AKAMAI 솔루션 설명서

IBM API Connect, DataPower를 위한 통합 API 보안 및 거버넌스

API의 가능성과 도전 과제

API는 디지털 혁신을 추진하는 원동력으로서 모든 업계 기업이 성장을 가속하기 위해 새로운 서비스와 비즈니스 모델을 창출하도록 지원해 왔습니다. 그러나 API가 확산하면서 이와 관련된 리스크도 증가하고 있습니다.

- 비즈니스 리더와 엔지니어링 리더들이 기업 전반에서 API 사용과 통합을 빠르게 늘려 왔지만, API를 효과적으로 관리하는 능력은 여전히 도전 과제로 남아 있습니다.
- 새로운 애플리케이션과 AI 기반 서비스를 신속하게 구축하고 출시하기 위한 경쟁 속에서 기본 API에 설정 오류, 코딩 오류, 비즈니스 로직 이슈가 매우 빈번하게 발생합니다.
- 고객, 파트너, 벤더사가 기업과 디지털 방식으로 소통할 때마다 데이터의 원활한 교환을 가능하게 하는 API가 그 배후에 존재하는데, 공격자들은 여기에 민감한 데이터가 포함된다는 점을 잘 알고 있습니다.

그 결과, API가 큰 위험을 수반하는 주요 공격 기법으로 부상했습니다. API에 대한 공격은 기업의 매출, 안정성, 규제 컴플라이언스에 심각한 영향을 미칠 수 있습니다.

이 문제를 해결하기 위해 기업은 설계, 개발, 테스트, 배포, 운영, 문제 해결을 포함한 거버넌스와 보안 모두에 대한 전체 수명 주기 접근 방식을 도입해야 합니다. Akamai API Security와 IBM은 기업이 신속하고 자신감 있게 API를 개발, 배포, 관리하도록 지원해 비즈니스에 따라 예측 가능하게 대응하고 확장할 수 있게 합니다.

도전 과제

- 자산 전반에 걸쳐 API 인벤토리 유지, 알려지지 않은 API 파악
- 규정을 준수하지 않거나 잘못 설정되었거나 취약한 API 식별
- 비즈니스 로직 공격을 포함한 API 남용 또는 오용 탐지, 중단
- 속도와 민첩성을 희생하지 않고 안전하고 일관된 API 구축
- API 보안 및 거버넌스 프로그램의 조정 및 감독

Akamai와 IBM이 고객을 지원하는 방법

API 자산 파악

볼 수 없는 공격은 방어할 수도 없습니다. Akamai API Security를 사용하면 API, 도메인, 이슈를 자동으로 파악해 전체 API 자산을 파악할 수 있는 강력한 API 인벤토리를 구축할 수 있으며, 기업은 일반적으로 예상보다 훨씬 더 많은 API를 보유하고 있습니다. 또한 유출된 정보와 같은 악용 가능한 정보를 쉽게 찾아 공격자가 이용할 수 있는 공격 경로를 파악할 수 있으며, API 게이트웨이와 관리 플랫폼에 인접한 가장 일반적인 인프라 구성요소와 원활하게 통합되어 기업 전체에서 보안 데이터를 일관되게 공유할 수 있습니다.

보안 및 거버넌스 체계 강화

API 거버넌스를 위해 Akamai API Security를 사용하면 운영 규모를 확장하고 모범 사례를 적용할 수 있습니다.

- 전체 비즈니스 맥락을 통해 생태계의 모든 API를 이해하고 API 관리 모범 사례에 맞춰 조정
- 개발 팀과 보안 팀 간의 커뮤니케이션 간소화
- 설정 오류부터 정책 위반 API에 이르기까지 취약점 파악
- 민감한 데이터를 보호하고 선제적으로 변경 사항을 모니터링해 API 리스크 축소

런타임 보호를 통해 API 남용과 공격 차단

데이터 유출, 데이터 변조, 데이터 정책 위반, 의심스러운 행동 등을 포함한 엣지에서 코어에 이르는 API 공격을 실시간 트래픽 분석, 대역 외 모니터링, 인라인 문제 해결 옵션, 워크플로우 통합을 통해 탐지하고 차단해 보안관제센터(SOC)의 효율성을 높일 수 있습니다.

Active Testing으로 안전한 API를 더 빠르게 전송

API 보안 테스트를 API 개발의 모든 단계에 원활하게 통합하고, API가 프로덕션 단계로 이동하기 전에 취약점, 설정 오류, 컴플라이언스 문제를 찾아낼 수 있습니다. DevSecOps 담당자는 Active Testing을 통해 필요에 따라 또는 기업 CI/CD 프로세스의 일부로서 200개가 넘는 API 중심 보안 테스트의 포괄적인 세트를 실행할 수 있습니다. Active Testing은 애플리케이션의 기본 비즈니스 로직에 대한 이해를 바탕으로 모든 API를 찾아 테스트하기 때문에 개발자는 다른 테스트 툴을 사용했을 때 놓칠 수 있는 복잡한 취약점을 발견할 수 있습니다.

