AKAMAI 솔루션 설명서

엔드투엔드 제로 트러스트를 통한 간소화 및 보안

제로 트러스트는 사용자, 디바이스, 네트워크, 데이터, 애플리케이션 전반에 걸친 묵시적 신뢰를 제거해 기업을 안전하게 보호하는 전략적인 사이버 보안 접근 방식입니다. 제로 트러스트 접근 방식은 기업 방화벽 뒤의 모든 것이 안전하다고 가정하는 대신, 언제든지 유출을 가정하고 요청의 발생 위치에 관계없이 모든 요청에 최소 권한 접속을 적용합니다.

지금 제로 트러스트가 중요한 이유

제로 트러스트는 끊임없이 변화하는 오늘날의 환경에 보다 효과적으로 적응해야 하는 기업에 가장 중요한 요소가 됐습니다. 이러한 기업은 하이브리드 인력을 수용하고 위치에 관계없이 사용자, 디바이스, 앱을 보호하는 새로운 보안 모델을 찾고 있습니다.

최신 제로 트러스트 아키텍처의 원칙

- 항상 맥락에 맞게 명시적으로 확인
- 명시적으로 최소 권한 적용
- 지속적으로 모니터링

통합은 필수

통합된 엔드투엔드 접근 방식

제로 트러스트에 대한 종합적 접근 방식은 ID, 네트워크, 애플리케이션을 포함한 모든 기업의 개체까지 확장돼야 합니다. 제로 트러스트는 엔드투엔드 전략의 역할을 하기 때문에 모든 요소에 걸쳐 통합이 필요합니다. 느슨하게 통합된 여러 포인트 솔루션을 사용하는 것은 이 전략적 접근 방식과 맞지 않습니다.

Akamai는 종합적이고 견고한 포트폴리오를 형성해 오늘날의 기업에 필수적인 모든 제로 트러스트 솔루션을 제공합니다. 여러 보안 제품을 설치, 실행, 수정하는 대신 필요한 모든 기술을 제공하는 단일 벤더사에 의존해 비용을 절감하고 운영 효율성을 높일 수 있습니다.

솔루션 간 신호 공유

Akamai는 제로 트러스트 포트폴리오 전반에 자동화 기능을 내장해 복잡성과 맞춤형에 대한 필요를 크게 줄였습니다. 이렇게 하면 포트폴리오 제품이 모든 제품에서 위협 지식을 공유할 수 있으므로 제품별 보안이 더욱 강화됩니다. 한 제품이 위협을 확인하면 다른 제품이 알림을 받고 위협을 방어할 수 있습니다.

장점

- **분산된 인력**
  사용자가 언제 어디서나 모든 디바이스에서 더 안전하게 일할 수 있도록 지원
- **클라우드 전환**
  클라우드 및 하이브리드 클라우드 환경 전반에서 안전한 접속 제어 제공
- **리스크 방어**
  위협을 차단하고 랜섬웨어와 기타 종류의 멀웨어의 측면 이동 최소화
- **컴플라이언스**
  민감한 데이터 주변의 마이크로 경계에 컴플라이언스 지원

Akamai

종합적 엔드투엔드 포트폴리오: 사용자, 애플리케이션, 네트워크

워크로드 보안

Akamai Guardicore Segmentation: 애플리케이션에 대한 제로 트러스트

Akamai Segmentation은 랜섬웨어와 기타 멀웨어의 확산을 제한하도록 설계된 업계 최고의 마이크로세그멘테이션 솔루션을 제공합니다. 이 제품은 워크로드, 프로세스, 애플리케이션에 대한 가시성과 이해를 제공하는 것은 물론 접속 정책을 적용합니다.

네트워크 보안

Enterprise Application Access: 제로 트러스트 네트워크 접속

Akamai의 제로 트러스트 네트워크 접속 기술은 기존의 VPN 기술을 대체해 사용자 ID를 강화하기 위해 설계됐습니다. Enterprise Application Access는 전체 네트워크를 위험에 빠뜨리지 않고 사용자가 업무를 하기 위해 접속해야 하는 특정 애플리케이션에 따라 사용자 접속을 허용합니다. Enterprise Application Access 기능은 사용자 ID에 대한 가시성을 제공하고 신원 확인과 인증을 강력하게 적용합니다.

사용자 보안

Secure Internet Access: 제로 트러스트 인터넷 접속

Secure Internet Access는 클라우드 기반의 보안 웹 게이트웨이입니다. Secure Internet Access는 사용자가 만들어내는 모든 웹 요청을 검사하고 실시간 위협 인텔리전스와 고급 멀웨어 분석 기술을 제공해 안전한 콘텐츠만 전송될 수 있도록 합니다. 악성 요청과 콘텐츠가 선제적으로 차단됩니다.

멀티팩터 인증: 강력한 제로 트러스트 ID

Akamai MFA는 피싱과 기타 중간 시스템 공격으로부터 직원 계정을 보호합니다. 강력하게 인증된 직원만 자신이 소유한 계정에 접속할 수 있고, 다른 접속이 거부되며, 직원 계정 탈취가 차단됩니다.

추적 및 모니터링

Hunt: 보안 서비스

Akamai의 엘리트 보안 위협 헌팅팀은 '항상 유출 상태를 가정'하는 접근방식을 도입함으로써, 종종 표준 보안 솔루션을 벗어나는 비정상적인 공격 행동, 최신 위협을 지속적으로 탐지합니다. Akamai의 보안 위협 헌팅팀은 네트워크에서 탐지된 중요한 인시던트를 즉시 고객에게 통보한 후 고객의 팀과 긴밀하게 협력해 문제를 해결합니다.

Akamai의 경쟁력

Akamai는 다른 제로 트러스트 벤더사와 차별화되는 몇 가지 장점을 제공합니다. Akamai는 레거시 및 최신, Windows 및 Linux, 온프레미스 및 가상화, 컨테이너 등의 가장 광범위한 영역을 포함합니다. 사용자는 우수한 가시성 기능을 통해 각 워크로드가 어떤 작업을 수행하고 있는지 완벽하게 파악할 수 있습니다. 그리고 Akamai의 사내 엘리트 위협 헌팅 서비스는 보안팀의 기능을 확장해 기업이 위협과 사이버 공격보다 앞서나갈 수 있게 지원합니다.

제로 트러스트에 관한 내용과 시작하는 방법을 자세히 알아보려면 akamai.com을 방문하세요.

 | 지원 | 2022년 6월 발행