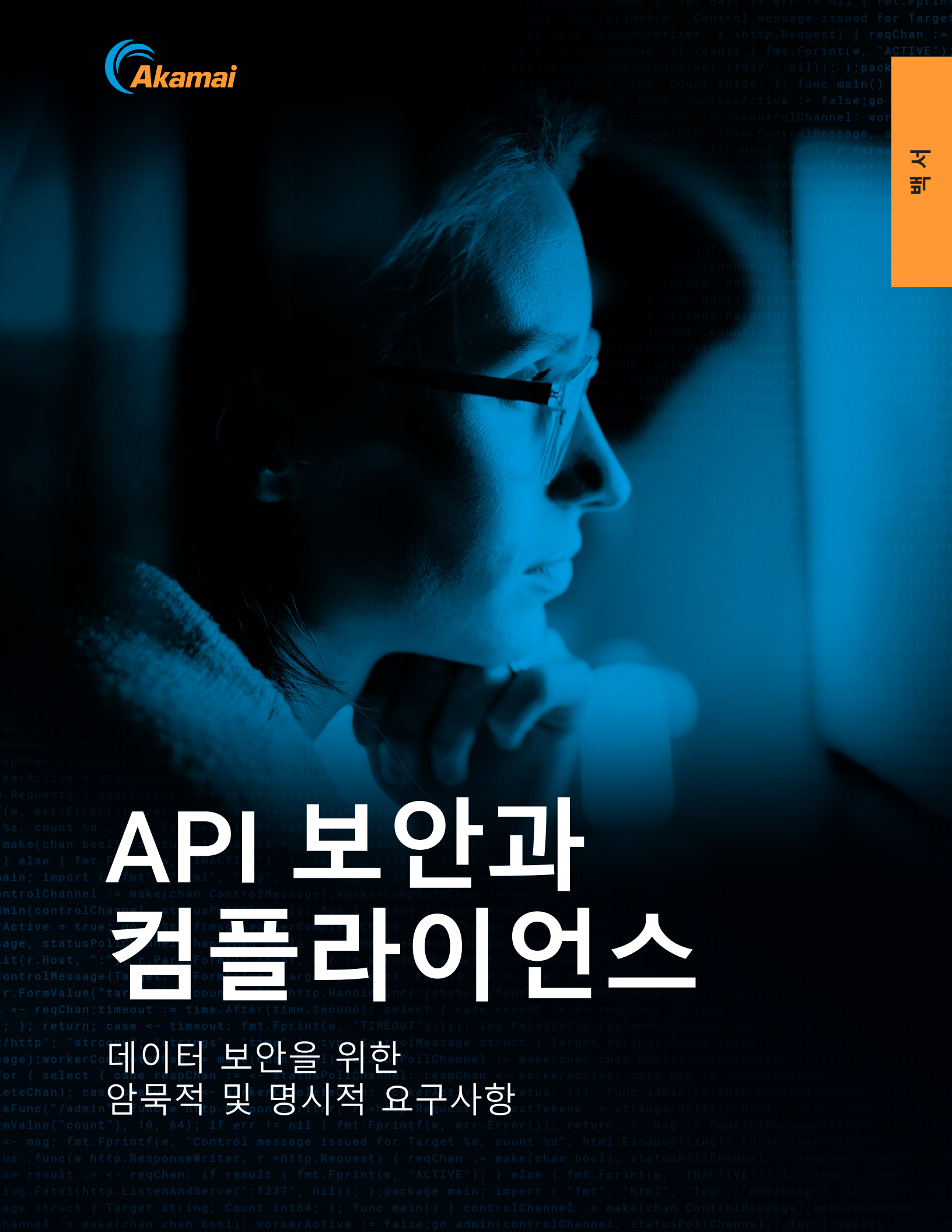
Akamai

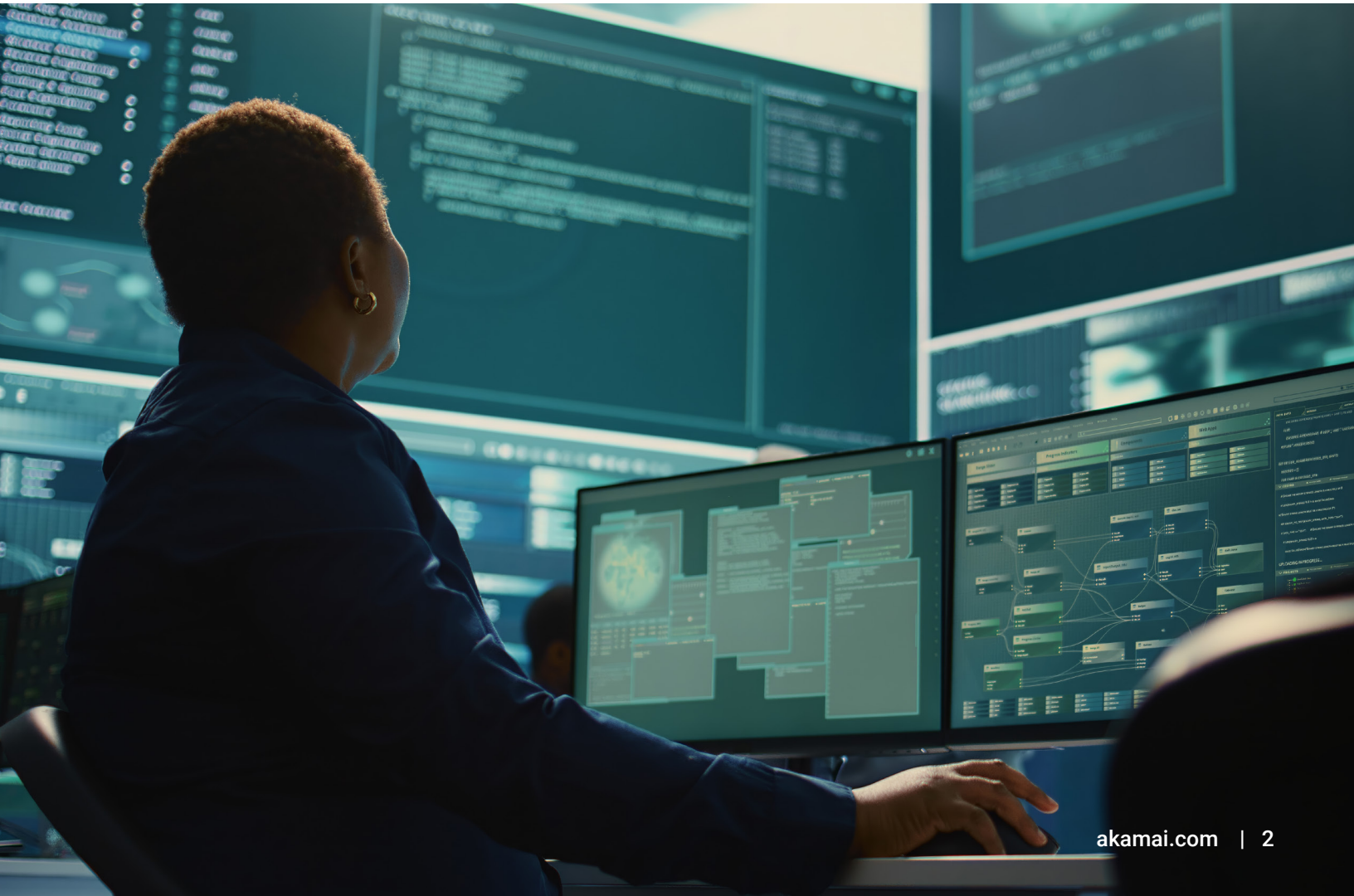
전자책



API 보안과 컴플라이언스

데이터 보안을 위한 암묵적 및 명시적 요구사항

보고서 내용



서론

데이터 보안 규제를 준수한다는 것은 전통적으로 대부분 익숙한 리스크에 대응하기 위해 많은 에너지와 자원을 소비하는 것을 의미했습니다. 하지만 이제는 달라지고 있습니다. 오늘날의 공격표면은 대부분의 기업 컴플라이언스 프로그램이 충분히 고려하지 못하는 위협으로 확장하면서 빠르게 진화하고 있습니다. 이는 규제 기관이 항상 그 속도를 따라갈 수 없고 유출 방지에 필요한 모든 측면에 대해 명확하게 규정할 수 없기 때문입니다.

API 보호의 경우도 마찬가지입니다. 고객, 파트너, 벤더사가 디지털 방식으로 기업과 상호작용할 때마다 그 배후에서 민감한 데이터를 포함한 신속한 정보 교환을 지원하는 API가 존재합니다. 공격자는 이제 API를 직접 표적으로 삼아 해당 데이터를 훔치는 전략을 간소화할 수 있다는 것을 알고 있습니다.

API를 인벤토리화, 평가, 보호해야 한다는 새로운 문구를 규제에서 이미 보셨을 겁니다. 그러나 API에 대한 구체적인 문구가 포함되어 있지 않더라도 API가 명백한 공격 기법이 되었다는 사실은 적절한 보호가 필요하다는 것을 *의미*합니다.

API가 주요 컴플라이언스 문제로 떠오른 것은 놀라운 일이 아닙니다. 노출되거나 잘못 설정된 API가 널리 퍼져 있고, 쉽게 감염될 수 있으며, 보호되지 않는 경우가 많습니다. 단 한 번의 API 유출로 수백만 개의 기록이 도난당할 수 있습니다. 다음의 수치를 보면 분명히 알 수 있습니다.

