

마이크로 서비스로 가기 위한 다르지만 같은 길, API 보안과 게이트웨이

F5 NETWORKS
이종민 부장

 ©2018 F5 NETWORKS

진화하는 앱의 변화

2000
초기 개발 이후 구조 및 기능 유지
모놀리식
단일 클러스터
데이터센터

현대
반복적인 개발
API를 이용한 느슨한 결합식
멀티 클러스터
데이터센서 | 퍼블릭 / 브라이빗 클라우드

마이크로 서비스의 핵심, API

75%

의 기업은 향후 10년 안에 디지털 트랜스포메이션을 완료할 것입니다. 그렇지 않는 기업은 살아남지 못 할 것입니다.

By 2022

90%

의 새로운 앱은 마이크로서비스 아키텍처를 사용할 것입니다. 35% 의 생선성 앱의 경우 클라우드 기반에서 서비스 될 것으로 예상됩니다.

참조: IDC / https://idc.com

API 에 대한 보안 취약성 증가

OWASP TOP10 2017

A3:2017- Sensitive Data Exposure

많은 웹 응용 프로그램 및 API 를 통해 취약한 데이터 (주민등록번호, 계좌번호) 가 탈취되거나 수정될 수 있습니다.

A7:2017- Cross-Site Scripting (XSS)

브라우저 API 를 이용하여 기존 사용자 세션으로 웹페이지를 업데이트 할 때 발생합니다.

A9:2017- Using Components with Known Vulnerabilities

알려진 취약점이있는 구성 요소를 사용하는 응용 프로그램 및 API 는 응용 프로그램 방어에 대한 권한 악용 시 보안을 약화시키고 다양한 공격에 영향을 받알 수 있습니다.

