 기업들은 Akamai 솔루션을 통해 멀티 클라우드 아키텍처를 강화하고 경쟁 우위를 확보하고 있습니다. Akamai는 가장 가까운 곳에서 사용자에게 의사 결정, 앱, 경험을 제공하고 공격과 위협을 먼 곳에서 차단합니다. Akamai 포트폴리오는 엣지 보안, 웹·모바일 성능, 엔터프라이즈 접속, 비디오 전송 솔루션으로 구성되어 있고 우수한 고객 서비스, 애널리틱스, 24시간 연중무휴 모니터링 서비스를 제공합니다. 대표적인 기업과 기관에서 Akamai를 신뢰하는 이유를 알아보려면 Akamai 홈페이지(www.akamai.com) 또는 블로그(blogs.akamai.com)를 방문하거나 Twitter에서 @Akamai를 팔로우하시기 바랍니다. 전 세계 Akamai 연락처 정보는 www.akamai.com/locations에서 확인할 수 있습니다. Akamai 코리아는 서울시 강남구 강남대로 382 메리츠타워 21층에 위치해 있으며 대표전화는 02-2193-7200입니다. 2019년 7월 발행.