- 기업의 78%가 API 보안 인시던트를 경험했습니다.[1]
- 44%는 API 보안 인시던트로 인해 규제 기관으로부터 벌금을 부과받은 경험이 있습니다.[2]

이것이 컴플라이언스 프로그램에 어떤 영향을 미칠까요? 규제 기관은 기업이 민감한 데이터에 대한 모든 접속 지점을 보호하기 위한 조치를 취하고 있는지 확인해야 합니다. 즉, 기업은 다음을 수행할 수 있음을 입증해야 합니다.

- 파악하기 어려운 섀도 API를 포함한 모든 API 설명
- 모든 API 취약점 발견 및 수정
- API 중심의 데이터 유출을 방지하기 위한 맞춤형 제어 적용

이 백서에서는 증가하는 API 리스크의 특성을 살펴보고, 명시적 또는 암묵적으로 API 보안을 요구하는 6가지 규제 및 프레임워크의 사례를 자세히 살펴보고, API 보안 모범 사례를 통해 컴플라이언스 요구사항을 충족하는 방법에 대한 조언을 제공합니다.

1., 2. Akamai Technologies, 'API 보안 단절(The API Security Disconnect),' 2023

API 리스크의 이해

API는 기업의 디지털 제품, 서비스, 클라우드 환경의 핵심입니다. 데이터에 대한 지속적인 접속은 매출 창출의 원동력이자 운영 리스크의 원인이기도 합니다. 문제는 대부분의 기업, 심지어 성숙한 보안 프로그램을 갖춘 기업조차도 피싱이나 랜섬웨어와 같은 다른 위협에 집중하는 만큼 API 관련 위협에 우선순위를 두지 않는다는 것입니다.

일부 기업은 기본적인 API 보호를 위해 API 게이트웨이와 웹 애플리케이션 방화벽(WAF)에 의존하지만, 이러한 툴은 전문 API 보안 솔루션이 제공할 수 있는 수준의 가시성, 실시간 보안, 지속적인 테스트를 제공하도록 설계되지 않았습니다. 이러한 툴로는 충분하지 않은 이유는 다음과 같습니다.

- API 게이트웨이와 WAF는 이를 통해 라우팅되는 *매니지드* API 트래픽만 관찰할 수 있습니다.
- 분석가들이 2025년까지 일반 기업 API 생태계의 거의 절반을 차지할 것으로 예상하는 언매니지드 API는 보호할 수 없습니다.
- 그 결과, 보안팀은 API가 라우팅되는 위치, 설정 방법, 교환되는 민감한 데이터의 종류, 리스크에 대해 거의 알지 못하기 때문에 가장 빠르게 확장되고 있는 공격표면을 방어할 수 있는 준비가 충분히 되어 있지 않습니다.

사용자 정보 보호는 규제 기관의 최우선 과제이며, 무단 접속으로부터 고객 데이터를 합리적으로 보호하지 못하는 기업에게 큰 벌금을 부과합니다. 전체 API 인벤토리를 보유한 보안 전문가 10명 중 4명만이 어떤 API가 민감한 데이터를 반환하는지 알고 있다는 점[3]과 공격자가 취약점을 테스트하기 위해 API 호출을 많이 한다는 점을 고려하면 API를 통한 데이터 유출은 더욱 증가할 것이며, 특히 현재 API 공격을 매우 쉽게 일으킬 수 있기 때문에 더욱 심각해질 것입니다.

3. Akamai Technologies, 'API 보안 단절(The API Security Disconnect),' 2023

컴플라이언스에 영향을 미치는 4가지 API 공격

API 유출이 기업의 컴플라이언스 체계에 어떤 영향을 미칠까요? 다음은 몇 가지 사례입니다.