참조: https://www.owasp.org/index.php/Top_10-2017_Top_10

API 서비스를 위한 필수 조건



원할한 API 서비스 아키텍처

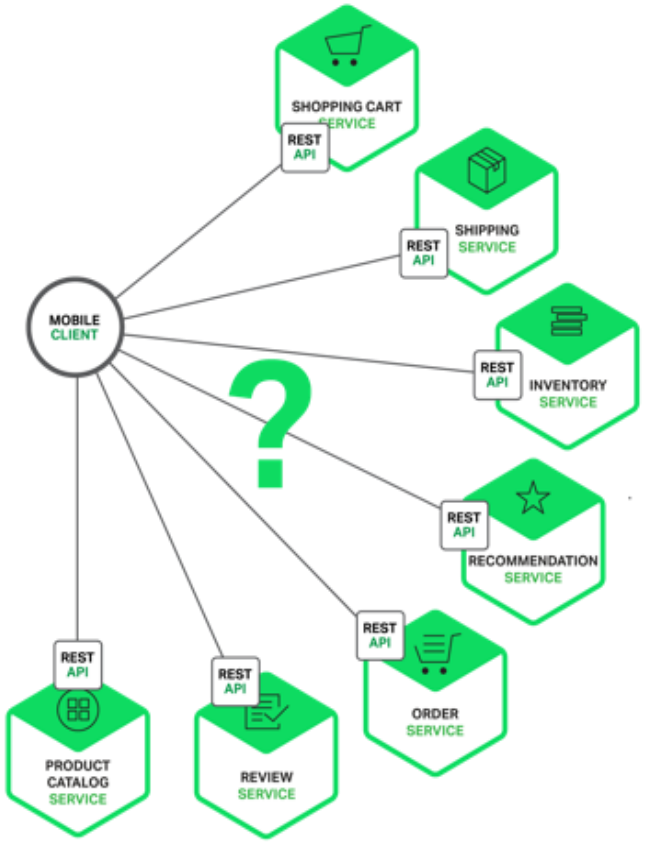


API 보안 아키텍처

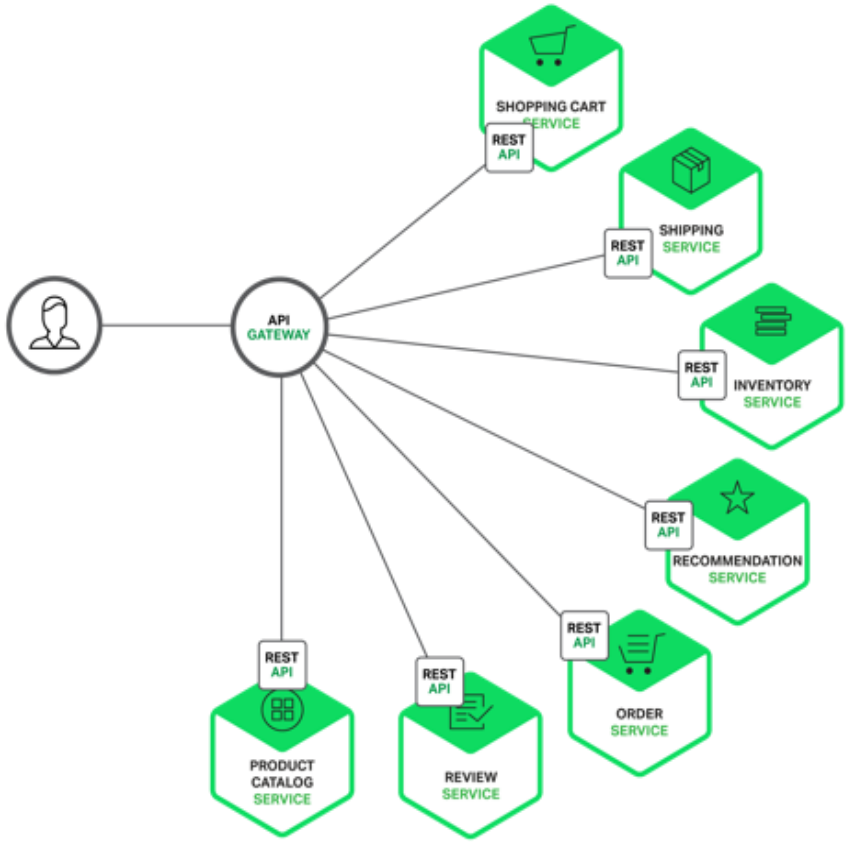
NGINX

원할한 API 서비스 아키텍처 - API Gateway

원할한 API 서비스 아키텍처의 필요



네트워크 데이터 대용량 소모



서비스의 엔드포인트 통합 필요

API, 컨테이너, 마이크로 서비스의 도전과제

컨테이너는 API 관리에 대한 챌린지를 제기합니다.

54%

현재의 API 관리 솔루션은 컨테이너 환경에서의 개선점 사항이 존재합니다.

Vendors need to rethink their solutions taking into account the dependencies and challenges containers bring



#1 PAIN POINT — **35%** API 관리 솔루션의 리소스 점유

#2 PAIN POINT — **35%** 인프라와 어플리케이션에 대한 복잡성

#3 PAIN POINT — **27%** 성능

#4 PAIN POINT — **25%** 가격

참조: IDC / https://idc.com

원할한 API 서비스를 위한 API Gateway의 “Must Have” 기능

- 기술지원 – 낮은 리소스 점유, 익숙한 인터페이스, 원할한 기술지원
- 직관성 - 직관적인 GUI 지원
- 비용절감 - API 처리에 대한 비용절감
- 성능 - API Gateway 의 대용량 성능 지원
- 신속한 개발 속도
- 보안 기능

