Akamai

백서

Akamai와 함께 제로 트러스트 성숙도 달성

연방 기관 및 부서를 위한
CISA의 교차 기능 지원

서론

제로 트러스트 보안은 민감한 정부 데이터, 핵심 인프라, 국가 안보 시스템을 보호하는 데 있어 중요한 기준이 되었습니다. 연방 기관 및 부처는 최신 위협에 대응하기 위해 더 이상 기존의 경계 기반 보안 모델에 의존할 수 없습니다. 사이버 범죄자들이 인증정보 도용, 랜섬웨어, 내부자 공격 등 최신 기법을 활용해 더욱 정교해짐에 따라, 연방 기관들은 보안 체계를 제로 트러스트 프레임워크로 전환하고 있습니다. 그러나 이러한 변화는 단절되어 있으며 연방 시스템을 보호하기 위한 더 많은 노력이 필요합니다.

CISA(Cybersecurity and Infrastructure Security Agency)의 제로 트러스트 성숙도 모델은 연방 기관 및 부처가 암묵적인 신뢰를 제거하고 엄격한 검증 메커니즘을 적용하는 보안 원칙을 구축하는 데 도움을 줄 수 있습니다. 이 모델은 ID, 디바이스, 네트워크, 애플리케이션 및 워크로드, 데이터의 5가지 핵심 축을 기반으로 구성되어 있습니다. 또한, 가시성 및 애널리틱스, 자동화 및 오케스트레이션, 거버넌스라는 세 가지 교차 기능은 사이버 보안에 대한 종합적이고 일관된 접근 방식을 보장합니다.

이러한 목표를 달성하기 위해 마이크로세그멘테이션은 제로 트러스트 보안의 핵심 원칙으로 고려되어야 하며, 내부(동서 방향) 네트워크 방어의 기본 구성요소로 기능합니다. 워크로드를 세그멘테이션하고 측면 이동을 제한함으로써 연방 기관은 잠재적인 유출을 차단하고 제로 트러스트 정책을 적용할 수 있습니다. 또한, 외부(남북 방향) 통신을 보호하기 위한 포괄적인 API(Application Programming Interface) 보안 솔루션을 구축해 정부 애플리케이션에 접근할 수 있는 권한이 있는 엔티티만 접속할 수 있게 해야 합니다.

이 백서는 제로 트러스트 성숙도를 달성하기 위한 필수 단계를 탐구하며, Akamai의 고급 보안 솔루션(Akamai Guardicore Segmentation, Akamai API Security, Akamai Enterprise Application Access)이 연방 기관 및 부서가 CISA의 지침을 준수하고 사이버 보안 체계를 강화하는 데 어떻게 기여하는지 집중 조명합니다.

경계 기반 보안에서 제로 트러스트로의 전환

기존의 사이버 보안은 경계 기반 방어를 기반으로 하며, 네트워크 내부에 있는 엔티티는 신뢰할 수 있다고 가정했습니다. 그러나 이 모델은 오늘날의 사이버 위협 앞에서 거듭 실패했습니다. 공격자는 약한 인증정보와 잘못된 보안 설정을 악용하고 측면 이동 기술을 사용해 기존의 방어를 우회하고 민감한 정보에 접근합니다.

제로 트러스트는 사용자, 디바이스, 애플리케이션, 네트워크 트래픽에 대한 지속적인 검증으로 암묵적인 신뢰를 제거합니다. 모든 접속 요청은 실시간 리스크 평가를 기반으로 인증, 권한 확인, 지속적인 모니터링을 거칩니다. 이 접근 방식은 공격 표면을 극적으로 줄이고 공격자가 네트워크의 일부에 침투하더라도 무단 접속을 차단할 수 있습니다.

CISA의 제로 트러스트 성숙도 모델

CISA의 제로 트러스트 성숙도 모델은 연방 기관 및 부서가 보안 프레임워크를 단계적으로 강화하기 위한 로드맵을 제공합니다(그림). 이 모델은 다음 5가지 핵심 필러를 기반으로 구축되었습니다.