- 한 유명 프로젝트 관리 애플리케이션이 인증 제어 기능이 없는 API 엔드포인트를 악용한 공격자에 의해 감염됐습니다. 공격자는 API를 유출해 수백만 명의 사용자 정보에 무단으로 접속했고, 몇 달 후 이메일 주소와 이사회 멤버십을 포함한 21GB가 넘는 데이터를 인터넷에 유출했습니다.
- 한 대형 통신 회사의 1100만 명 이상의 고객 기록이 노출되었는데, 이는 관리자가 알아채지 못하는 사이에 인증이 필요 없는 API가 인터넷에 노출되었기 때문으로 알려졌습니다. 공격자는 API에 침입해 고유 식별자가 없는 것을 확인하고 ID 번호를 추측해 민감한 데이터를 쉽게 요청했습니다.
- 한 소셜 미디어 회사는 최근 몇 년 동안 부적절한 API 사용을 통한 스크레이핑 기법으로 두 차례 공격을 받은 것으로 알려졌습니다. 첫 번째 사례에서는 5억 명의 사용자 프로필에서 개인 데이터를 스크레이핑한 후 판매했습니다. 두 번째 사례에서는 공격자가 7억 명의 사용자로부터 스크레이핑한 전화번호와 급여 데이터를 포함한 데이터베이스를 만들었습니다.
- 또 다른 소셜 미디어 기업에서도 동일한 기법을 사용해 수백만 명의 사용자 데이터를 유출했습니다. 이 기업은 써드파티 벤더사가 회사의 API를 사용해 민감한 데이터를 수집했다는 이유로 50억 달러의 벌금을 부과받았습니다. 벤더사가 API를 남용한 것은 중요하지 않았고, 이 기업이 애플리케이션을 모니터링하지 않았기 때문에 *회사*에 벌금이 부과되었습니다.

API 보안과 관련된 규정 및 프레임워크의 6가지 사례

많은 규정과 프레임워크에서 API의 이름이 반드시 언급되지는 않지만, 요구사항은 API가 작동하는 애플리케이션과 인프라를 보호하는 데 중점을 두고 있습니다. 예를 들면 다음과 같습니다.

- PCI DSS(Payment Card Industry Data Security Standard) v4.0은 기업의 소프트웨어가 외부 구성요소의 기능을 안전하게 사용하는지 확인하기 위한 가이드를 제공합니다. 여기에는 모바일 앱에서 은행 시스템으로 결제 데이터를 전송하는 API가 포함됩니다.
- NIST 보안 소프트웨어 개발 프레임워크는 보안이 우수한 소프트웨어를 제작하고, 지속적으로 보안을 유지하고, 취약점에 대응하기 위한 가이드를 제공합니다. API는 소프트웨어 개발의 핵심입니다.

많은 경우, '적절한 보안 조치'에 관한 GDPR(General Data Protection Regulation)의 요구사항과 같이 명확하게 정의되지 않은 목표를 제시하는 규제들이 있습니다. API는 고객*그리고* 공격자로부터 데이터를 요청하는 콜을 하루 수백만 건 받을 수 있습니다. 어떤 보안 제어가 필요한지 결정한 다음 어떻게 작동할지 입증하는 것은 기업의 책임입니다.

API 생태계에 직접적인 영향을 미치는 규제와 프레임워크를 자세히 살펴보겠습니다.

1. PCI DSS v4.0

Payment Card Industry Data Security Council에서 만든 PCI DSS는 결제 데이터 보호를 위한 글로벌 표준이 되었습니다. 주요 신용 카드를 수락하고 카드 소유자의 데이터를 전자적으로 처리, 저장, 전송하는 기업들은 이 규제를 준수해야 합니다.

기존 버전의 요구사항은 시스템 및 카드 소유자 데이터에 대한 접속 권한을 필요한 만큼 할당하고 업무별 접속 요구사항을 정의하는 등 2006년 PCI DSS가 발표되었을 때와 마찬가지로 현재도 중요한 보안 주요 사항을 다루고 있습니다.

그러나 PCI DSS v4.0이 시행됨에 따라 기업은 결제 기술 내에 존재하는 수천 개의 API를 자주 노리는 공격자를 고려해 컴플라이언스 프로그램을 조정해야 합니다. 전반적으로 PCI DSS v4.0은 다음과 같은 4가지 핵심 목표에 중점을 두고 있습니다.

1. 결제 업계의 보안 요구사항을 지속적으로 충족
2. 보안을 지속적인 프로세스로 구축
3. 기업이 요구사항을 충족하는 방식에 있어 유연성(새로운 툴, 새로운 제어 등) 제공
4. 검증 방법 및 프로세스 개선

PCI DSS v4.0 요구사항 6.2.3은 기업이 맞춤형 사용자 지정 애플리케이션 코드(써드파티 벤더사가 개발한 코드지만, 상용 표준 애플리케이션 기성품을 의미하지는 않음)를 검토해 취약점이 프로덕션 환경에 노출되지 않게 해야 한다는 점을 강조합니다. API와 관련된 이 요구사항은 기업의 소프트웨어가 외부 구성요소의 기능(라이브러리, 프레임워크, API 등)을 안전하게 사용하는지 확인하기 위한 가이드를 제공합니다. 이와 같은 요구사항은 광범위한 소프트웨어 공급망에서 API의 핵심 역할과 이를 보호하기 위해 필요한 사항을 강조합니다.