원할한 API 서비스를 위한 API Gateway의 “Must Have” 기능, 기술지원



Open Source-Driven

일년간 9천만건 다운로드
탑 고객사의 약 66% 가 Nginx 사용
375 백만개의 웹사이트가 Nginx 사용



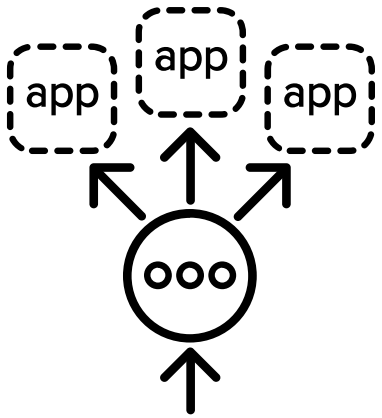
Enterprise-Driven

25,000 개의 고객사 확보
글로벌 ADC 업계 1위 벤더
포춘 50개 업체 중 49개가 F5 사용

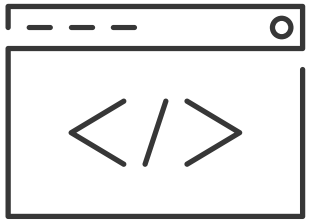
원할한 기술 지원 및 Nginx의 기존 인터페이스 사용

원할한 API 서비스를 위한 API Gateway의 “Must Have” 기능, 직관성

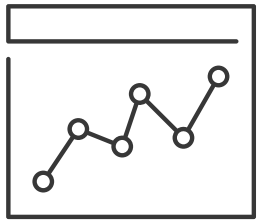
API Gateway

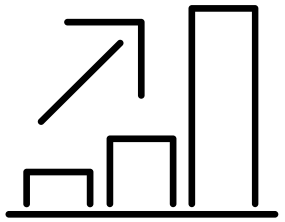


API Management



App 개발자를 위한 포털 제공