- **ID:** 강력한 인증, 권한 확인, 접속 제어를 통해 정상 사용자만 민감한 리소스와 상호작용할 수 있도록 제한
- **디바이스:** 정부 네트워크에 접속하기 전에 엔드포인트 디바이스가 보안 정책을 준수하는지 모니터링, 보호, 검증
- **네트워크:** 마이크로세그멘테이션 및 최신 접속 제어 정책을 구축해 무단 측면 이동 방지
- **애플리케이션 및 워크로드:** 엄격한 ID 기반 접속 정책, 런타임 보안, API 보안 제어 등을 통해 애플리케이션 및 워크로드 보호
- **데이터:** 민감한 정부 데이터를 암호화, 모니터링하고 무단 접속 및 유출로부터 보호

CISA의 제로필러 트러스트 성숙도 모델(출처: CISA)

이 필러 외에도 제로 트러스트 성숙도 모델은 모든 제로 트러스트 구성요소에 적용되는 세 가지 핵심 교차 기능을 통합합니다.

- **가시성 및 애널리틱스:** 실시간 위협 탐지 및 방어를 위한 지속적인 모니터링, 로깅, 비정상 탐지
- **자동화 및 오케스트레이션:** 정책 적용, 위협 대응, 접속 제어 간소화를 위한 AI 기반 보안 자동화
- **거버넌스:** FISMA(Federal Information Security Modernization Act) 및 NIST(National Institute of Standards and Technology) 특별 간행물 800-207 같은 연방 규정을 준수하기 위한 중앙화된 정책 적용

마이크로세그멘테이션 및 API 보안의 중요성

기존의 네트워크 보안 모델에서는 네트워크 기반 방화벽을 사용해 네트워크를 광범위한 세그먼트로 나누는 것이 일반적입니다. 이 접근 방식은 일정 수준의 보안을 제공하지만 오늘날의 분산된 환경을 완전히 보호하기 위해 필요한 정밀한 제어 기능을 갖추지 못합니다. 연방 환경에서 네트워크 기반 세그멘테이션은 일반적으로 과도한 리소스 할당을 초래합니다. 즉, 사용자와 애플리케이션이 실제로 필요한 것보다 더 많은 리소스에 접속할 수 있게 됩니다. 이로 인해 의도치 않았던 측면 이동의 기회가 만들어집니다. 공격자는 네트워크의 한 부분을 감염시키면 별다른 저항 없이 더 민감한 영역으로 이동할 수 있습니다.

마이크로세그멘테이션은 네트워크 내 동서 방향 트래픽에 대한 세분화된 제어를 도입해 이 문제를 해결합니다. 마이크로세그멘테이션 환경에서 각 애플리케이션, 워크로드 또는 서비스는 서로 격리되며 접속은 특정 정책에 따라 제한됩니다. 따라서 사용자, 디바이스, 애플리케이션은 명시적으로 권한이 부여된 리소스에만 통신할 수 있습니다. 마이크로세그멘테이션은 ID 기반, 애플리케이션 인식 세그멘테이션을 구축함으로써 사이버 공격으로 인한 잠재적 피해를 제한하고, 공격 표면을 줄이고, 제로 트러스트 원칙을 적용합니다.

남북 네트워크 트래픽의 경우, 연방 네트워크는 시스템 간 통신을 촉진하기 위해 API에 점차 더 많이 의존하고 있습니다. 결과적으로 API 엔드포인트를 최우선으로 보호해야 합니다. API 공격(인젝션 공격, 크리덴셜 스터핑, 무단 데이터 접속 등)이 최근 몇 년간 급격히 증가했습니다. 연방 기관 및 부서는 API의 전체 라이프사이클을 보호하는 포괄적인 API 보안 솔루션을 확보해 보안 담당자가 API 트래픽을 실시간으로 탐지하고, 모니터링하고, 보호할 수 있도록 해야 합니다. API 발견이 특히 중요합니다. 알려지지 않은 API가 존재하는 경우가 흔하기 때문입니다.

