AKAMAI 솔루션 설명서

기밀 컴퓨팅: 사용 중인 데이터 보호

위협의 범위와 규모, 정교함이 계속 증가함에 따라, 일반적으로 보안팀은 데이터를 이동 중에 암호화하고 저장할 때 접속을 제한하는 등의 방식으로 도전과제에 대응해 나가고 있습니다. 하지만 일반적으로 사용 중인 데이터라고 불리는 데이터를 편집, 읽기, 처리되는 중에 보호해야 하는 필요성이 점차 커지고 있습니다.

컴퓨팅이 진화하고 AI가 확산되는 오늘날, 사용 중인 데이터 보호 기술의 격차는 더욱 중요해지고 있습니다. 하이브리드 컴퓨팅과 멀티클라우드 컴퓨팅이 널리 보급되면서 기업이 데이터를 수집하고 저장하는 방법 역시 확대되었습니다. 한편, 기업이 AI를 활용하는 과정에서 많은 데이터 세트(종종 가장 중요하면서도 민감한 데이터)를 암호화 및 보호하지 않은 상태로 사용하고 있습니다.

이러한 리스크 때문에 애플리케이션, 프로세스, 서비스에서 사용되는 민감한 데이터를 암호화 및 보호하는 보안 접근 방식인 기밀 컴퓨팅에 대한 관심이 높아졌습니다.

복잡성을 가중시키는 API

API가 확산되고 있는 이유는 기업이 지속적으로 클라우드 환경 및 서비스와 AI 모델에 리소스를 제공하는 두 가지 영역에서 API가 중요한 역할을 맡고 있기 때문입니다. 클라우드에서 API는 여러 기술이 데이터를 전달하고 공유하는 데 필수적입니다. 대규모 언어 모델(LLM)은 AI를 기반으로 데이터 접속 및 결합에 API를 사용해 언어 이해 및 텍스트 생성 등의 복잡한 작업을 수행합니다.

그러나 아직 보안팀은 애플리케이션 및 인프라만큼 API에 큰 관심을 보이고 있지 않습니다. 공격자들은 이러한 보안 격차를 악용하고 있으며, 지난 12개월 동안 기업의 84%에서 API 보안 인시던트가 발생했습니다.[1] 클라우드 및 AI 관련 API에 사용되는 민감한 데이터를 보호하기 위해 기업은 기밀 컴퓨팅 환경에서 실행되는 포괄적인 API 보안 기능을 갖추어야 합니다.

3개의 도어 모두 잠그기

전송 및 저장 상태의 데이터를 잠가도 여전히 하나의 도어(사용 중인 데이터)가 활짝 열려 있어 기업에 리스크를 초래할 수 있습니다.

기밀 컴퓨팅에서 사용 중인 데이터는 하드웨어 수준에서 신뢰할 수 있는 환경에서 처리됩니다. API를 통해 기업은 퍼블릭 클라우드 API 서비스를 활용하는 대신 API 트래픽을 보호하기 위해 특별히 설계된 전용 머신 러닝 인스턴스를 배포해 공격 표면을 획기적으로 줄일 수 있습니다. 기밀 컴퓨팅 환경에서 API 보안 솔루션을 실행하면 보안을 한층 더 강화할 수 있습니다. 시스템의 일부가 감염되더라도 보호된 환경의 데이터는 안전하게 유지됩니다. 신뢰할 수 있는 환경에서 이러한 데이터에 대한 API 분석을 실행하면 보안이 강화되고 기존 환경에 존재하던 리스크가 사라집니다.

AI, API 보안, 기밀 컴퓨팅을 결합하면 하이퍼바이저, 호스트 운영자, 시스템 인프라 소유자, 물리적 접속 권한이 있는 임의의 사용자와 같이 권한이 없는 사람이 실행 중에 코드나 데이터를 보거나 변경하지 못하도록 차단하고, 내부 위협(신뢰할 수 없는 인프라에서 실행되는 비공식 시스템 관리자나 워크로드)과 외부 위협(취약점을 악용하는 공격자)으로부터 데이터를 보호합니다.

기업이 얻을 수 있는 혜택

데이터 보안 개선
강력한 제어 기능을 통해 사용 중인 데이터에 대한 접속을 제한함으로써 공격 표면을 줄이고 무단 접속으로부터 민감한 API 기반 프로세스 보호

API 보호
민감한 데이터를 암호화된 상태로 유지하면서 API 트래픽에 대한 심층 분석을 통해 모니터링 중 노출 리스크 감소

컴플라이언스 강화
진화하는 엄격한 글로벌 데이터 보호 규정을 준수해 업계 및 정부 표준에 대한 컴플라이언스 확보

1. Akamai, API 보안 영향 연구, 2024년

이점

API 위협이 급증하고 사용 중인 데이터 자체가 매력적인 표적이 되면서 공격자들은 이 리스크를 좌시하지만은 않을 것입니다. 미래 지향적인 기업은 다음과 같이 여러 가지 이유로 기밀 컴퓨팅을 도입하기 시작했습니다.