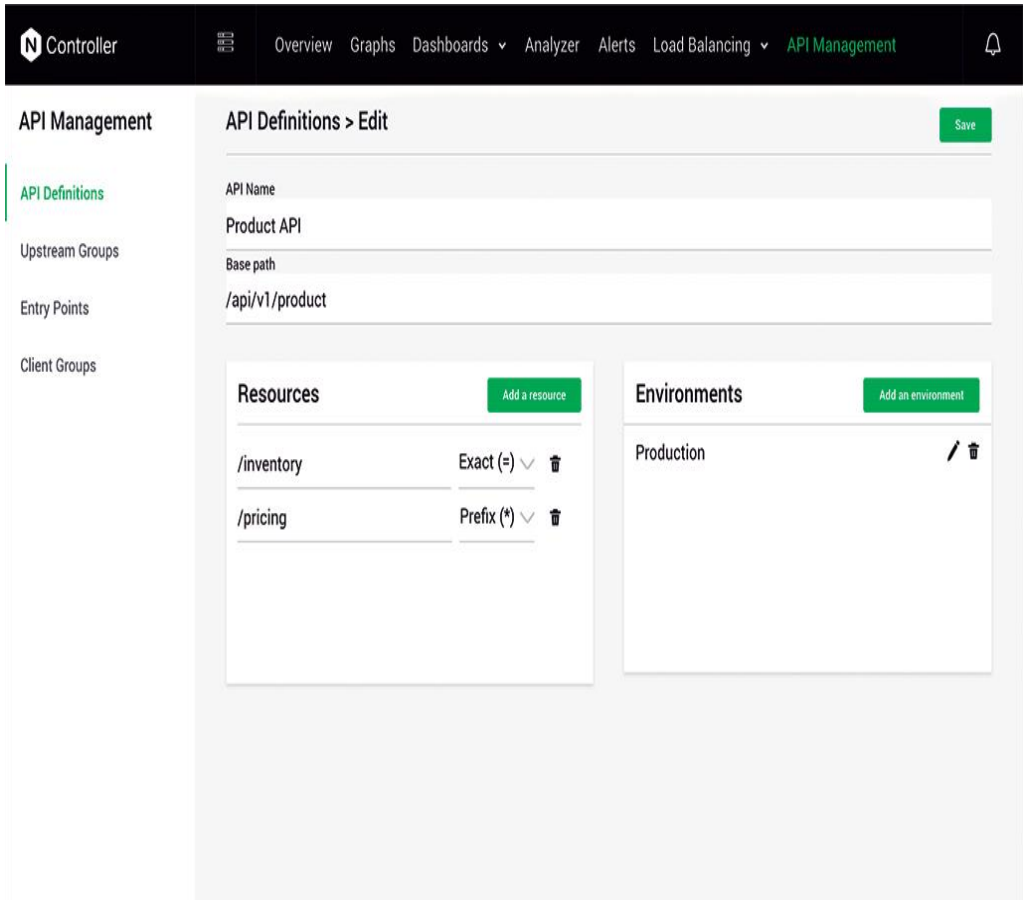


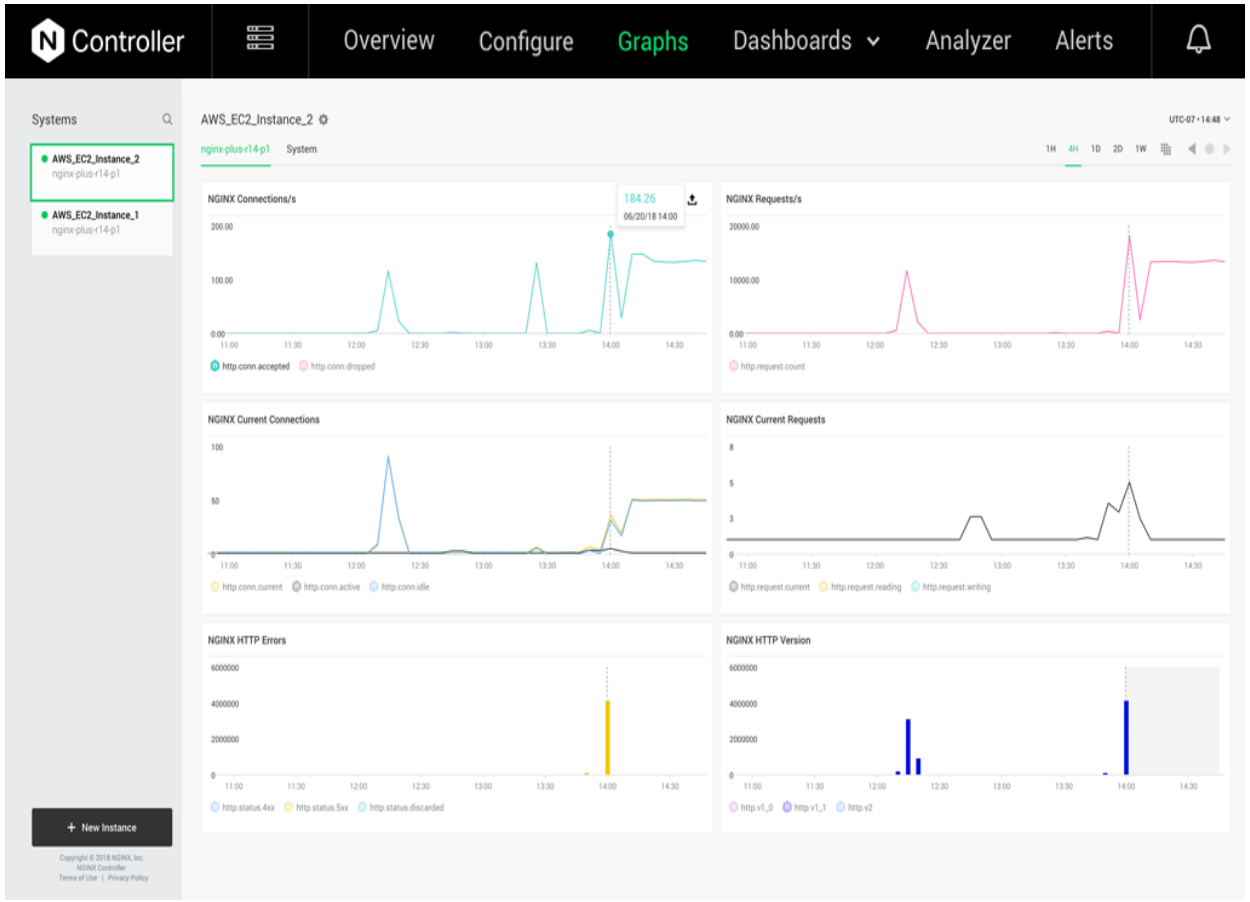


- ✓ API 분석, 사용량 분석,
- ✓ 행동 분석 툴,
- ✓ 정책 설정 툴 제공

직관적인 설정, 모니터링 GUI 지원

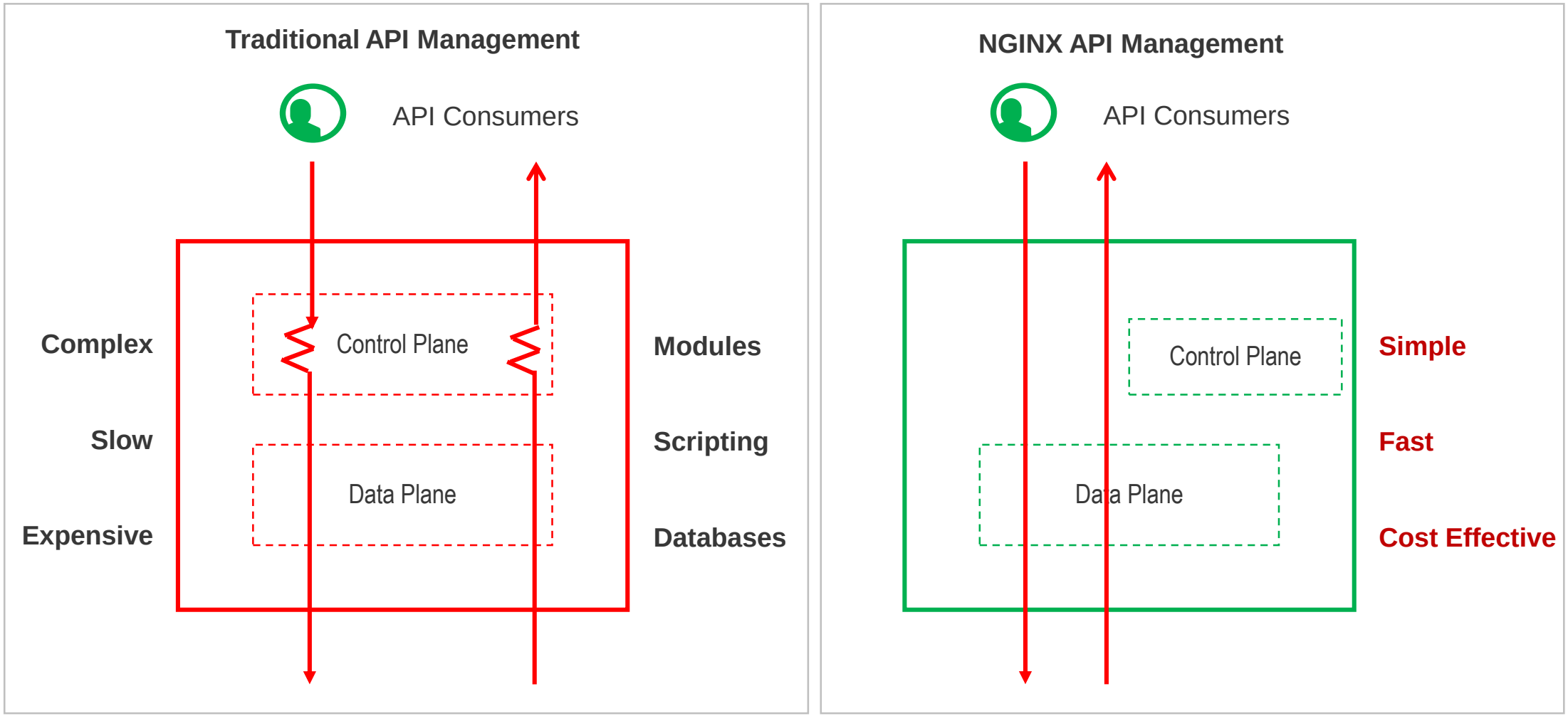
원할한 API 서비스를 위한 API Gateway의 “Must Have” 기능, 직관성