API는 최신 애플리케이션 환경에서의 기본적인 연결 및 데이터 교환 방법이 되었습니다. 따라서 프리프로덕션(시프트 레프트) 및 포스트프로덕션(쉴드 라이트) 관점에서 API를 보호하는 것은 공격으로부터 디지털 비즈니스의 안정성을 높이는 데 필수적입니다. 다음은 요구사항 6.2.3을 준수하기 위해 따라야 할 몇 가지 API 보안 모범 사례입니다.

- API 기반 구성요소의 사용과 보안 체계를 확인합니다(예: 취약한 암호화 암호 사용 등 취약점을 유발하는 잘못된 설정을 찾아냅니다).
- API 사용의 정상적이고 예상되는 행동을 검증하고 의심스러운 행위자가 시스템을 악용하는 것을 차단하기 위한 제어를 구축합니다(예: 애플리케이션의 행동을 확인해 논리적 취약점을 탐지).
- API를 구동하는 데 사용되는 써드파티 프레임워크를 탐지해 오래되고 취약할 수 있는 프레임워크를 파악합니다.
- 실행 중인 여러 버전을 포함해 모든 API의 전체 인벤토리를 구축해 백도어 및 관리해야 할 잠재적인 문서화되지 않은 기능에 대한 인사이트를 제공합니다.
- API 코드의 보안을 검증하고 API 관련 취약점이 프로덕션에 적용되지 않도록 합니다.
- API에 대한 보안 코딩 모범 사례를 구축해 프로그래밍 접근 방식을 도입하고 지속적으로 안전하게 코드를 제공할 수 있게 합니다.

2. GDPR(General Data Protection Regulation)

GDPR은 유럽 연합(EU) 내 개인에 대한 데이터 보호를 강화하고 통합하는 것을 목표로 하는 EU의 법입니다. 그러나 GDPR은 EU에 기반을 둔 기업에만 국한되지 않으며, EU에서 소비재나 서비스를 제공하는 모든 기업은 GDPR을 준수해야 합니다.

GDPR은 개인 데이터를 개인과 연결되거나 연결될 수 있는 정보로 규정합니다. GDPR에 따라 규제되는 데이터에는 개인의 이름, 연락처 정보, 은행 및 금융 데이터, 의료 정보가 포함될 수 있습니다. 보다 기술적인 측면에서는 IP 주소 및 웹 쿠키와 같은 지리적 위치 데이터도 규제 대상 데이터에 포함됩니다.

이것이 API 보안에 어떤 의미가 있을까요? 애플리케이션, 마이크로서비스, 사물 인터넷(IoT) 디바이스를 개발하든, 이러한 기술의 핵심에 있는 API는 GDPR의 규제를 받는 데이터를 교환하고 있을 가능성이 높습니다. 따라서 인터넷에 접속할 수 있는 API를 개발하는 기업은 사후가 아닌 처음부터 데이터 보호를 API 설계에 고려해야 합니다.

사용자에게 업무 수행에 필요한 최소한의 권한만 부여해야 한다는 최소 권한 원칙을 고려해야 합니다.

GDPR 제25조는 최소 권한에 *근간*을 두고 있으며, 기업은 '기본적으로 각 특정 목적에 필요한 개인정보만 처리하도록 보장하기 위한 기술 및 조직적 조치'를 구축해야 합니다. 이에 따라 API 개발자는 사용자 인증 및 권한 제어를 구축해 API를 통해 흐르는 민감한 데이터를 보호해야 합니다. 또한, API 개발팀은 보안 통신 프로토콜을 사용해 클라이언트와 서버 간의 정보 교환을 암호화함으로써 데이터가 전송 중에도 기밀로 유지되도록 해야 합니다.

하지만 기업이 지난 수년 또는 수십 년 동안 구축해 온 기존의 API 생태계는 어떨까요? 기업 API의 상당 부분이 관리되지 않거나, 잊히거나, 견제와 균형 없이 영구적으로 실행되고 있습니다. 이러한 경우 GDPR은 다음을 요구합니다.

- IT 환경의 모든 API 파악
- 리스크 요소 평가(예: 교환한 데이터의 종류, 해당 데이터에 접속할 수 있는 사람 또는 대상)
- 잘못된 설정이나 취약한 인증 메커니즘과 같은 모든 취약점 수정
- 기존 및 새로운 유출 및 공격 방법 모두에 대한 안정성을 위해 지속적으로 API 테스트

3. DORA(Digital Operational Resiliency Act)

중요 인프라 운영자로서의 EU 금융 부문의 역할을 고려할 때, DORA의 요구사항은 EU 회원국의 기업이 사이버 공격을 견디고 복구하는 데 도움을 주기 위한 것입니다. DORA를 통해 금융 부문은 정보통신 기술(ICT)에 대한 구속력 있는 포괄적인 리스크 관리 프레임워크를 갖추게 됩니다. DORA는 현재 수많은 규제와 표준이 존재하는 상황에서 EU 금융 회사가 준수해야 하는 요구사항을 통합하고 강화하는 것을 목표로 합니다.