Akamai 제로 트러스트 솔루션 개요

ID

Akamai MFA는 피싱 및 기타 중간자 공격으로부터 직원 계정을 보호하는 키리스 FIDO2 ID 인증 솔루션입니다. 강력한 ID 기반 인증을 통해 해당 계정을 소유한 직원만 접속할 수 있도록 보장합니다. 기타 접속을 차단해 직원 계정 탈취를 방지합니다.

디바이스

Akamai Guardicore Segmentation은 랜섬웨어 및 기타 멀웨어의 동서 확산을 제한하도록 설계된 업계를 선도하는 마이크로세그멘테이션 솔루션입니다. Akamai Guardicore Segmentation은 디바이스에 대한 정책을 지속적으로 모니터링하고 적용함으로써, 디바이스 설정, 소프트웨어 설치, 잠재적 취약점을 검증해 규정을 준수하는 디바이스만 네트워크에 접속할 수 있도록 합니다. 또한 에이전트 없이 IoT 디바이스를 보호하는 에이전트리스 접근 방식을 지원합니다.

Akamai Enterprise Application Access는 인증된 사용자 및 디바이스만 애플리케이션에 접속할 수 있도록 보장하는 포괄적인 제로 트러스트 네트워크 접속 솔루션입니다. Enterprise Application Access는 디바이스의 ID 및 상태를 검증해 Akamai Guardicore Segmentation의 기능을 보완합니다. 디바이스가 규정을 준수하지 않거나 보안 리스크를 초래하는 경우 Enterprise Application Access는 해당 디바이스가 민감한 애플리케이션에 접속하는 것을 제한할 수 있습니다.

네트워크

Akamai API Security는 지속적인 탐색과 실시간 분석을 통해 남북 트래픽을 모니터링함으로써 연방 보안 전문가에게 전체 API 환경에 대한 포괄적인 가시성을 제공합니다. 알려지지 않은 API를 탐지하고, 취약점을 식별하고, API 행동을 분석해 보안팀이 빠르게 성장하는 공격 표면에서 공격을 탐지하고 리스크를 방어할 수 있도록 지원합니다.

Akamai App & API Protector는 웹 애플리케이션 방화벽, 봇 방어, API 보안, 레이어 7 DDoS(Distributed denial-of-Service) 방어 기능을 하나의 솔루션으로 통합합니다. 전체 네트워크 및 API 환경 전반에서 취약점을 신속하게 식별하고 위협을 방어합니다.

Akamai Secure Internet Access Enterprise는 클라우드 기반 보안 DNS(Domain Name Service)로써 다른 보안 솔루션과 관련된 복잡성과 관리 부담 없이 사용자와 디바이스가 어디에 있든 안전하게 인터넷에 연결되도록 보장합니다.

Akamai Guardicore Segmentation은 네트워크 트래픽에 대해 정밀 제어를 제공해 정상적인 트래픽만 허용합니다.

Akamai 제로 트러스트 솔루션 개요

애플리케이션 및 워크로드

Akamai Enterprise Application Access는 위치에 관계없이 직원, 써드파티 계약자, 파트너, 모바일 사용자 등에 제로 트러스트 접속을 제공합니다.

Akamai Guardicore Segmentation은 애플리케이션 및 워크로드에 대한 가시성과 이해를 제공합니다.

데이터

Akamai Secure Internet Access Enterprise는 콘텐츠 필터링, 최신 위협 방어, 데이터 손실 방지 등과 같은 기능을 통해 데이터에 대한 안전한 접속을 제공합니다. 무단 접속 및 데이터 유출을 방지해 데이터 인벤토리 관리를 지원합니다.

Akamai Guardicore Segmentation: 동서 트래픽 보호의 핵심

Akamai Guardicore Segmentation은 특히 연방 기관 및 부서를 포함한 기업이 온프레미스 및 클라우드 환경 전반에 걸쳐 정밀한 보안 제어를 구축하도록 설계된 선도적인 마이크로세그멘테이션 솔루션입니다.