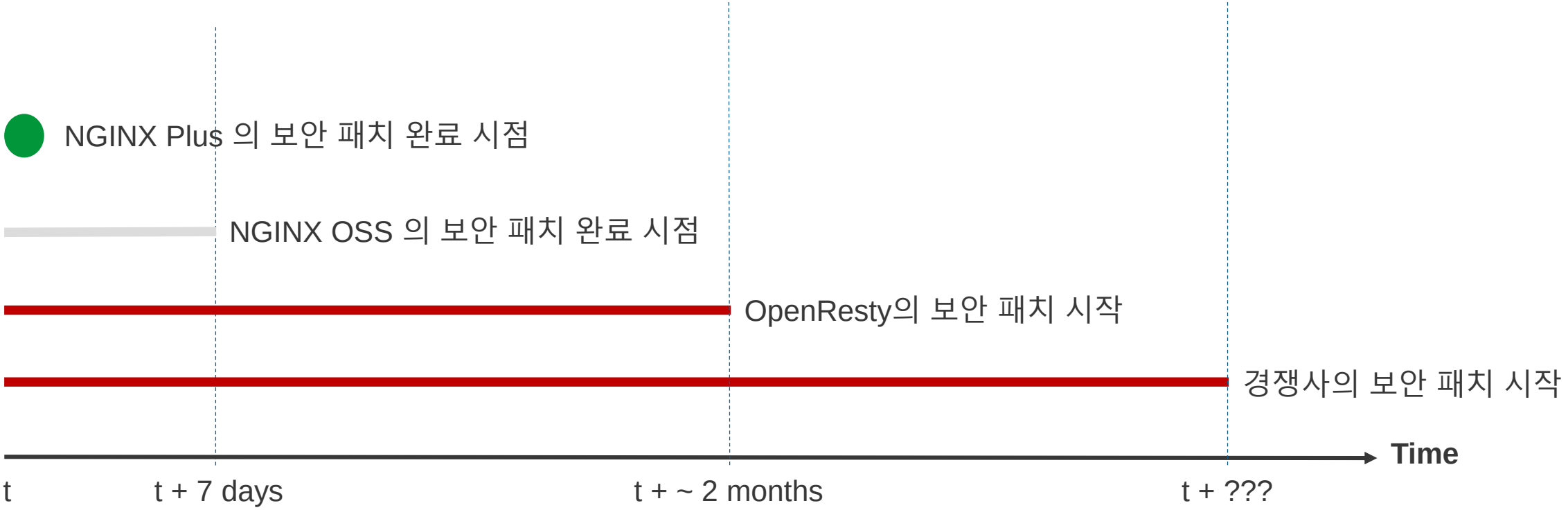
직관적인 설정, 모니터링 GUI 지원

원할한 API 서비스를 위한 API Gateway의 “Must Have” 기능, 비용절감



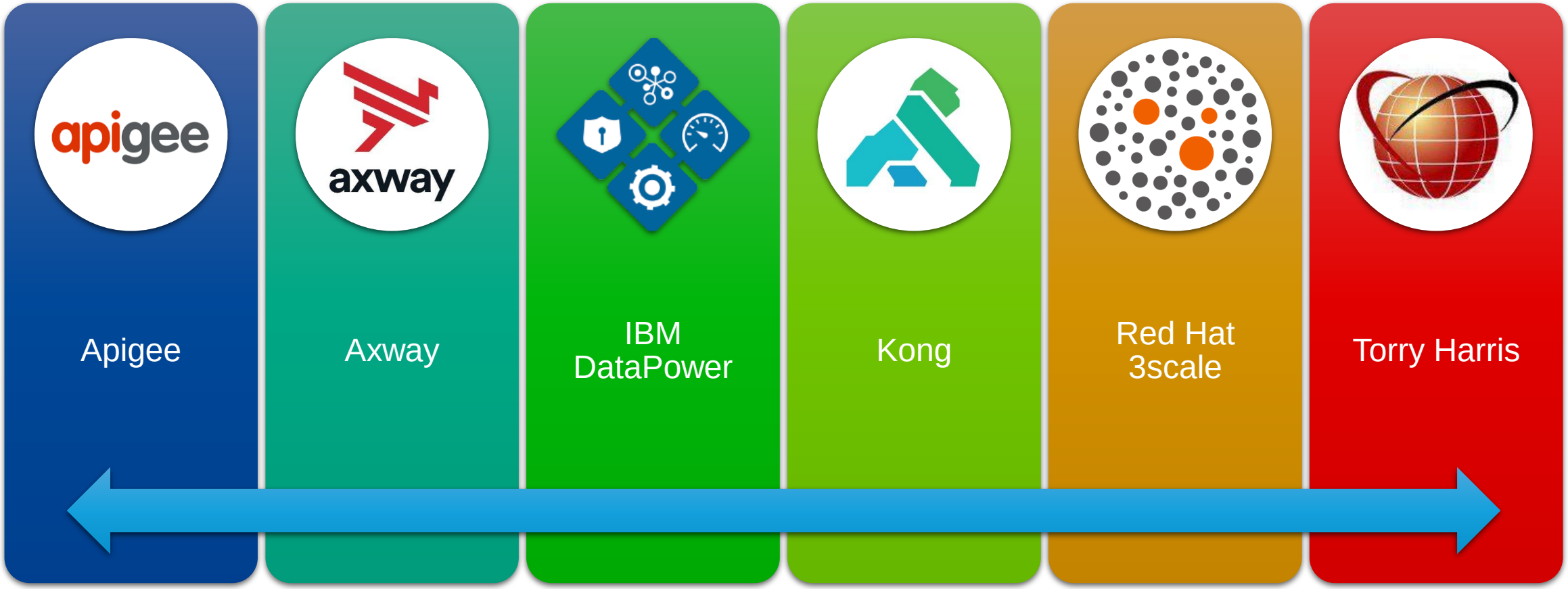
API 처리에 대한 딜레이 감소 및 비용절감

원할한 API 서비스를 위한 API Gateway의 “Must Have” 기능, 개발속도



NGINX OSS를 코어로 사용하는 공급 업체는 고객을 취약하게 만듭니다!

Nginx 는 오리지널 솔루션입니다.