EU의 총 2만 2000개 이상의 금융 기관과 IT 서비스 공급업체가 DORA의 영향을 받습니다. 여기에는 클라우드 서비스 공급업체를 포함해 EU 금융 회사에 ICT 시스템과 서비스를 제공하는 써드파티 업체도 포함됩니다. 이 법에 따라 금융 기관은 ICT 써드파티 리스크 전략을 개발하고 공급업체의 적합성을 검증하기 위한 실사를 수행해야 합니다.

DORA는 디지털 운영 안정성에 대한 잠재적 격차, 취약점 또는 결함을 식별하는 정기적인 테스트 프로그램을 구축하도록 요구하는 등 API 보안과 관련된 몇 가지 요구사항을 명시하고 있습니다. 네트워크 보안 테스트, 침투 테스트, 웹 애플리케이션 테스트 등을 생각해 보세요. 금융 기업의 규모, 리스크도, 비즈니스 프로필에 따라 위협 주도 모의 해킹(TLPT)을 기반으로 필수 검토를 수행해야 합니다. 마찬가지로 중요한 것은 API의 취약점을 정기적으로 테스트하는 것입니다.

DORA는 웹 기반 애플리케이션 및 API 테스트를 포함하는 보안 테스트 사례를 간략하게 설명합니다. 여기에는 OWASP(Open Worldwide Application Security Project)와 같은 공개 리소스를 활용하는 것도 포함됩니다. 특히 OWASP 10대 API 보안 리스크는 공격자가 기업 리소스에 접속하거나, 조작하거나, 기타 방식으로 제어할 수 있는 설정 오류, 약점, 논리 취약점, 코드 문제를 식별하는 데 도움이 됩니다.

4. HIPAA(Health Insurance and Portability and Accountability Act)

HIPAA는 전자 건강 기록(EHR), 컴퓨터화된 의사 처방 입력 플랫폼 및 기타 헬스케어 IT 시스템에서 보호하는 건강 정보(PHI)를 보호하기 위한 데이터 개인정보 보호 및 보안 원칙에 중점을 두고 있습니다. PHI를 전자적으로 저장하거나 전송하는 모든 미국 헬스케어 공급업체, 보험 관리자 또는 클리어링 하우스(clearing house)는 HIPAA를 준수해야 합니다. 여기에는 PHI의 기밀성, 무결성, 가용성을 보장하고 무단 공개와 부적절한 사용으로부터 보호하는 것이 포함됩니다.

HIPAA는 요구사항에 명시적으로 API를 언급하지 않더라도 API에 중대한 영향을 미치는 규제의 한 사례입니다.

연중무휴 24시간 운영되는 헬스케어 클리닉을 위한 환자 포털을 구축하는 기술 벤더사를 생각해 봅시다. 이러한 포털의 기본 기능은 환자가 의사 방문, 검사 결과, 결제 등에 관한 데이터에 효율적이고 안전하게 접속할 수 있도록 하는 것입니다. API는 이러한 교환을 촉진하는 역할을 합니다. 클리닉과 벤더사는 모두 HIPAA 요구사항을 준수해야 합니다.

HIPAA의 개인정보 보호 규정은 적용 대상 기관이 '직원들의 특정 업무에 따라 보호되는 건강 정보의 접속 및 사용을 제한하는 정책과 절차를 개발하고 구축해야 한다'고 명시합니다. 따라서 기업의 API 개발자는 인증, 고유 사용자 ID, 업무 기반 접속 제어와 같은 기술적 보호 장치를 포함시켜 최소 권한을 보장해야 합니다.

IT팀이 맞춤형 API를 생성하는 벤더사나 공급업체를 위해 API를 개발하는 벤더사 등 HIPAA 적용 대상 기업에게도 가시성은 필수입니다. 기업은 전송하는 PHI 종류를 포함해 각 API의 리스크 체계에 대한 실시간 평가 및 보고가 필요합니다. 이는 컴플라이언스 및 개인이 자신의 PHI가 언제, 어디서, 왜, 누구에게 공개되었는지에 대한 정보를 요청하는 개인에게 응답해야 하는 HIPAA의 요구사항을 충족하는 것과 관련이 있습니다.

5. NIS2(Network and Information Security Directive)

EU는 2023년 1월에 IT 인프라 보안 및 인시던트 보고에 관한 기존 버전의 가이드를 기반으로 한 NIS 가이드 버전 2.0을 도입했습니다. 버전 2.0은 API를 구체적으로 언급하지는 않지만, 이 가이드의 적용을 받는 기업의 많은 디지털 서비스 기능에 필수적인 API를 보호하고 관리하는 데 중요한 영향을 미칩니다. NIS2에는 다음이 포함됩니다.