워크로드 및 애플리케이션의 정밀한 세그멘테이션

기존의 세그멘테이션은 네트워크 수준에서 접속을 제어하지만, Akamai Guardicore Segmentation은 애플리케이션 및 워크로드 수준에서 보안 정책을 적용합니다. 이를 통해 접속이 엄격히 제한됩니다. 예를 들어, 연방 기관에서 HR(Human Resource) 애플리케이션은 지정된 HR 데이터베이스와 통신하도록 제한되어, 유출 발생 시 공격자가 측면 이동을 시도할 수 없습니다.

ID 기반 마이크로세그멘테이션

Akamai Guardicore Segmentation은 IP 주소가 아닌 사용자 및 디바이스 ID을 기반으로 세그멘테이션을 적용합니다. 따라서 업무, 신뢰 수준, 실시간 검증에 따라 접속이 동적으로 부여됩니다. 예를 들어, 계약업체 및 써드파티 파트너를 필요한 시스템에만 접속할 수 있도록 제한해 무단 접속 리스크를 줄일 수 있습니다.

동적 정책 적용

Akamai Guardicore Segmentation은 사용자 행동, 디바이스 상태, 네트워크 활동과 같은 실시간 요소에 따라 보안 정책을 지속적으로 조정합니다. 비정상적인 데이터 전송량 같은 의심스러운 활동이 탐지되면 Akamai Guardicore Segmentation은 자동으로 접속을 제한하거나, 트래픽을 차단하거나, 보안팀에 알림을 제공합니다. 이러한 사전 예방적 접근 방식은 보안 정책이 새로운 위협에 대응할 수 있도록 합니다.

기업은 Akamai Guardicore Segmentation의 마이크로세그멘테이션을 통합하면 제로 트러스트 아키텍처를 강화하고, 리스크를 최소화하고, 네트워크에 대한 엄격한 접속 제어를 유지할 수 있습니다.

사례 연구

연방 환경의 Akamai Guardicore Segmentation

한 연방 기관은 내부 시스템을 측면 이동 공격으로부터 보호하기 위해 Akamai의 마이크로세그멘테이션 솔루션을 도입했습니다. 해당 기관은 Akamai Guardicore Segmentation을 도입하기 전에 기존의 네트워크 기반 세그멘테이션을 사용해 제한된 세그멘테이션 수준을 제공했고 서로 다른 네트워크 세그먼트 간 광범위한 접속을 허용했습니다. 이로 인해 네트워크의 어느 부분이 감염될 경우 측면 이동의 심각한 리스크가 발생했습니다.

Akamai Guardicore Segmentation을 통해 기관이 얻은 장점:

- 정밀한 세그멘테이션 구축: 애플리케이션 수준에서 워크로드를 세그멘테이션함으로써 측면 이동 리스크를 줄이고 각 애플리케이션이 필요한 리소스에만 접근할 수 있도록 했습니다.
- 가시성 향상: 솔루션의 시각화 툴로 내부 트래픽에 대해 심층 인사이트를 확보함에 따라 보안팀은 실시간으로 잠재적 위협을 식별하고 방어할 수 있었습니다.
- 보안 강화: 기존 ID 관리 및 접속 제어 시스템과 Akamai Guardicore Segmentation을 통합함으로써 네트워크 전체에 제로 트러스트를 적용하고, 실시간 리스크 평가에 따라 접속을 지속적으로 모니터링하고 동적으로 조정할 수 있었습니다.

이 사례는 Akamai Guardicore Segmentation이 네트워크 보안을 강화하고, 측면 이동 리스크를 줄이고, 항상 권한을 최소한으로 유지하는 데 얼마나 강력한 힘을 발휘하는지 보여줍니다.

API 보안: 남북 트래픽 보호

Akamai는 API 보안을 보장하기 위해 다양한 솔루션을 제공합니다. Akamai의 API 보안 플랫폼은 API 상호작용에 대한 포괄적인 가시성을 제공하고 남북 위협을 실시간으로 자동 탐지 및 방어합니다. 연방 기관 및 부서는 고급 행동 애널리틱스를 통해 다음과 같은 작업을 수행할 수 있습니다.