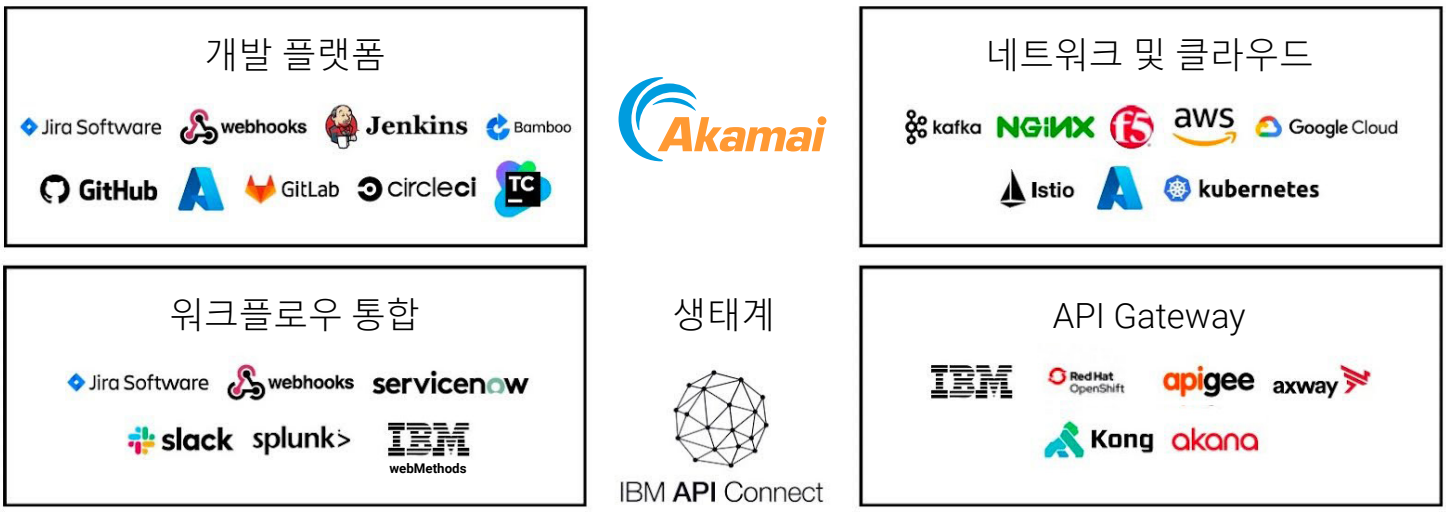
Akamai가 IBM 사용자에게 효율성을 높이는 통합을 통해 가시성과 보안 기능을 제공하는 방법

Akamai API Security는 여러 클라우드 플랫폼과 배포 옵션에서 API Connect와 DataPower 모두에 통합됩니다. 또한 API Connect가 DataPower를 관리할 때 시스템 전반에 일방적인 설정 변경이 이루어져 운영 효율성이 향상되는 동시에 승인되지 않은 개발 활동과 규정을 위반하는 개발 활동의 리스크가 줄어듭니다.

