



ISDP2025

INFORMATION SECURITY & DATA PRIVACY 2025

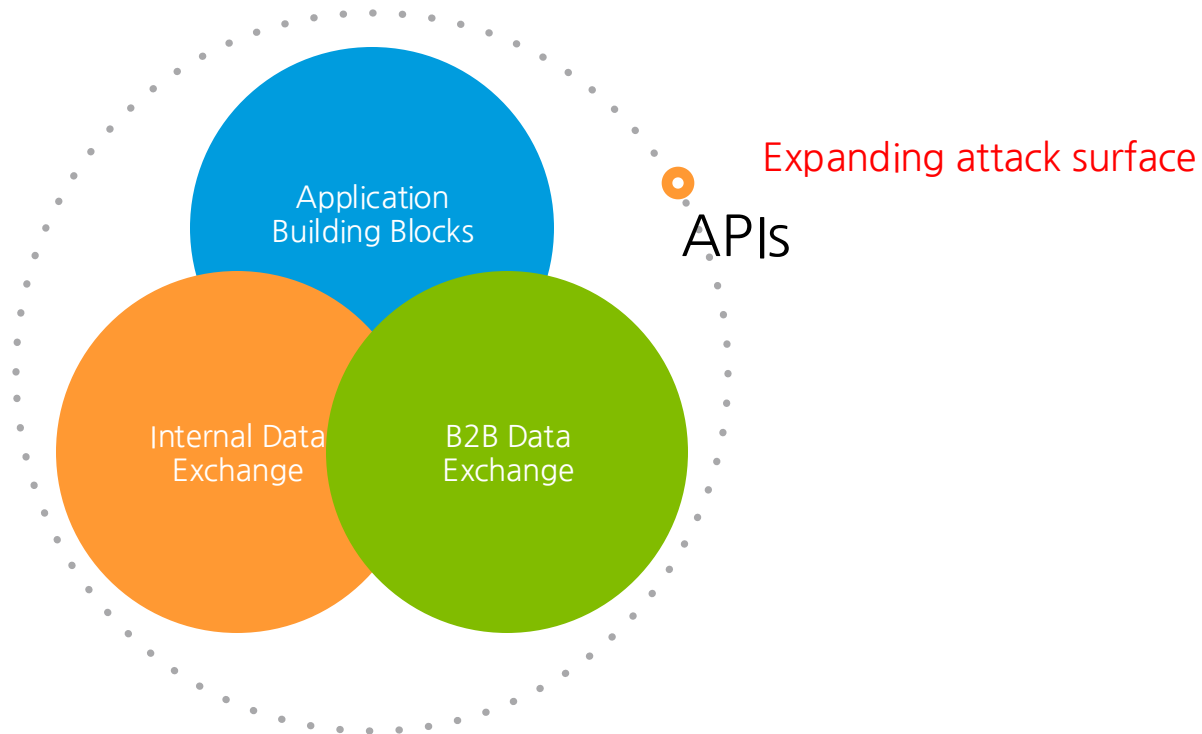
Noname API Security

해커들의 새로운 타겟 – 귀사의 API는 안전하십니까?

Sang-Won Cho

Senior Enterprise Sales Executive
2025.02

APIs Power Your Business



Why is API Security Important?

A circular gauge with a red arc and four red dots, indicating 83% completion.

83%

웹 트래픽의 83%는 Digital Transformation을 주도하는데 중요한 API에 기인합니다.

Integration Demands

Dependency on APIs

A circular gauge with a purple arc and four purple dots, indicating 72% completion.

72%

기업의 72%는 API의 인증/인가와 관련된 문제로 인해 새로운 앱 및 서비스 개선사항의 출시가 지연되는 것을 경험하고 있습니다.

Diverse API Implementations

Complex Ecosystems

A circular gauge with a teal arc and four teal dots, indicating 44% completion.

44%

기업의 44%는 내/외부 API에서 개인정보 보호 및 데이터 유출과 관련된 보안문제를 경험하고 있습니다.

Unique API Vulnerabilities

Exposure to Threats

External Risks

API Attack – New Normal

70% of malicious requests targeting APIs

*"The share of malicious requests targeting APIs vs. Web Applications increased from **54% in 2022** to **70% in 2023**, an increase of 16%."* *



* Source : Annual API ThreatStats™ Report 2024 by Wallarm

API Attacks Are Not An If, But When



*In the last 2024, **24 of 70** major data breaches stemmed from API vulnerabilities, impacting 15 different industries.*



Dell API abused to steal 49 million customer records in data breach

BLEEPINGCOMPUTER

By [Lawrence Abrams](#)

May 10, 2024 03:30 PM 0



Cox Biz Auth-Bypass Bug Exposes Millions of Devices to Takeover

The US broadband provider fixed an issue that allowed attackers to gain access to business customers' modems, and then access info and execute commands with the same permissions of an ISP support team.

DARK
READING



Two Santa Cruz students uncover security bug that let anyone do their laundry for free

CSC ServiceWorks belatedly apologized and thanked the security researchers after the laundry giant ignored requests to fix a security bug.

Zack Whittaker / 9:05 AM PDT • May 17, 2024

Comment



Trello API abused to link email addresses to 15 million accounts

BLEEPINGCOMPUTER

By [Lawrence Abrams](#)

January 23, 2024 04:31 PM 0

OWASP Top10 API 위협

OWASP Top10 API Security		설명	OWASP Top 10 Web Application	
API 1	Broken Object Level Authorization (BOLA)	손상된 개체 수준 권한 부여 : API가 개체 수준에서 접근제어를 적절하게 시행하지 못해 권한이 없는 사용자가 개체 식별자를 조작하고 시스템 내의 민감한 데이터에 대한 권한 없는 액세스로 이어지는 취약점	Broken Access Control	A01
API 2	Broken Authentication	손상된 인증 : API 인증 작동방식이 손상되거나 부적절하게 구현되어 무단 접근과 사용자 계정 및 민감한 정보의 잠재적 오용으로 이어질 수 있는 취약점	Identification & Authentication Failure	A07
API 3	Broken Object Property Level Authorization	깨진 객체 속성 수준 권한 부여 : API가 특정 객체 속성에 대한 접근을 적절하게 제어하지 못해 민감한 데이터 속성에 대한 무단 접근으로 이어질 수 있는 취약점	Cryptographic Failures	A02
API 4	Unrestricted Resource Consumption	무제한 리소스 소비 : API에 적절한 리소스 소비 제어가 없어 공격자가 시스템 리소스를 압도하여 서비스 거부 시나리오나 성능 저하를 초래할 수 있는 취약점	Injection	A03
API 5	Broken Function Level Authorization (BFLA)	손상된 기능 수준 권한부여 : 사용자에게 특정 기능을 수행하는데 필요한 권한이 있는지 적절하게 확인하지 못해 중요한 기능에 대한 무단 접근으로 이어질 수 있는 취약점	Insecure Design	A04
API 6	Unrestricted Access to Sensitive Business Flows	민감한 비즈니스 흐름에 대한 무제한 액세스 : API가 민감한 비즈니스 프로세스 또는 워크플로우에 대한 무제한 접근을 허용하여 중요한 비즈니스 운영을 조작하거나 방해하는 것으로 이어질 수 있는 취약점	Vulnerable & Outdated Components	A06
API 7	Server-Side Request Forgery (SSRF)	서버 측 요청 위조 : API를 통해 공격자가 내부 리소스에 대한 무단 요청을 할 수 있어 네트워크 내 취약성의 추가 악용, 정보 공개, 데이터 조작으로 이어질 수 있는 취약점	Server-side Request Forgery (SSRF)	A10
API 8	Security Misconfiguration	보안 오설정 : API가 제대로 구성되지 않아 기본 설정, 불필요한 서비스 또는 지나치게 관대한 액세스 제어가 가능하여 민감한 데이터를 노출 및 무단 접근이 가능할 수 있는 취약점	Security Misconfiguration	A05
API 9	Improper Inventory Management	부적절한 재고관리 : 조직은 모든 API에 대한 인식이 부족하거나 이러한 자산에 대한 적절한 제어를 구현하지 못하여 관련 위협으로 이어질 수 있는 취약점	Software & Data Integrity Failures	A08
API 10	Unsafe Consumption of APIs	API에 대한 안전하지 않는 소비 : API가 소비되는 방식과 관련된 취약성이 존재하여 부적절한 입력 데이터 검증의 포함, 잠재적 주입 공격, 데이터 침해 또는 기타 보안 침해로 이어질 수 있는 취약점	Security Logging & Monitoring Failures	A09

API is Different!