- 적용 부문 확대 - 클라우드 서비스 공급업체와 소셜 미디어 회사 등이 기존 목록에 추가되었으며, 여기에는 중요 인프라 운영자도 포함됩니다. 통합 및 서비스 제공을 위해 API가 광범위하게 사용되는 이러한 분야에서는 API 보안 확보가 우선순위가 됩니다.
- 공급망 보안을 다시 강조 - 기업은 리스크를 평가하고 IT 공급망과 써드파티 공급업체 관계를 보호해야 합니다. API는 종종 외부 서비스를 통합하는 데 사용되기 때문에 보안을 보장하는 것이 컴플라이언스의 핵심입니다.
- 민감한 리소스를 보호하고 안정성을 보장하기 위해 사람, 정책, 기술을 평가하는 정보 보안 관리 시스템을 구축해야 합니다. API는 빠르게 성장하는 공격 기법이므로 리스크 관리 전략에 반드시 포함되어야 합니다.
- API 유출을 포함한 중대한 사이버 보안 인시던트를 보고해야 합니다. 따라서 기업은 API 관련 인시던트를 모니터링하고, 탐지하고, 보고할 수 있는 메커니즘을 마련해야 합니다.

6. 미국 금융 서비스 규제 기관을 위한 가이드

FFIEC(Federal Financial Institutions Examination Council)는 연방 규제 기관이 미국 금융 업계를 감독하기 위한 가이드와 표준을 만듭니다. 여기에는 연방준비제도이사회, FDIC, OCC, NCUA가 포함됩니다. 이 위원회의 임무는 사기, 남용, 위법 행위로부터 소비자와 투자자를 보호하는 것입니다. 규제는 아니지만 FFIEC의 가이드는 금융 회사가 권장 보안 조치를 준수하는 방법을 알 수 있도록 하는 데 핵심적인 역할을 합니다.

여기에는 API를 보호하고 사기 및 신원 도용으로부터 소비자를 보호하는 방법에 대한 구체적인 가이드가 포함되어 있습니다. 간략한 내용은 다음과 같습니다.

- **인벤토리:** FFIEC는 인증 및 접속 제어가 필요한 API를 포함한 모든 정보 시스템의 인벤토리를 구축할 것을 권장합니다. 이는 금융 기관뿐 아니라 클라우드 서비스 공급업체와 같은 써드파티에도 적용됩니다.
- **인증:** API는 권한이 부여된 사용자에게만 접속을 허용해야 합니다. 접근 제어가 필요한 모든 사용자(고객 등)를 식별해야 합니다. 또한, 멀티팩터 인증과 같은 강화된 제어가 필요한 사용자를 식별하는 것도 중요합니다.
- **권한 부여:** API는 권한이 부여된 사용자에게만 특정 리소스에 대한 접속을 허용해야 합니다. 이를 위해 FFIEC는 무단 접속을 식별하고 추적하기 위해 활동을 모니터링하고, 기록하고, 보고하는 등 계층형 보안을 구축할 것을 권장합니다.
- **리스크 관리:** FFIEC는 최신 가이드에서 여러 가지 효과적인 리스크 관리 방법을 제시하고 있습니다. 그러나 정보 시스템 인벤토리 범주에서 명시적으로 API를 언급하고 있으므로 정확한 API 인벤토리가 필요합니다.

기업은 피싱이나 랜섬웨어와 같이 잘 알려진 위협에 대해 잘 알고 있을 수 있지만, FFIEC는 '금융 기관 정보 시스템에 영향을 미칠 합리적인 가능성'이 있는 *모든* 사이버 위협과 해당 데이터를 식별할 것을 요구합니다. 서론에서 언급했듯이 78%의 기업이 API 보안 인시던트를 경험한 적이 있으므로 금융 규제 기관의 요구사항이 계속 진화함에 따라 API 보안은 컴플라이언스 필수 요소가 될 것입니다.

API 보호 모범 사례로 컴플라이언스 과제 해결

오늘날의 위협 환경에서는 API 검색, 체계 관리, 런타임 보호, API 보안 테스트를 제공하는 완벽한 API 보안 솔루션이 필요합니다. 이러한 포괄적인 접근 방식은 이미 구축되어 있는 WAF 또는 API 게이트웨이를 보완하는 역할을 합니다.

1. API 검색

아무도 모르는 API가 생각보다 많습니다. 대부분의 기업은 API 트래픽의 대부분에 대한 가시성이 거의 없거나 전혀 없는데, 모든 API가 API 게이트웨이를 통해 라우팅된다고 가정하기 때문입니다. 하지만 사실은 그렇지 않습니다. 완전하고 정확한 인벤토리가 없으면 기업은 다양한 리스크에 노출됩니다. 필요한 핵심 기능은 다음과 같습니다.