원할한 API 서비스를 위한 API Gateway의 “Must Have” 기능, API 보안



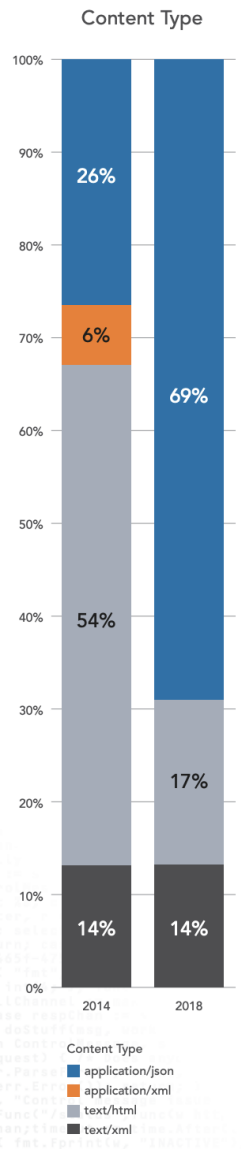


API 보안 아키텍처

API 보안 아키텍처의 필요성

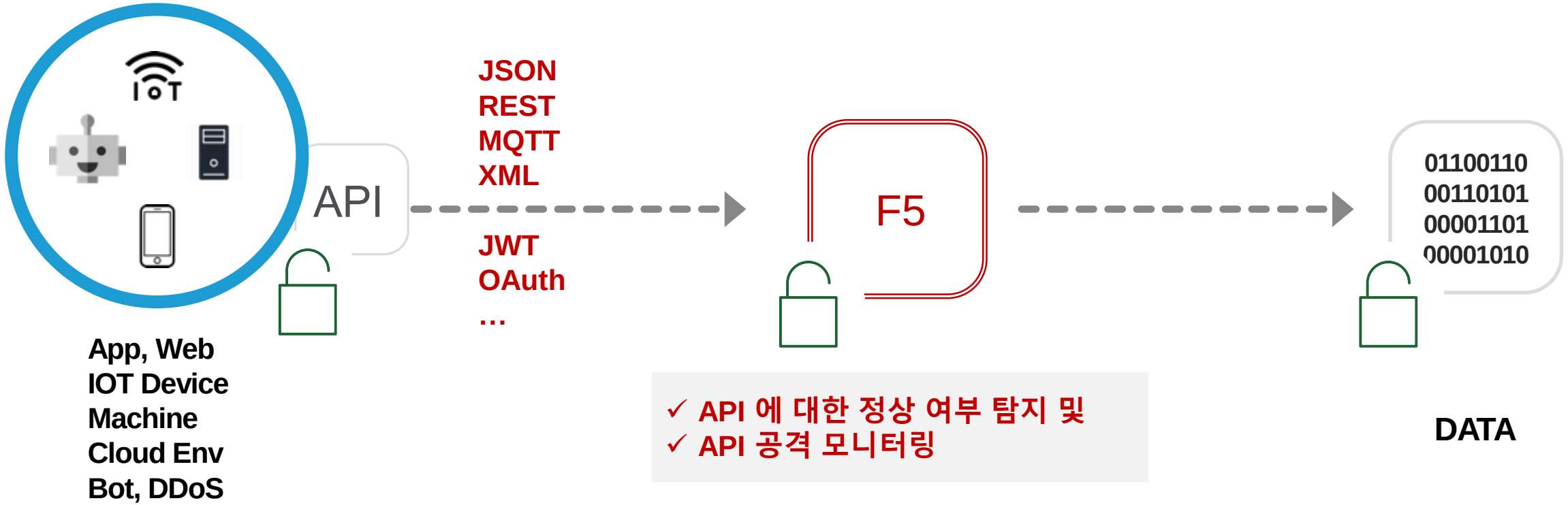
83%