Four API-Related Factors That Impact Security Programs



Source: Gartner
759813_C

Gartner

Gartner predicts that "by 2025, less than 50% of enterprise APIs will be managed, as explosive growth in APIs surpasses the capabilities of API management tools" (see [Predicts 2022: APIs Demand Improved Security and Management](#)). The situation will be even worse for APIs that organizations consume from third parties.

API Security Gap

Lack of control

모든 API의 인벤토리가 있습니까?



Lack of knowledge

API는 정상적으로 이용되고 있나요?



Lack of Protection

API는 어떻게 보호되나요?



Lack of process

공격/문제가 발생한 경우 어떻게 해야 합니까?

새로운 솔루션의 필요

API Protection Capabilities by Gartner



Source: Innovation Insight for API Protection by Gartner (Published 10 October 2022 - ID G00775426)

Discovery

“.....use a mix of traffic mirroring analysis and querying existing infrastructure (such as API GWs, web application firewalls [WAFs] and container platforms) to discover and inventory the APIs that are being used”

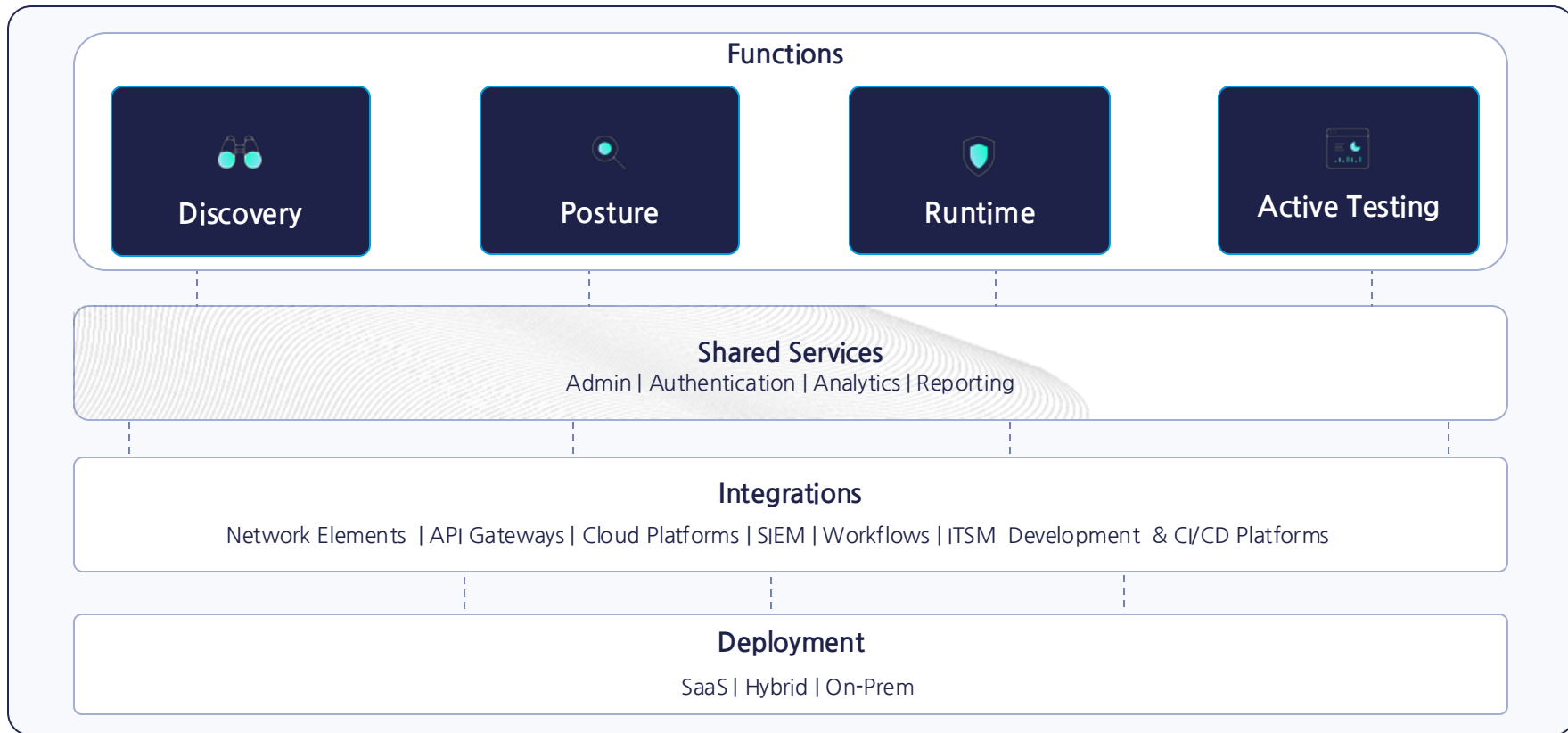
Posture Management

“...We have seen solutions that try to understand the criticality of the API, the business logic behind the API, the severity of the misconfiguration, and various other elements that can indicate more or less risk.”

Runtime Protection

“...The third component of API security solutions focuses on recognition of patterns that are indicators of malicious behavior. A typical example could be a BOLA attack”

API Security Solution 선택 기준



Akamai API Security Platform – Noname

개발부터 운영까지 API Lifecycle 전반에 대한 지원



Discover & Document

What

레거시 API 및 새도 API를 포함하여 환경 전반에 걸쳐 모든 API를 검색하고 카탈로그화

How

데이터 정책 및 거버넌스 규칙을 준수하는 리스크가 전혀 없고, 가볍고, 마찰이 없는 구축 모델



Analyze (이상징후 분석)

What

소스, 정책, 구성 및 런타임에서 잘못된 구성, 이상 징후 및 취약성을 식별

How

비지도 머신 러닝을 사용하여 API를 위해 특별히 구축된 행동 기반 상황별 모델링



Remediation (문제 해결)

What

소스 코드 또는 API 보안 소건의 런타임 문제 해결을 위한 사용자 친화적인 워크플로 제공

How

수동, 반자동 및 완전 자동 프로세스로 구성된 광범위한 고정 라이브러리 (차단 시스템과 연계 시 차단 정책 사용 가능)



Active Testing (보안 테스트)

What

API 엔드포인트를 지속적으로 테스트하여 API 리스크가 발생하기 전에 이를 파악하고 전반적인 API SDLC를 개선

How

API, CI/CD 등을 통해 수동으로 실행하거나 자동화할 수 있는 API 보안 테스트 모델

경쟁사 대비 다양한 개발 플랫폼 및 CI/CD와 연계를 지원하며 차단 정책을 유연하게 운용할 수 있음
이 전략은 소스코드 개발에서 운영까지 API 에코시스템 전반의 전체 보안 범위를 포괄

Akamai API Security Platform – Noname

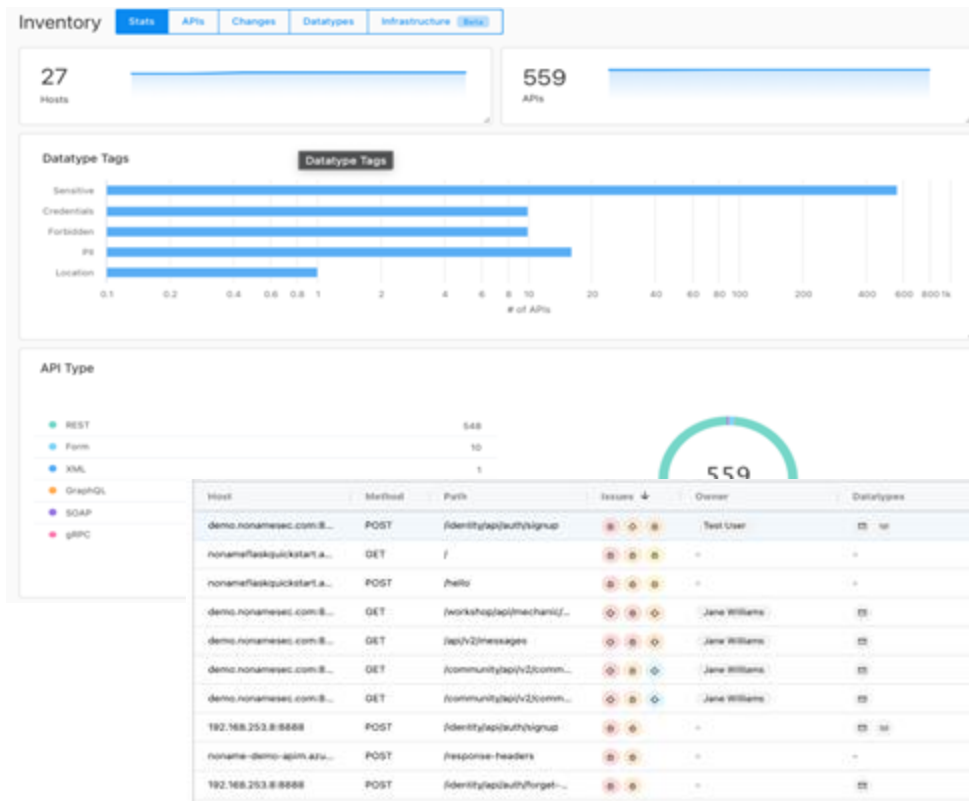
가시화 – Discover (자동 API 검색)