- 설정이나 종류에 관계없이 모든 API의 위치 및 인벤토리 파악
- 휴면, 레거시, 좀비 API 탐지
- 잊히거나, 방치되거나, 알려지지 않은 섀도 도메인 식별
- 사각지대 제거 및 잠재적 공격 경로 파악

2. API 체계 관리

완전한 API 인벤토리를 구축한 후에는 API를 통해 어떤 종류의 데이터가 이동하고 있는지, 이것이 규제 요구사항을 준수하는 데 있어서 어떤 영향을 미치는지 파악해야 합니다. API 체계 관리는 트래픽, 코드, 설정에 대한 포괄적인 보기를 제공해 기업의 API 보안 체계를 평가합니다. 필요한 핵심 기능은 다음과 같습니다.

- 인프라를 자동으로 스캔해 설정 오류와 숨겨진 리스크 발견
- 주요 이해관계자에게 취약점을 알리는 맞춤형 워크플로우 생성
- 민감한 데이터에 접속할 수 있는 API 및 내부 사용자 식별
- 탐지된 문제에 심각도 순위를 할당해 해결 우선순위 지정

3. API 런타임 보안

'유출 가정'이라는 개념에 대해 다들 잘 알고 계실 것입니다. API 관련 유출 및 공격도 이와 같이 불가피한 수준에 도달하고 있습니다. 프로덕션 환경에서 운영 중인 모든 API에 대해 실시간으로 공격을 탐지하고 차단할 수 있어야 합니다. 필요한 핵심 기능은 다음과 같습니다.

- 데이터 변조 및 유출, 정책 위반, 의심스러운 행동, API 공격 모니터링
- 추가적인 네트워크 변경이나 설치하기 어려운 에이전트 없이 API 트래픽 분석
- 기존 워크플로우(티켓팅, SIEM 등)와 통합해 보안 및 운영팀에 알림 제공
- 부분적으로 또는 완전히 자동화된 해결을 통해 실시간으로 공격 및 오용 방지

4. API 보안 테스트

API 개발팀은 가능한 한 빨리 작업해야 한다는 압박을 받고 있습니다. 모든 애플리케이션을 개발할 때 속도가 필수적인데, 개발 속도가 빠르면 취약점이나 설계 결함이 발생하고 이를 발견하지 못할 가능성이 큽니다. 개발 중인 API를 프로덕션에 출시하기 전에 테스트하면 취약한 API를 수정하는 데 드는 리스크와 비용을 크게 줄일 수 있습니다. 필요한 핵심 기능은 다음과 같습니다.

- 악성 트래픽을 시뮬레이션하는 광범위한 자동화된 테스트 실행
- API가 프로덕션 환경에 들어가기 전에 취약점을 발견해 공격 성공 리스크 줄이기
- 확립된 거버넌스 정책 및 룰에 따라 API 사양 검사
- 온디맨드 또는 CI/CD 파이프라인의 일부로 실행되는 API 중심 보안 테스트 실행

Akamai API Security로 API 컴플라이언스 복잡성을 간소화하는 방법

API는 현재 규제를 통해 차단하려고 하는 유출 인시던트의 주요 원인입니다. API와 리스크가 증가하는 상황에서 기업을 보호하는 데 필요한 것은 무엇일까요? 많은 기업에서 기본적인 API 보호를 위해 사용하는 기존 툴은 어느 정도 보안 기능을 제공하지만 충분하지 않습니다. 기업의 API를 보호하고 컴플라이언스를 입증할 수 있는 더 나은 방법을 찾고 있다면 Akamai에 문의하시기 바랍니다.

이 백서에서 다루는 모든 요구사항과 가이드에 대해 Akamai API Security는 컴플라이언스뿐 아니라 고객의 데이터와 신뢰를 보호하기 위해 기업이 필요로 하는 보안 기능을 강화합니다.

Akamai의 포괄적인 솔루션은 개발 초기 단계부터 프로덕션 이후까지 API를 보호해 핵심 모범 사례를 준수할 수 있도록 지원합니다.

- API 검색
- 체계 관리
- 런타임 보호
- 보안 테스트

API와 공격으로부터 API를 보호하는 방법을 자세히 알아보세요.

Akamai API Security가 기업에 어떤 도움을 줄 수 있는지 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 관한 자세한 정보를 보려면 akamai.com과 akamai.com/blog를 방문하거나 X(기존의 Twitter)와 LinkedIn에서 Akamai Technologies를 팔로우하시기 바랍니다. 2024년 9월 발행.