- 공격자가 악용할 수 있는 **섀도 API 식별**
- **API 트래픽 패턴 모니터링**을 통해 무단 접속 시도 탐지
- **API 비율 제한을 구축**해 악용 및 서비스 거부 공격 방지
- **잊혀진 API, 방치된 API, 알려지지 않은 API 를 식별**해 잠재적인 공격 경로 발견
- 설정이나 종류에 관계없이 **모든 API의 인벤토리 구축**(RESTful, GraphQL, SOAP, XML-RPC, JSON-RPC, gRPC 포함)

Akamai Secure Internet Access Enterprise는 보안팀이 네트워크 안팎의 모든 사용자와 디바이스가 인터넷에 안전하게 접속할 수 있도록 지원하는 클라우드 기반 DNS 방화벽입니다. 멀웨어, 랜섬웨어, 피싱, 처리량이 적은 DNS 데이터 유출을 비롯한 악성 DNS 요청을 사전에 차단합니다. Secure Internet Access Enterprise는 배포, 관리, 업그레이드할 어플라이언스가 없기 때문에 보안 복잡성이 줄어듭니다. 이 솔루션은 사용하기 쉽고 직관적입니다.

Akamai App & API Protector는 Akamai Cloud를 통해 실행되는 앱과 API에 대한 API 위협을 발견 및 방어하고, Akamai API Security에서 발견되지 않은 잠재적인 위협이 포함된 모든 트래픽을 차단합니다. Akamai의 API 보안을 함께 배포하면 API에 대한 포괄적이고 지속적인 가시성을 확보하고 보안팀이 모든 애플리케이션 자산에서 API 보안 문제를 발견, 감사, 탐지, 대응할 수 있습니다.

제로 트러스트와 함께 교차 기능 지원

제로 트러스트 아키텍처의 주요 과제 중 하나는 기술 사일로 생성 리스크입니다. 각 사일로가 독립적으로 운영됨에 따라 분산된 보안 제어, 정책 적용, 위협 탐지 문제가 초래됩니다. 따라서 모든 보안 레이어에 걸쳐 반드시 통합이 이루어져야 합니다.

고도로 민감한 데이터와 복잡한 인프라를 관리하는 연방 기관 및 부서에서 이러한 분산된 접근 방식은 심각한 보안 리스크를 초래할 수 있습니다. 공격자는 사일로(또는 필러) 간의 가시성 부족을 악용하거나 서로 다른 시스템 간 일관되지 않은 정책 적용을 활용할 수 있습니다. 연방 기관은 이러한 리스크를 차단하기 위해 모든 필러에 걸쳐 가시성, 거버넌스, 자동화를 통합하는 통합된 교차 필러 보안 모델을 도입해 일관된 정책 적용을 보장하고 공격자가 악용할 수 있는 간극을 줄여야 합니다.

통합된 보안 모델을 달성하기 위해 교차 필러 통합은 CISA의 제로 트러스트 성숙도 모델의 세 가지 핵심 영역, 즉 가시성 및 애널리틱스, 자동화 및 오케스트레이션, 거버넌스에 초점을 맞춰야 합니다. 이러한 요소는 실시간 리스크 평가에 따라 모든 필러에서 접속 및 권한을 동적으로 조정하는 제로 트러스트 아키텍처를 구축하는 데 필수적입니다.

가시성 및 애널리틱스

가시성은 위협 탐지, 사용자 행동 이해, 모든 필러에 걸친 동적 보안 정책 적용에 필수적입니다. ID, 디바이스, 애플리케이션, 데이터 간의 상호작용에 대한 완전한 가시성 없이는 보안팀이 비정상 행동이나 무단 접속 시도를 탐지하기 어렵습니다. Akamai 솔루션은 포괄적인 교차 필러 가시성을 제공합니다.