Discovery

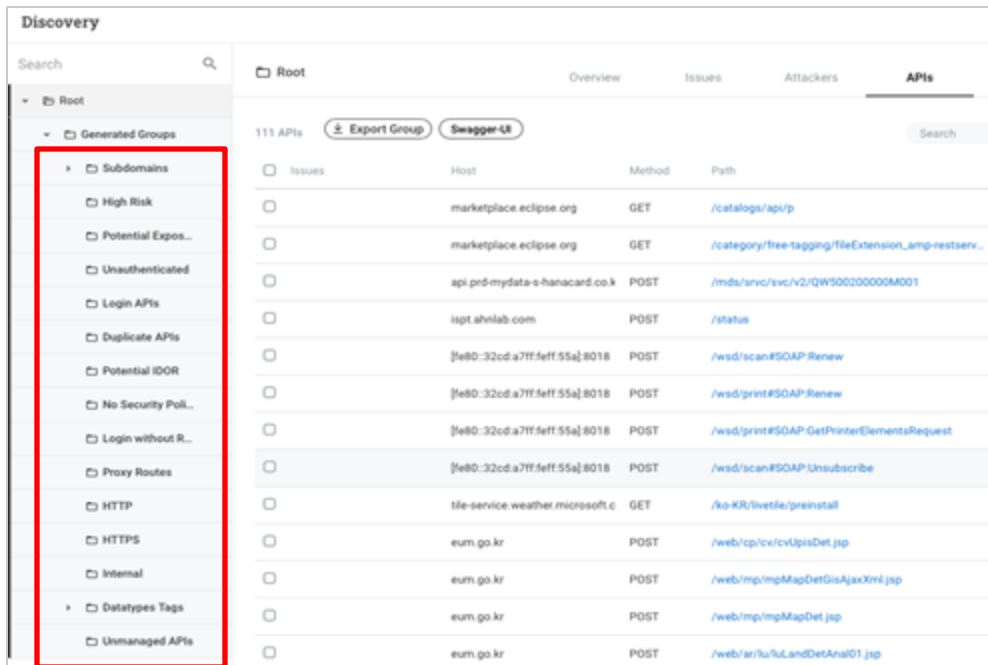
> 레거시/신규/악성 API 식별 및 목록화

- API 목록
- API 사용자 (또는 상대 기관)
- 데이터 식별 (중요 데이터)
- API 소유자 식별
- 서버 식별
- 보안정책 (인증 여부, 암호화 등)
- API 사용 추이 > 문제 발견 및 검증



Akamai API Security Platform – Noname

가시화 – Discover (API 자동 분류)



Discovery

Search

Root

Generated Groups

Subdomains

High Risk

Potential Expos...

Unauthenticated

Login APIs

Duplicate APIs

Potential IDOR

No Security Poi...

Login without R...

Proxy Routes

HTTP

HTTPS

Internal

Datatypes Tags

Unmanaged APIs

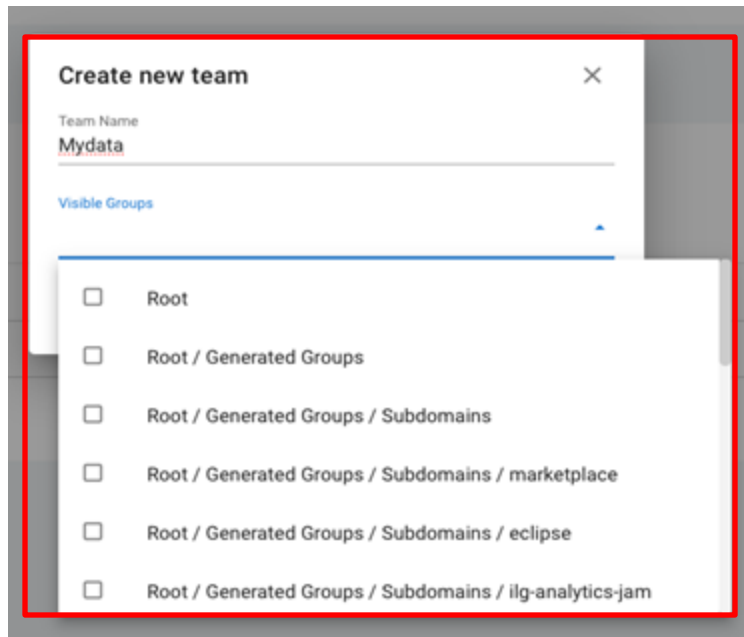
111 APIs

Export Group

Swagger UI

Issues	Host	Method	Path
<input type="checkbox"/>	marketplace.eclipse.org	GET	/catalogs/api/p
<input type="checkbox"/>	marketplace.eclipse.org	GET	/category/free-tagging/fileExtension_amp-restserv...
<input type="checkbox"/>	api.pr0-mydata-s-hanacard.co.kr	POST	/mds/srvc/v2/QW500200000M001
<input type="checkbox"/>	ispt.ahnlab.com	POST	/status
<input type="checkbox"/>	[fe80:32cd:a7ff:feff:55a]:8018	POST	/wsd/scan#SOAP:Renew
<input type="checkbox"/>	[fe80:32cd:a7ff:feff:55a]:8018	POST	/wsd/print#SOAP:Renew
<input type="checkbox"/>	[fe80:32cd:a7ff:feff:55a]:8018	POST	/wsd/print#SOAP:GetPrinterElementsRequest
<input type="checkbox"/>	[fe80:32cd:a7ff:feff:55a]:8018	POST	/wsd/scan#SOAP:Unsubscribe
<input type="checkbox"/>	tile-service.weather.microsoft.co.kr	GET	/ko-KR/livetile/preinstall
<input type="checkbox"/>	eum.go.kr	POST	/web/cp/cv/cvUpsisDet.jsp
<input type="checkbox"/>	eum.go.kr	POST	/web/mp/mpMapDetGisAjaxXml.jsp
<input type="checkbox"/>	eum.go.kr	POST	/web/mp/mpMapDet.jsp
<input type="checkbox"/>	eum.go.kr	POST	/web/ar/ku/kuLandDetAnal01.jsp

API 자동 분류



Create new team

Team Name

Mydata

Visible Groups

- ☐ Root
- ☐ Root / Generated Groups
- ☐ Root / Generated Groups / Subdomains
- ☐ Root / Generated Groups / Subdomains / marketplace
- ☐ Root / Generated Groups / Subdomains / eclipse
- ☐ Root / Generated Groups / Subdomains / ilg-analytics-jam

사용자 그룹별 접근 통제

Akamai API Security Platform – Noname

가시화 – Discover (API 변경 탐색)

> API의 변경 사항(신규 API 등)에 대한 탐지로 최신 API 목록 및 내역 유지

Drag here to set row groups				
Type	Host	Method	Path	Detected At ↓
New Auth	demo.nonamesec.com:8001	POST	/soap#SOAP:getuserid	2023-04-23 14:46
New Auth	demo.nonamesec.com:8001	POST	/soap#SOAP:checklogin	2023-04-23 14:46
New Auth	demo.nonamesec.com:8001	POST	/soap#SOAP:equal	2023-04-23 14:46
New Auth	demo.nonamesec.com:8001	POST	/soap#SOAP:echo	2023-04-23 14:46
New Auth	demo.nonamesec.com:8001	POST	/soap#SOAP:sum	2023-04-23 14:46
New Auth	demo.nonamesec.com:8001	POST	/soap#SOAP:createArray	2023-04-23 14:46
New Auth	demo.nonamesec.com:8001	POST	/soap#SOAP:createuser	2023-04-23 14:45
New API	demo.nonamesec.com:8001	POST	/soap#SOAP:getuserid	2023-04-23 14:45
New API	demo.nonamesec.com:8001	POST	/soap#SOAP:checklogin	2023-04-23 14:45
New API	demo.nonamesec.com:8001	POST	/soap#SOAP:equal	2023-04-23 14:45
New API	demo.nonamesec.com:8001	POST	/soap#SOAP:echo	2023-04-23 14:45
New API	demo.nonamesec.com:8001	POST	/soap#SOAP:sum	2023-04-23 14:45
New API	demo.nonamesec.com:8001	POST	/soap#SOAP:createArray	2023-04-23 14:45
New API	demo.nonamesec.com:8001	POST	/soap#SOAP:createuser	2023-04-23 14:44
Field Requirement Changed	demo.nonamesec.com:8025	GET	/api/v2/search	2023-04-04 22:53
New Header	demo.nonamesec.com:8888	POST	/identity/api/auth/signup	2023-03-29 20:28