- 강력한 제어 조치를 통해 먼저 사용 중인 데이터에 대한 접속 제한
- 증가하는 API를 안전하게 분석
- 기밀 컴퓨팅에서 지원하는 제어 기능을 사용해 전 세계에서 새로운 엄격한 데이터 보호 컴플라이언스 요구사항 준수

기밀 컴퓨팅은 온라인 거래를 보호하려는 금융 서비스 기업, 환자 데이터를 보호하는 생명 과학 기업 등 규제가 엄격한 기업에 가장 큰 이점을 제공합니다. 이 접근 방식은 독립 소프트웨어 벤더사(ISV)가 엣지에서 클라우드에 이르는 여러 위치의 고객에게 분산된 AI 모델을 보호하는 데 도움이 될 수 있습니다. 실제로 중요한 데이터에 대해 실시간 분석 처리를 실행하는 모든 IT 대기업은 기밀 컴퓨팅을 고려해야 합니다.

Akamai와 파트너의 지원

효과적인 기밀 컴퓨팅을 위해서는 포괄적인 제어 및 보호를 제공하도록 긴밀하게 협력하는 통합 솔루션 세트가 필요합니다. Akamai는 파트너인 Intel 및 IBM과 함께 하드웨어 수준에서 클라우드, API에 이르기까지 사용 중인 데이터에 대한 보안을 제공합니다.

먼저, Intel® Trust Domain Extensions(TDX)는 다음과 같이 신뢰할 수 있는 실행 환경을 제공합니다.

- 공격자 또는 접속 권한을 가져서는 안되는 사용자로부터 발생하는 외부 침입 차단
- 네트워크, 서버 및 스토리지와 같이 클라우드에서 가상 리소스를 생성하는 데 사용되는 기술을 제어하는 소프트웨어 보안 개선
- 이러한 분산 시스템을 관리하는 사용자와 관련된 필수적인 보안 레이어를 추가해 실수로 인한 리스크와 내부자의 악의적인 활동 가능성 감소

또한 Intel Tiber™ Trust Authority 확인 및 토큰을 통해 기업은 암호화되지 않은 사용 중인 데이터에 대한 접속을 제한하고 관리할 수 있습니다.

Akamai API Security 솔루션은 기업에서 사용되는 API의 인벤토리를 제공하고, 이러한 API의 사용을 모니터링하고 탐지합니다. 트래픽 패턴과 행동을 분석해 악성 API 요청을 자동으로 탐지 및 방지하면서 수동 개입 없이 네트워크 엣지에서 위협을 효과적으로 차단합니다. 이를 통해 데이터 유출, 무단 접속, 로직 남용과 같은 API 공격을 실시간으로 차단할 수 있습니다.

이와 함께 IBM 클라우드 가상 서버의 Intel Xeon® 프로세서와 결합된 Akamai의 원격 머신 러닝 엔진(Intel TDX로 안전하게 보안되고 Intel Tiber Trust Authority로 보증됨)은 AI 기반 봇 공격이든 인간 공격자이든 관계없이 사용 중인 데이터의 최종 단계에서 암호화되지 않은 경우 외부 위협이 데이터에 접속하지 못하도록 설계된 대규모로 확장 가능한 프라이빗 환경을 제공합니다.

사용 중인 데이터에 대한 보안이 필요한 시기

기업은 가장 소중한 기업 데이터를 안전하게 보안하기 위해 신뢰할 수 있는 환경이 필요합니다. 데이터가 저장되고 접속될 때 뿐만 아니라 실제로 사용될 때에도 데이터를 보호해야 합니다. 기업은 포괄적인 보안을 제공하기 위해 Akamai와 파트너의 도움을 받고 있습니다. 신뢰할 수 있는 컴퓨팅 기업들이 협력을 통해 데이터의 라이프사이클의 모든 레이어에 걸쳐 보안을 보장합니다.

기밀 컴퓨팅을 위한 파트너십을 통해 민감한 데이터를 보호하는 방법에 대해 자세히 알아보세요.

Akamai API Security 솔루션에 대해 자세히 알아보세요.