- Akamai Guardicore Segmentation은 분할된 워크로드 간의 네트워크 트래픽을 모니터링해 동서 트래픽을 가시화하고 네트워크 내부의 측면 이동 시도를 탐지합니다.
- Enterprise Application Access는 애플리케이션 접속 패턴에 대한 인사이트를 제공해 사용자가 민감한 애플리케이션과 상호작용하는 방식을 추적하고 맥락 데이터에 따라 접속을 동적으로 조정합니다.

연방 기관은 이러한 기능을 통합함으로써 모든 영역의 데이터를 상관 분석하고 보안 이벤트에 대한 통합된 관점을 확보할 수 있습니다. 사용자가 애플리케이션에 접속을 요청하면 Akamai의 솔루션은 사용자의 ID뿐만 아니라 사용 중인 디바이스의 보안, 네트워크 상태, 애플리케이션의 실시간 행동을 확인합니다. 따라서 보안팀은 잠재적 위협을 더 빠르게 탐지하고, 권한 상승 리스크를 최소화하며, 실시간 리스크 평가에 따라 권한을 동적으로 조정할 수 있습니다.

자동화 및 오케스트레이션

여러 시스템에서 인시던트 대응 및 정책 적용은 느리고 수동적인 프로세스가 될 수 있습니다. 제로 트러스트 원칙에 따라 모든 영역에 보안 정책을 동적으로 적용하려면 높은 수준의 자동화 및 오케스트레이션이 필요합니다. 이렇게 하면 리스크 수준이 변경될 때 권한이 즉시 필요한 최소 수준으로 조정되어 인간 오류나 대응 지연의 가능성이 감소합니다. Akamai의 솔루션은 ID, 네트워크, 애플리케이션 보안을 아우르는 자동화된 워크플로우를 제공합니다.

- Akamai Guardicore Segmentation은 실시간 트래픽 패턴과 탐지된 비정상에 따라 네트워크 세그멘테이션 정책을 동적으로 조정하는 자동화된 마이크로세그멘테이션을 제공합니다. 이를 통해 네트워크 내의 의심스러운 활동을 신속하게 격리하고 측면 이동을 방지합니다.
- Enterprise Application Access는 애플리케이션 접속 보안을 자동화해 사용자가 안전한 프록시를 통해 애플리케이션에 접속할 수 있도록 하고 리스크 요인 변화에 따라 권한을 지속적으로 업데이트합니다.

연방 기관 및 부서는 이러한 프로세스를 자동화함으로써 보안 정책을 일관되고 신속하게 적용하고 공격자의 공격 기회를 줄일 수 있습니다.

거버넌스

거버넌스는 모든 보안 전략의 기반이 되며, 정책이 일관되게 적용되고 컴플라이언스 요구사항이 충족되도록 보장합니다. 교차 필러 모델에서 거버넌스는 모든 보안 통제가 제로 트러스트 원칙과 일치하도록 보장해야 합니다. Akamai의 솔루션을 통해 모든 필러를 아우르는 거버넌스 정책을 구축할 수 있습니다.

- ID 거버넌스: ID 기반 접속 통제가 디바이스, 애플리케이션, 네트워크 전반에서 일관되게 적용되도록 보장하고 실시간 리스크 평가에 따라 접속 권한을 정기적으로 검토하고 업데이트합니다.
- 네트워크 거버넌스: 온프레미스, 클라우드, 하이브리드 인프라를 포함한 모든 환경에서 네트워크 세그멘테이션 및 트래픽 모니터링 정책을 적용합니다. 따라서 Akamai Guardicore Segmentation을 통해 네트워크 세그멘테이션 정책을 정의하고 전체 인프라에 일관되게 적용할 수 있습니다.
- 데이터 거버넌스: 민감한 데이터를 보호하기 위해 최소 권한 원칙에 따라 접속을 제한하고, 모든 데이터 전송을 지속적으로 모니터링해 무단 접속이나 의심스러운 활동을 파악합니다.

Akamai의 기술은 연방 기관에 제로 트러스트를 지원하는 완전히 통합된 교차 필러 보안 아키텍처를 제공하기 위해 원활하게 협력하도록 설계되었습니다.