변경 내용

변경된 API

Akamai API Security Platform – Noname

가시화 – Discover (API 데이터 식별)

> API에서 사용하는 중요 데이터(인증정보, 개인정보 등)를 자동 식별하여 중요 관리 대상 API 식별

Datatype ↑	In APIs (Requests) ⓘ	In APIs (Responses) ⓘ	Total Requests ⓘ	Total Responses ⓘ
Authorization	3	0	9	0
Coordinates	0	2	0	1695
Credit Card	0	2	0	300
Email	13	15	397337	659668
Full Name	0	3	0	376
Password	8	0	341408	0
Phone Number	0	2	0	300
SSN	0	2	0	300
URL	8	9	14448	14641

데이터 유형

API 사용 정보

Akamai API Security Platform – Noname

가시화 – Discover (API 사용자 식별)

> API 을 사용하는 사용자(또는 상대방)을 자동으로 식별하여 문제 발생 시 공격자 및 사용자를 식별하여 즉시 조치

Drag here to set row groups					
Alias	Identifier	Identifier Type	IPs	User Agent	Locations
54.177.52.174	54.177.52.174	IP	54.177.52.174	Mozilla/5.0 (Windows NT 10.0; Win6...	United States
Benjamin1053@mail.com	Benjamin1053@mail.com	Header	54.177.52.174	Mozilla/5.0 (Windows NT 10.0; Win6...	United States
Benjamin10551@mail.com	Benjamin10551@mail.com	Header	54.177.52.174	Mozilla/5.0 (Windows NT 10.0; Win6...	United States
Benjamin12610@mail.com	Benjamin12610@mail.com	Header	54.177.52.174	Mozilla/5.0 (Windows NT 10.0; Win6...	United States
Benjamin18445@mail.com	Benjamin18445@mail.com	Header	54.177.52.174	Mozilla/5.0 (Windows NT 10.0; Win6...	United States
Benjamin20900@mail.com	Benjamin20900@mail.com	Header	54.177.52.174	Mozilla/5.0 (Windows NT 10.0; Win6...	United States
Benjamin25947@mail.com	Benjamin25947@mail.com	Header	54.177.52.174	Mozilla/5.0 (Windows NT 10.0; Win6...	United States
Benjamin27352@mail.com	Benjamin27352@mail.com	Header	54.177.52.174	Mozilla/5.0 (Windows NT 10.0; Win6...	United States
Benjamin2783@mail.com	Benjamin2783@mail.com	Header	54.177.52.174	Mozilla/5.0 (Windows NT 10.0; Win6...	United States
Benjamin6630@mail.com	Benjamin6630@mail.com	Header	54.177.52.174	Mozilla/5.0 (Windows NT 10.0; Win6...	United States
Benjamin6680@mail.com	Benjamin6680@mail.com	Header	54.177.52.174	Mozilla/5.0 (Windows NT 10.0; Win6...	United States
Benjamin6943@mail.com	Benjamin6943@mail.com	Header	54.177.52.174	Mozilla/5.0 (Windows NT 10.0; Win6...	United States
Daniel12418@mail.com	Daniel12418@mail.com	Header	54.177.52.174	Mozilla/5.0 (Windows NT 10.0; Win6...	United States
Daniel28788@mail.com	Daniel28788@mail.com	Header	54.177.52.174	Mozilla/5.0 (Windows NT 10.0; Win6...	United States
Daniel3247@mail.com	Daniel3247@mail.com	Header	54.177.52.174	Mozilla/5.0 (Windows NT 10.0; Win6...	United States
Daniel3457@mail.com	Daniel3457@mail.com	Header	54.177.52.174	Mozilla/5.0 (Windows NT 10.0; Win6...	United States

사용자 정보

지역 및 Agent 정보

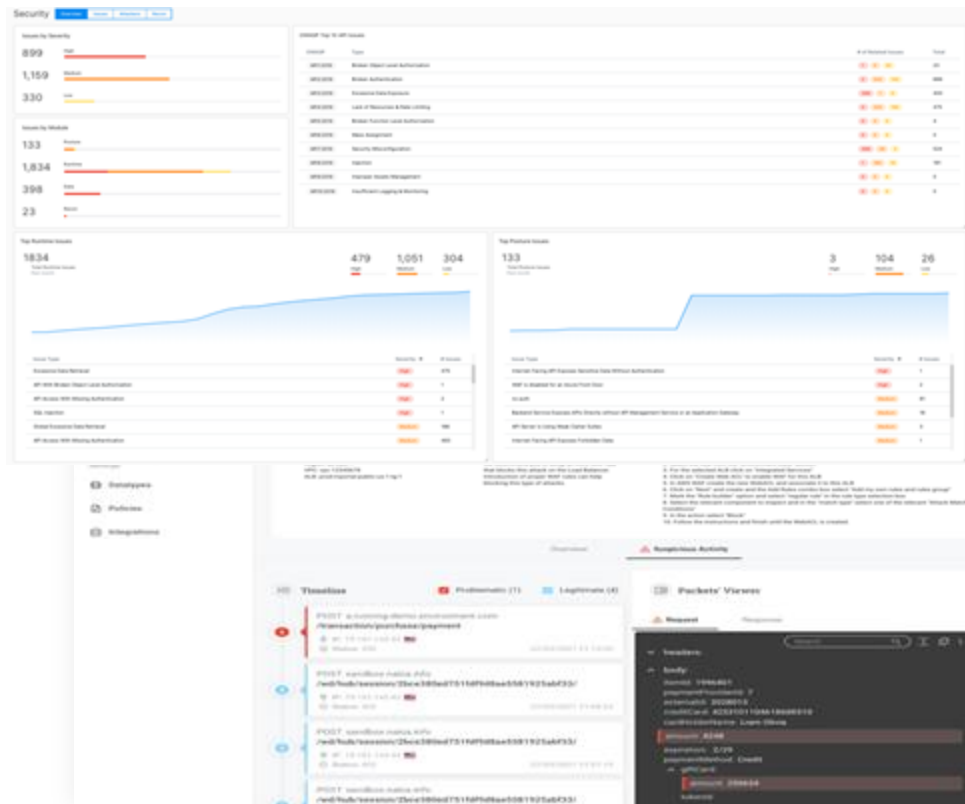
Akamai API Security Platform – Noname

위협 인지/분석 – Analyze



Analyze

- 잘못된 구성 탐지 및 취약점 탐지
- AI 기반의 공격자, 의심스러운 동작 탐지



Akamai API Security Platform – Noname

위협 인지/분석 – Analyze (이상징후 상세 정보)

- > 탐지된 이상징후에 대한 중요도 및 내용에 대한 자동 분류, 상세정보(내용, 조치방법 등) 제공
- > 탐지된 위협에 대한 트래픽 타임라인 및 상세 트래픽 정보 문제 내용에 대한 정보 제공

Module: Severity: Type:

Group ↑

- Data (2)
 - High (2)
 - Data Policy Violation (2)
- Posture (213)
 - High (25)
 - Azure App Service Directly Accessible From the Internet (5)
 - Azure App Service exposes APIs without API Management (1)
 - Internet Facing +No Auth (13)
 - Internet-Facing API Exposes Sensitive Data Without Authenticati... (2)
 - Internet-Facing API Receives Sensitive Data in Query Params (1)
 - Technical Information Exposed on Server Header (1)
 - WAF is disabled for an Azure Front Door (2)
 - Medium (134)
 - API Exposes Excessive Data in an Older Version (1)
 - API Server is Using Weak Cipher Suites (3)
 - An API accepts expired JWT (1)

API Access With Malformed Authentication

Detection Time: 2023-02-21 14:48

Evidence Block Attacker Take Action Status Open

What Happened

사용자는 손상된 인증으로 API에 성공적으로 접속하였습니다.:

- 인증 유형: Cookie
- 결정된 값: null

Why That's a Problem

잘못된 인증으로 API에 접근하면 API의 인증 무효화를 나타냅니다. API의 인증 메커니즘을 무효함으로써 공격자는 다른 사용자

API With Broken Object Level Authorization

What You Should

- 'Evidence'에
 - 인증 유형
 - API에
- API에 성공하
- 임에 긴급 태
- 공격자를 차단

How To Investigate

Incident Result: Succeeded

API Information

Triggered on: POST nci.akamai.com

Attackers Timeline	Type	API	Client IP	Request Timestamp	Status
1	API With Broken Object L...	GET demo.nonameapi.com/api/v2/accounts/8176-417...	204.30.68.159	2023-01-01 10:11	200
2	API With Broken Object L...	GET demo.nonameapi.com/api/v2/accounts/77347763-947...	204.30.68.159	2023-01-01 10:25	200
3	API With Broken Object L...	GET demo.nonameapi.com/api/v2/accounts/535206-8ba...	204.30.68.159	2023-01-04 10:11	200
4	API With Broken Object L...	GET demo.nonameapi.com/api/v2/accounts/90cf269-8a6...	204.30.68.159	2023-01-06 14:24	404
5	API With Broken Object L...	GET demo.nonameapi.com/api/v2/accounts/90cf269-8a6...	204.30.68.159	2023-01-06 14:24	200

Request

```
GET /api/v2/accounts/8176-4176-8484-149858324432/details HTTP/1.1
Host: demo.nonameapi.com
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/108.0.0.0 Safari/537.36
Accept: application/json
Accept-Encoding: gzip, deflate
Referer: https://demo.nonameapi.com/
```

Response

```
HTTP/1.1 200 OK
Content-Type: application/json
Content-Length: 1024
Server: Apache/2.4.18 (Ubuntu)
Date: Mon, 01 Jan 2023 10:11:11 GMT
Access-Control-Allow-Origin: *
Access-Control-Allow-Headers: X-Requested-With, X-JSON-Response
Access-Control-Allow-Methods: GET, POST, PUT, DELETE, PATCH, OPTIONS
Cache-Control: no-cache, no-store, max-age=0, must-revalidate
Expires: 0
Pragma: no-cache
```

트래픽 정보 및 문제
인식 정보

Akamai API Security Platform – Noname

위협 인지/분석 – Analyze (공격자 정보)

> 이상징후와 관련된 공격자 정보를 식별하여 중요 이상징후 발생 시 공격자 차단 등 정책 결정 정보 제공

Drag here to set row groups												
Last Attack Time	1 ↓	Identifier	Identifier Type	Issues	Risk Score	2 ↓	IPs	Locations	User-Agents	Atten	Is Blocked	
2023-04-10 01:38		mike@mail...	JWT	1 1 0	Medium		37.1... +1	Israel	Script Postm... +1	8	False	
2023-04-04 15:17		kleingrego...	JWT	2 5 3	High		109... +1	France	Chrome 90.0.4430.9...	10	False	
2023-03-30 14:52		3.11.23.240	IP	0 0 4	Low		3.11.23.240	United Ki	Chrome Hea... +22	4	False	
2023-03-30 08:20		18.117.238....	IP	0 0 1	Low		18.117.238....	United St	Chrome 74.0.3... +1	1	False	
2023-03-30 03:40		35.178.144...	IP	0 0 3	Low		35.178.144...	United Ki	Chrome 41.0... +23	3	False	
2023-03-30 03:39		52.56.195....	IP	0 0 7	Low		52.56.195....	United Ki	Chrome 35.0... +21	7	False	
2023-03-30 00:15		77.137.35....	IP	15 62 3	High		77.137.35....	Israel	Firefox 88.0 o... +7	101	False	
2023-03-29 20:44		james.san...	JWT	0 1 0	Low		77.137.35....	Israel	Script python-requ...	1	False	
2023-03-29 15:58		62.219.65....	IP	0 7 0	High		62.219.65....	Israel	Script python-requ...	7	False	
2023-03-28 21:52		shoop@m...	JWT	1 1 0	Medium		62.2... +1	Israel	Script python-requ...	2	False	
2023-03-27 10:54		54.177.52.1...	IP	617 662 C	High		54.177.52.1...	United St	Firefox 88.0 o... +1	1372	False	

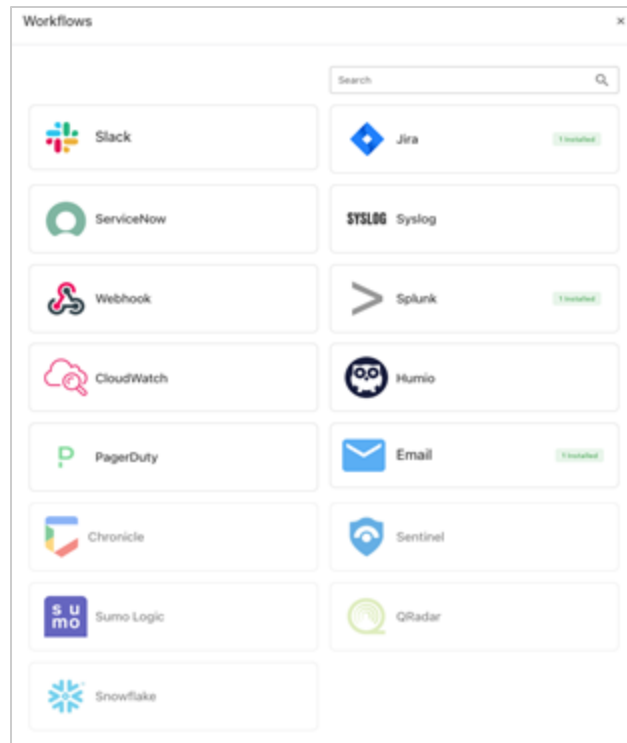
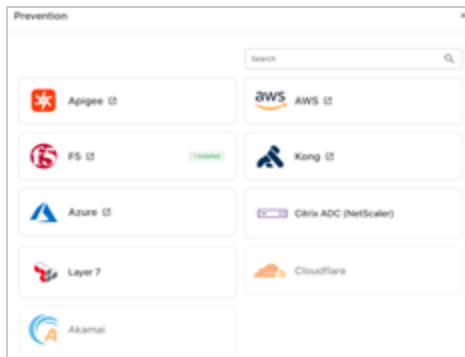
Akamai API Security Platform – Noname

문제 교정 - Remediate



Remediate

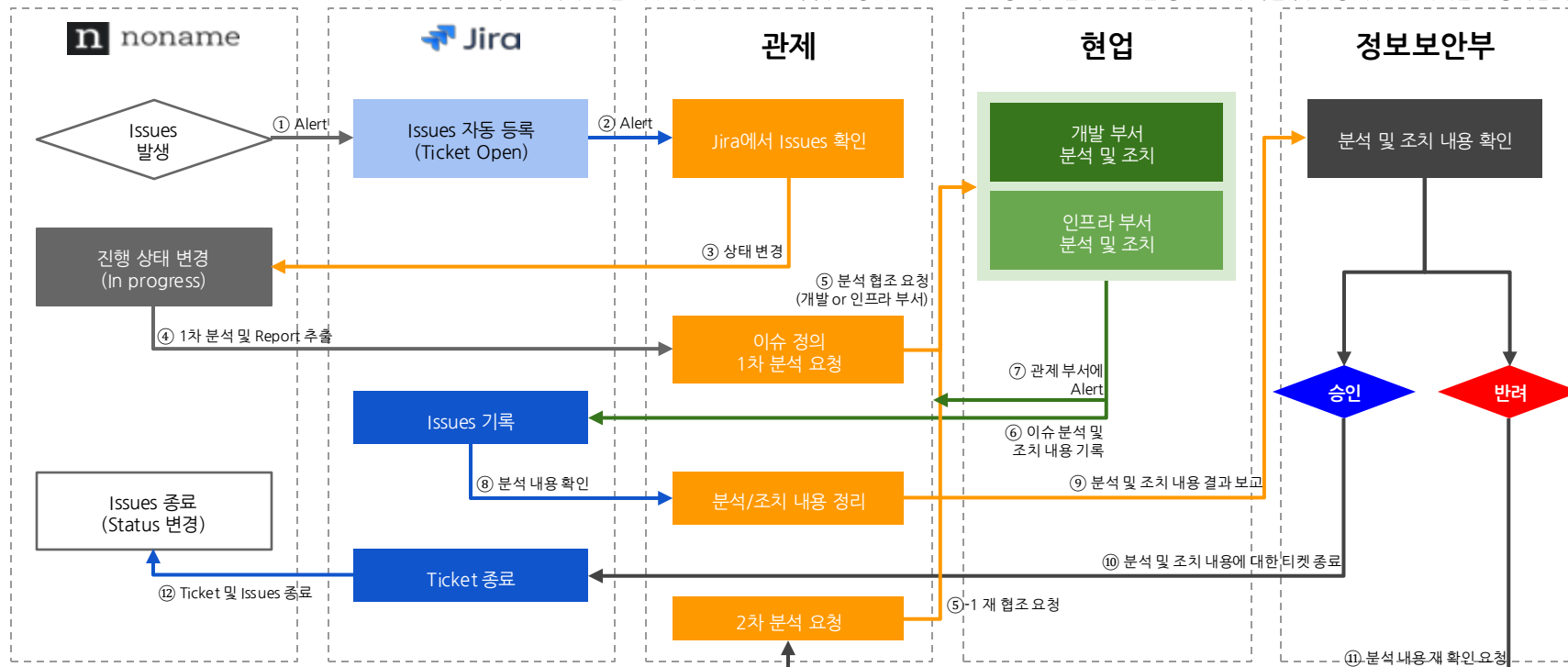
＞ 공격을 차단하고 기존 워크플로를 활용하여 취약성 및 잘못된 구성 해결



Akamai API Security Platform – Noname

문제 교정 - Remediate (조치 자동화)

> Noname은 각 API 서비스 별 이상징후에 대한 분석 및 대응 방안으로 JIRA 등 워크플로 연계를 통해 문제 식별 및 대응에 대한 체계를 자동화합니다.