원활한 공격 방향 및 대응

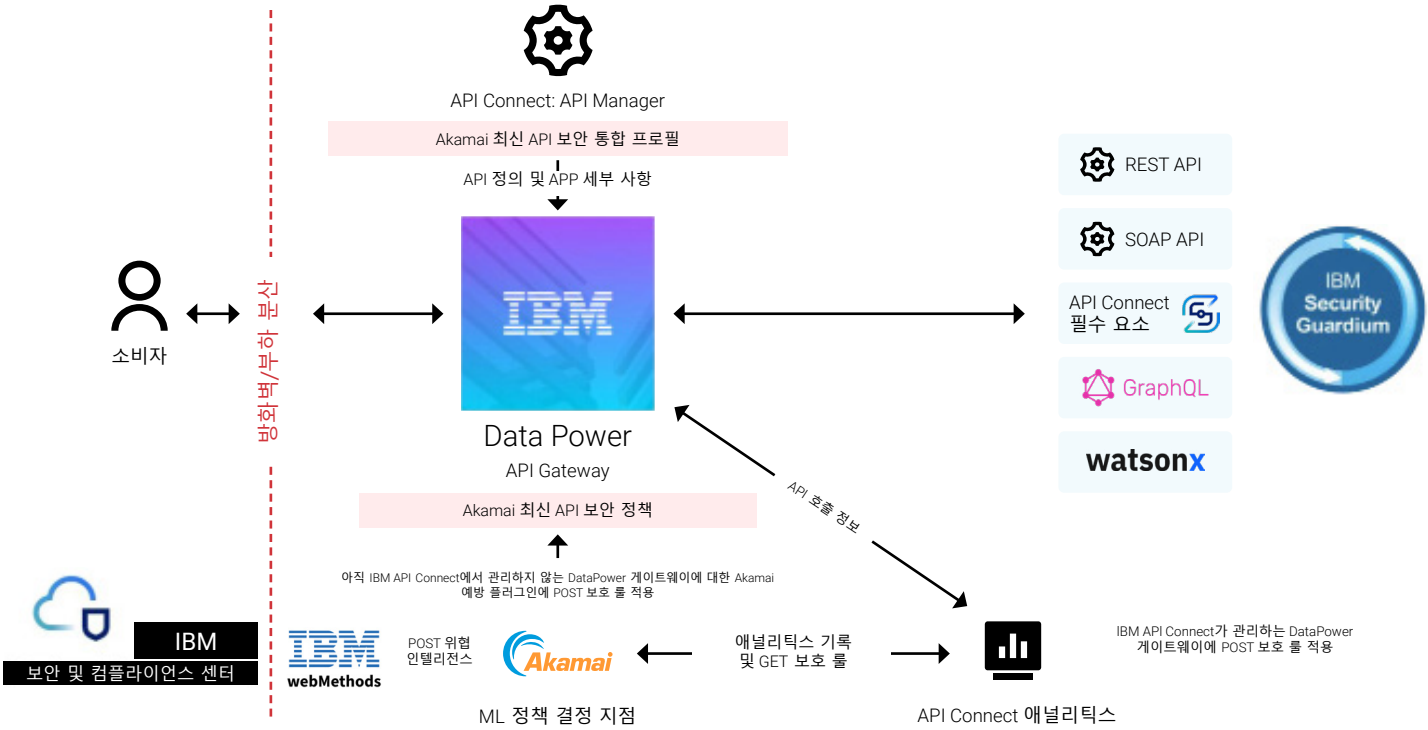
또한 IBM DataPower 고객은 Akamai API Security 솔루션과 통합해 DataPower 게이트웨이에 추가 플러그인을 설치할 필요 없이 성능과 지연 시간의 영향을 받지 않고 거의 실시간으로 위협을 탐지하고 차단할 수 있습니다.

IBM API Connect는 Akamai API Security 권한 확인 정책에 따라 리소스에 대한 접속 요청을 평가하고 IBM DataPower 클러스터 전체에 차단 룰을 적용해 수정 시간을 며칠에서 몇 분 또는 몇 초로 단축할 수 있습니다.



IBM webMethods와 Akamai API Security의 강력한 기능을 결합해 API를 탁월하게 관리하고 보호하세요. 이 파트너십은 Akamai의 최신 API 검색 기능과 IBM webMethods의 강력한 거버넌스 및 실시간 데이터 통합 기능을 결합한 완벽한 솔루션을 제공합니다. API에 대한 완벽한 가시성과 제어를 확보해 보안과 컴플라이언스를 보장하세요. 이 통합은 방어력을 강화할 뿐 아니라 효율성을 높여 기업이 시장 요구사항 변화에 신속하고 안전하게 대응하게 합니다.

마지막으로, IBM DataPower 고객은 Akamai eBPF Red Hat OpenShift 통합을 활용해 API Connect에서 아직 관리하지 않거나 DataPower에서 프록시하지 않는 API를 발견할 수 있기 때문에 고리스크 거래와 기밀 데이터를 처리하는 API를 찾아 보호할 수 있습니다. 이러한 기능은 온프레미스 환경뿐 아니라 클라우드와 하이브리드 환경으로 확장되어 AWS(Amazon Web Services), Microsoft Azure, GCP(Google Cloud Platform)를 지원합니다.



다음 단계

API는 기업이 고객의 요구사항을 충족하고, 매출을 창출하며, 빠르게 변화하는 디지털 경제에서 경쟁력을 갖추는 데 중요한 원동력입니다. 그러나 지속적인 성장, 데이터와의 근접성, 수많은 취약점으로 인해 공격자들의 매력적인 표적이 되고 있습니다. API 보안 인시던트가 꾸준히 증가함에 따라 기업 전체의 모든 API를 보고 보호하며 테스트할 수 있는 기능을 갖춰야 합니다. IBM과 Akamai의 만남은 API를 안전하고 규모에 맞게 구축하고 유지하며 사용할 수 있는 자신감을 기업에 제공합니다.

맞춤 Akamai API Security 데모 일정을 예약해 어떤 도움을 받을 수 있는지 알아보세요. IBM 담당자에게 자세한 내용을 문의하실 수 있습니다.