사례 연구

연방 기관의 교차 필러 통합

대규모 연방 기관은 ID, 네트워크, 애플리케이션 레이어에 걸쳐 분산된 보안 정책으로 인해 심각한 문제를 겪었습니다. ID 검증, 애플리케이션 접속, 네트워크 세그멘테이션을 관리하는 시스템이 서로 달랐기 때문에 보안 정책의 일관성이 부족하고 가시성 격차가 발생했습니다.

해당 기관은 Akamai의 통합 솔루션을 도입함으로써 다음과 같은 성과를 달성했습니다.

- **ID 및 애플리케이션 보안 통합:** Akamai의 ICAM(Identity, Credential, and Access Management) 솔루션과 Enterprise Application Access를 통합해 실시간 ID 데이터 기반으로 애플리케이션 접속을 항상 인증할 수 있게 되었습니다. 이를 통해 사용자 행동과 디바이스 상태에 따라 애플리케이션 권한을 동적으로 조정할 수 있게 되었습니다.
- **동적 네트워크 세그멘테이션 적용:** Akamai Guardicore Segmentation을 배포해 ID 및 애플리케이션 접속에 따라 네트워크 트래픽을 분할함으로써 민감한 시스템 간 측면 이동을 방지하고 실시간 리스크 평가에 따라 권한을 지속적으로 업데이트했습니다.
- **가시성 및 자동화 강화:** Akamai의 통합 애널리틱스 및 자동화 툴을 활용해 보안 체계에 대한 전체적인 가시성을 확보하고 모든 영역에서 정책 적용을 자동화했습니다.

그 결과, 공격 표면을 줄이고, 인시던트 대응 시간을 단축하고, 연방 보안 규정을 완전히 준수했습니다. 이 사례는 분산된 보안 아키텍처를 제로 트러스트를 지원하는 통합된 동적 보안 모델로 전환하는 교차 필러 통합의 장점을 보여줍니다.

결론

제로 트러스트 보안은 더 이상 선택 사항이 아닙니다. 연방 기관을 최신 사이버 위협으로부터 보호하기 위한 필수 요소입니다. 연방 기관 및 부서는 마이크로세그멘테이션, API 보안, 강력한 ID 제어 조치를 구축함으로써 연방 사이버 보안 지침을 준수하면서 리스크를 크게 줄일 수 있습니다.

Akamai는 Akamai Guardicore Segmentation, Akamai API Security, Akamai Secure Internet Access Enterprise를 포함한 포괄적인 제로 트러스트 솔루션 포트폴리오를 제공해 기관이 선제적인 적응형 보안 체계를 도입할 수 있도록 지원합니다. 연방 기관은 Akamai의 전문성을 활용해 제로 트러스트 전환을 가속하고 장기적인 보안 안정성을 확보할 수 있습니다.

연방 기관은 지금 행동해야 합니다. Akamai의 보안 솔루션을 통합해 제로 트러스트 성숙도를 달성하고, 사이버 리스크를 방어하고, 국가의 가장 중요한 디지털 자산을 보호할 수 있습니다.

지금 Akamai에 문의해 포괄적인 보안 솔루션에 대해 자세히 알아보세요.

Akamai Security는 성능이나 고객 경험에 영향을 주지 않으면서 모든 상호 작용 지점에서 비즈니스의 원동력이 되는 애플리케이션을 보호합니다. 글로벌 플랫폼의 규모와 위협에 대한 가시성을 활용해 고객과 협력함으로써 위협을 예방, 탐지, 방어하고 브랜드 신뢰를 쌓고 비전을 실현할 수 있도록 지원합니다. Akamai의 클라우드 컴퓨팅, 보안, 콘텐츠 전송 솔루션에 관해 자세히 알아보려면 akamai.com, akamai.com/blog를 확인하거나 X, LinkedIn에서 Akamai Technologies를 팔로우하시기 바랍니다. 04월 25일 발행.