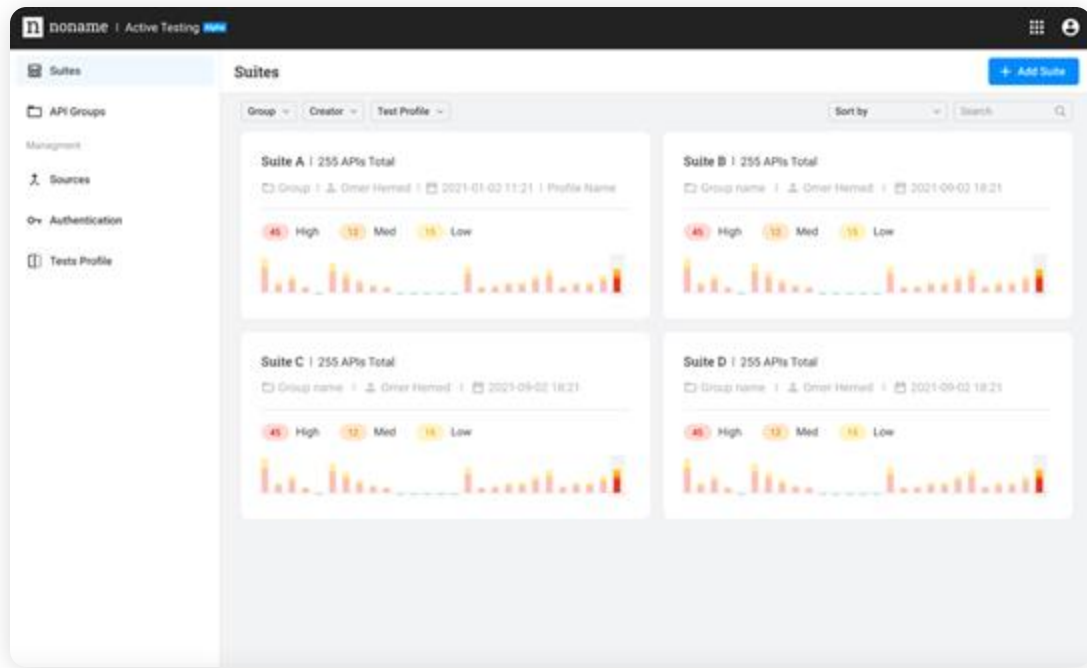
Akamai API Security Platform – Noname

능동적 보안 테스트 - Active Testing



Test

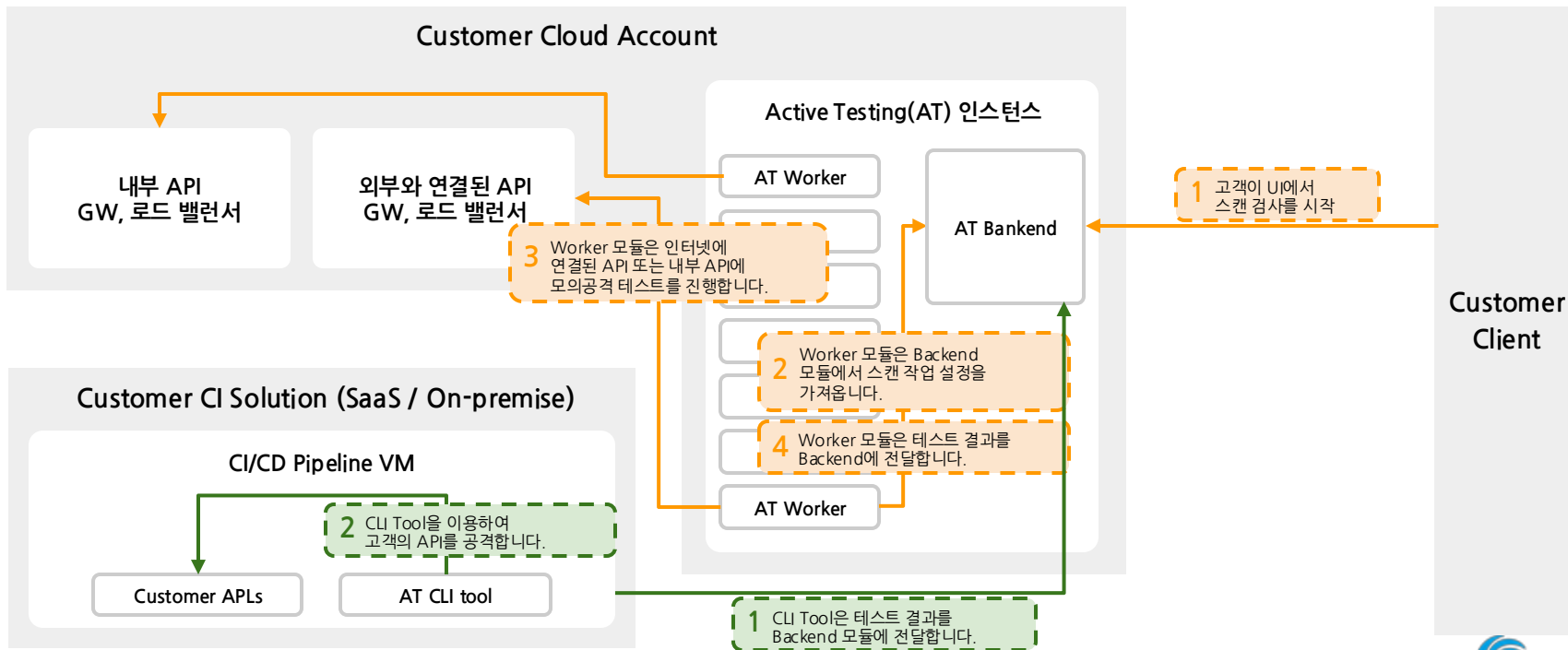
- > 운영 전에 API의 무결성을 적극적으로 테스트
- > 문제 발견 및 검증
- > CI/CD와 연계하여 개발시 실시간 검증
(학습기반으로 문제를 테스트)



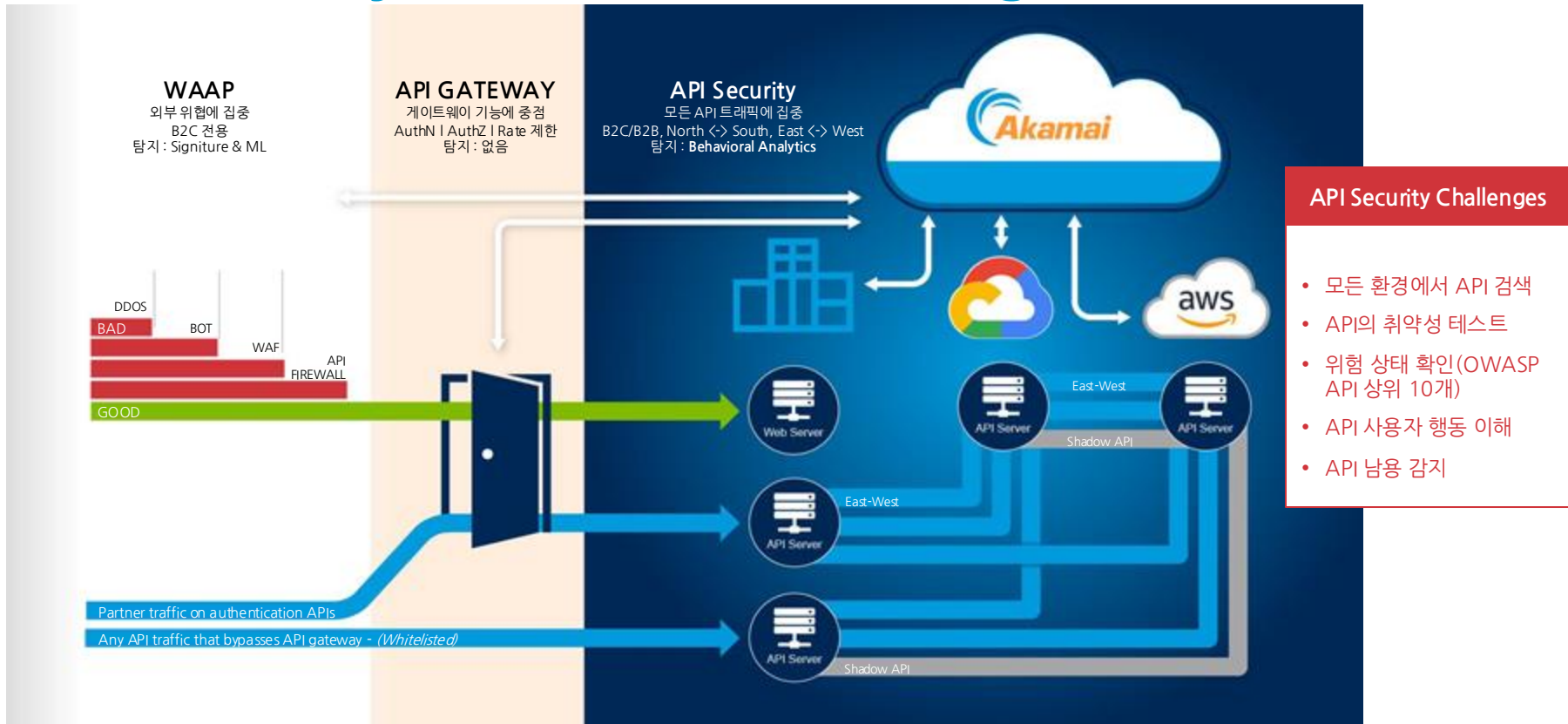
Akamai API Security Platform – Noname

능동적 보안 테스트 - Active Testing

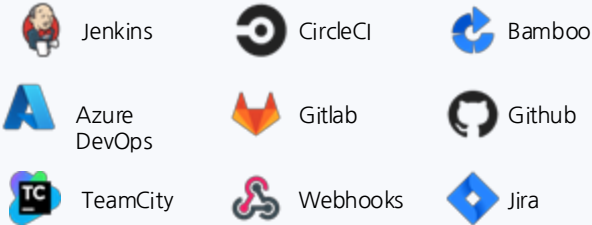
> On-Premise, SaaS, Hybrid 구성을 지원하며 On-Premise 구성의 경우, 스캔 및 모의 공격을 담당하는 Active Testing(AT) Backend 모듈과 AT Worker 모듈을 포함하여 플랫폼의 모든 구성 요소가 고객의 인프라에 호스팅되며 내부 API에 액세스하여 검사할 수 있습니다.



API Security Solution Positioning



Development Platforms

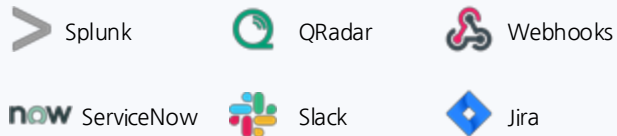


Traffic Source (Network and Cloud)



Akamai API Security Platform Ecosystem

Workflow Integrations



API Gateway



* Speak to us for more details of other integration options

API Security Deployment Options

SaaS

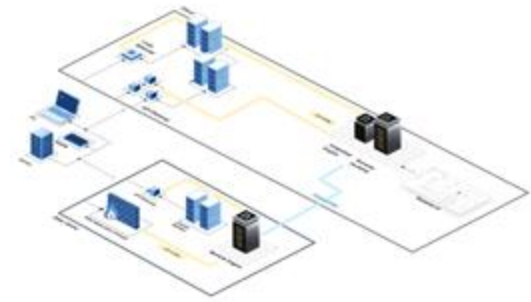
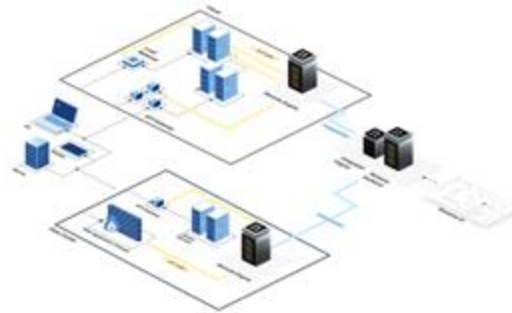
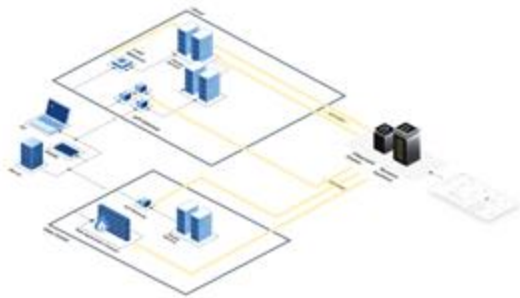
Akamai API Security manages the Akamai API Security Platform in the cloud.

Hybrid

Deploy remote engines into customer environment e.g. your data centre or cloud

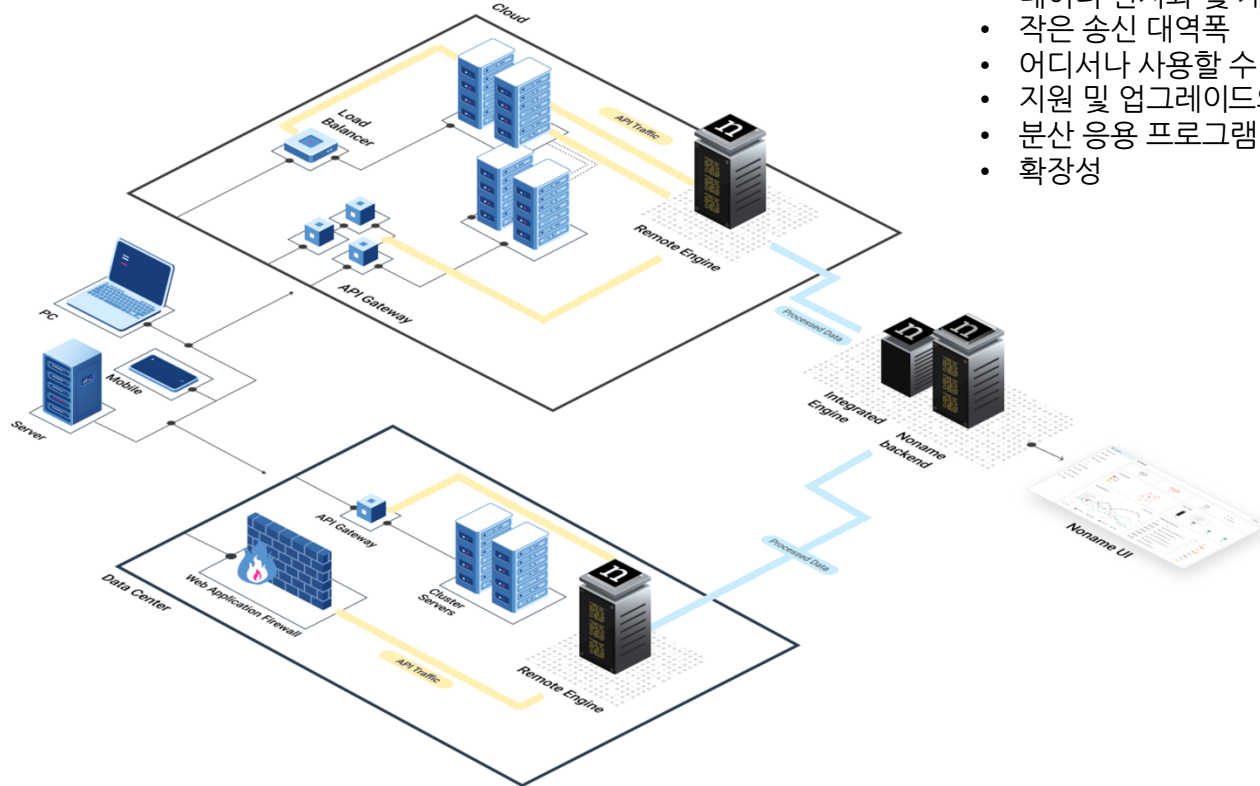
On-Prem

Backend and its UI and management API, is installed at your data center or private cloud.



Akamai API Security Platform – Noname

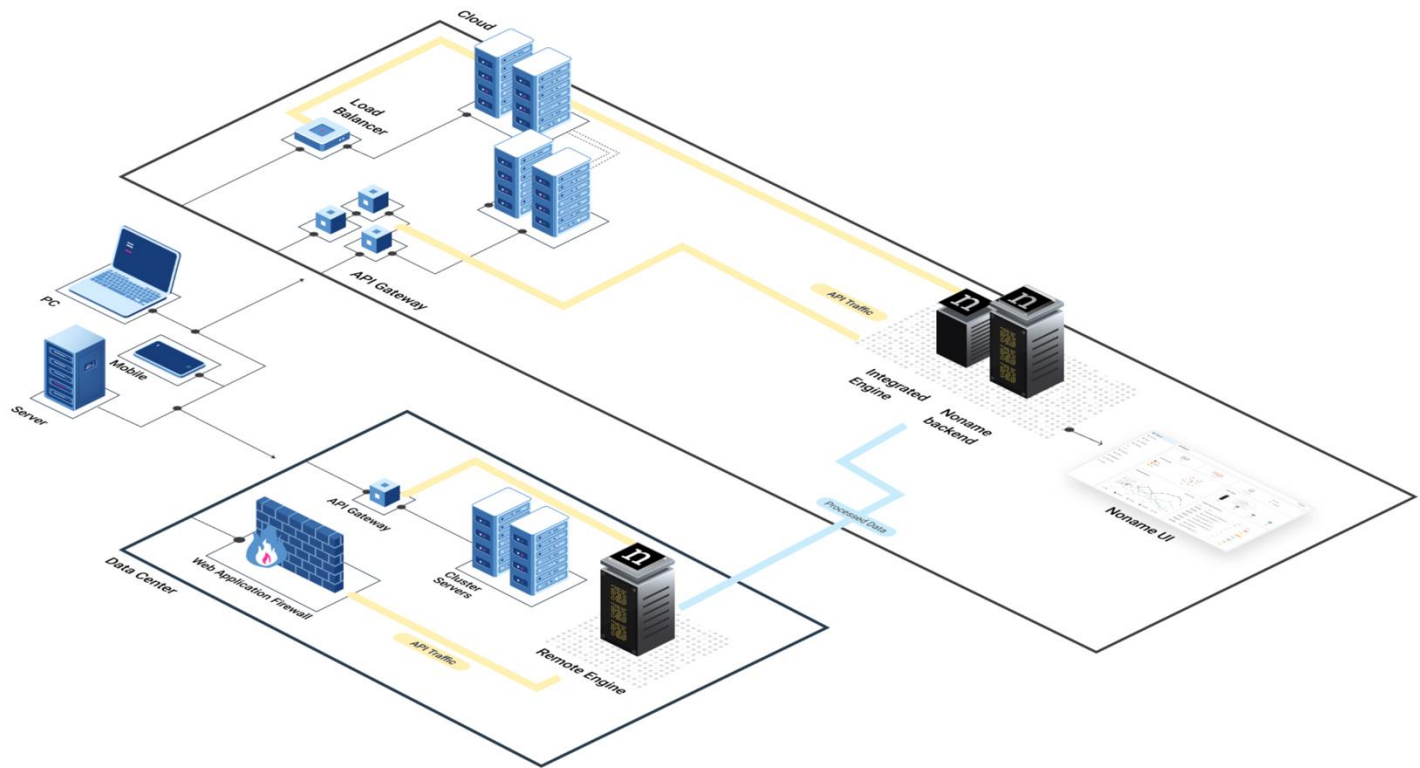
구축 옵션 – Hybrid Model Deployment



- 데이터 현지화 및 개인 정보 보호
- 작은 송신 대역폭
- 어디서나 사용할 수 있는 관리 서버
- 지원 및 업그레이드의 용이성
- 분산 응용 프로그램 아키텍처 지원
- 확장성

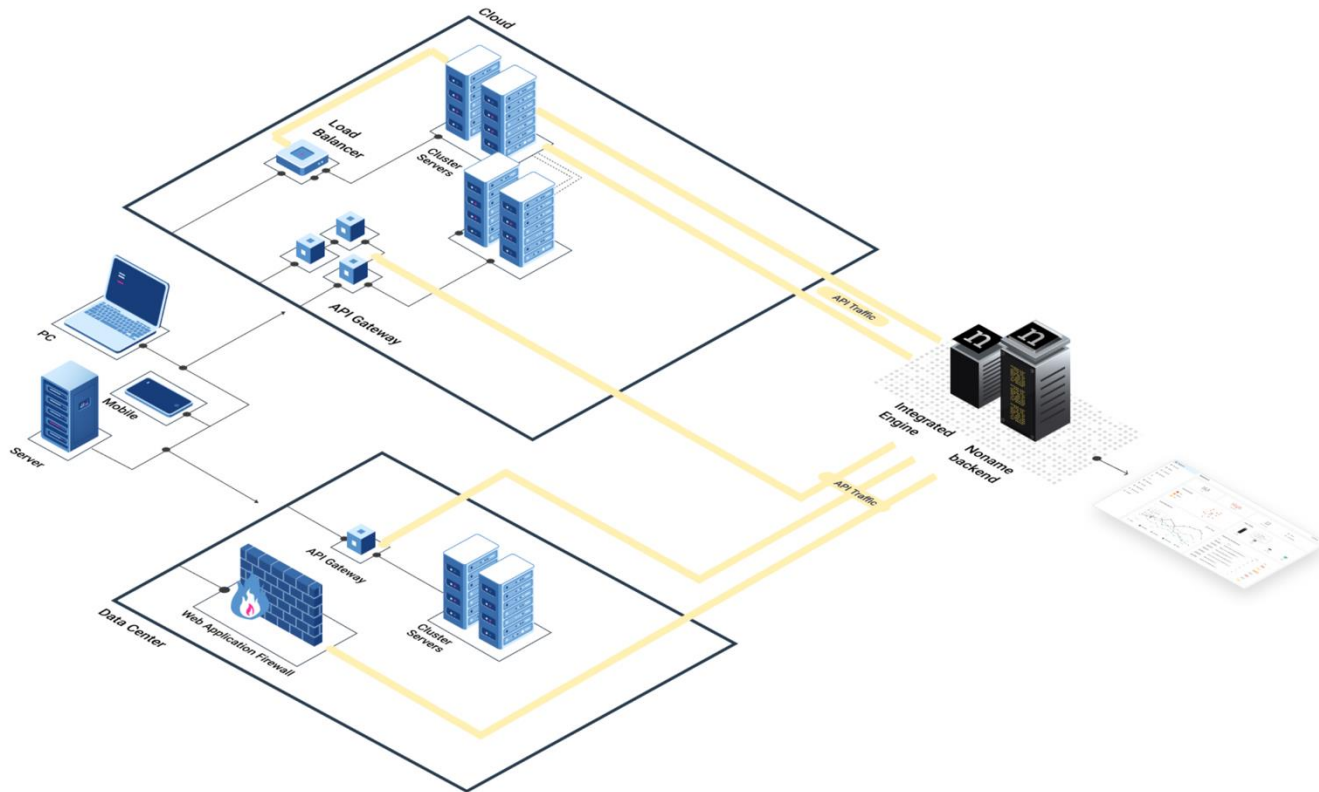
Akamai API Security Platform – Noname

구축 옵션 – Customer Managed Deployment (On-premises)



Akamai API Security Platform – Noname

구축 옵션 – SaaS Deployment



Akamai API Security Platform – Noname

Akamai API Security Platform에 대한 시장 평가



GOLD
Fastest Growing Cybersecurity Company
North America



GOLD
API Security category
North America



Cybersecurity Posture



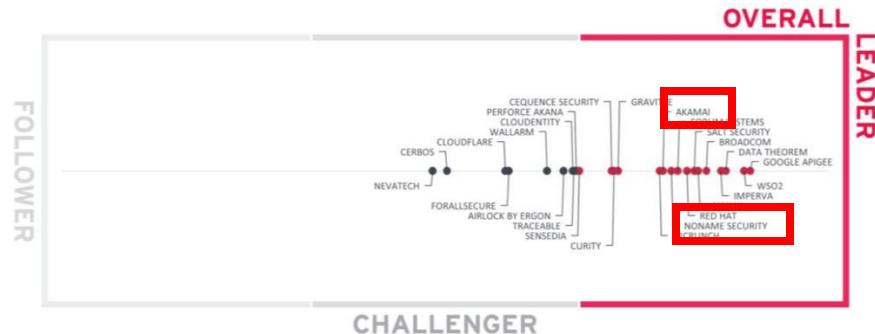
Security Platform



API Security



Attack Surface Management



< Leadership Compass : API Security and Management by Kuppingercole, 2024 >