인터넷 트래픽의 83%는 API 트래픽으로 확인(JSON/XML)



Source: Akamai State of the Internet Feb-2019

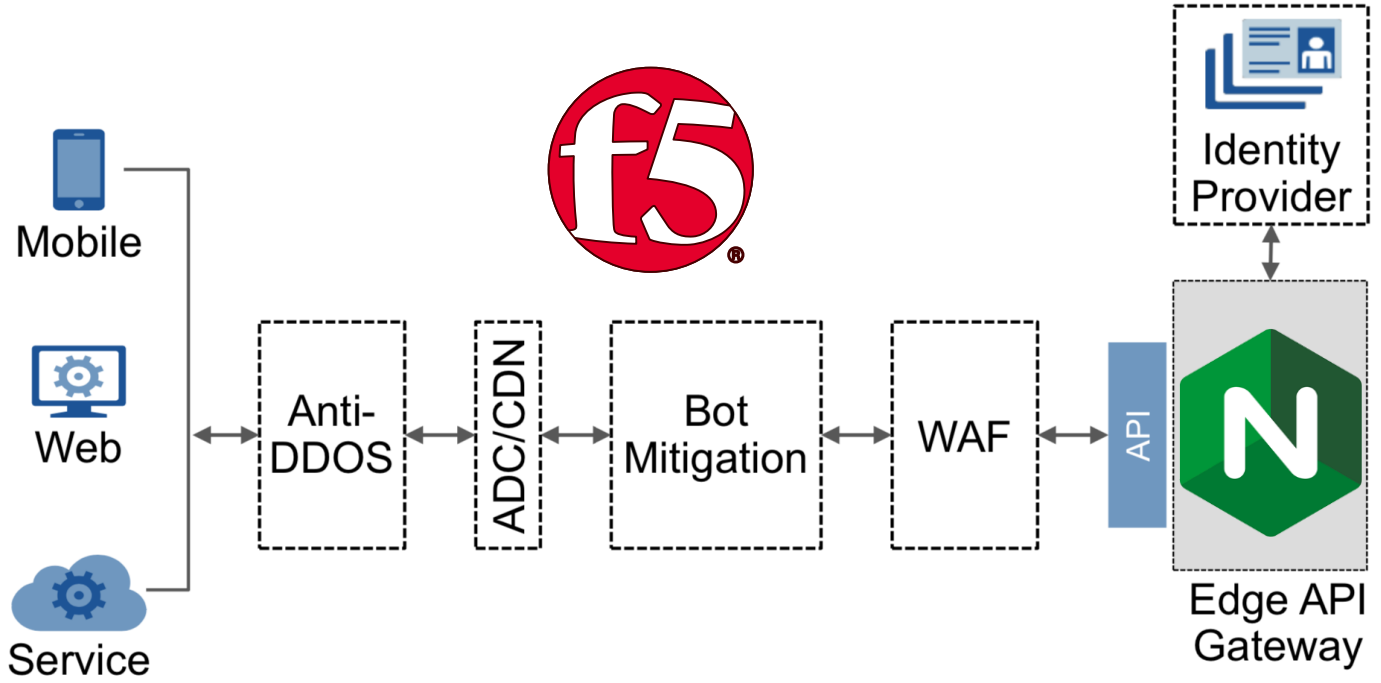
API 이용환경과 직면한 사이버위협



클라우드 고객을 위한 API 보안/탐지/모니터링 기능을 제공합니다.

가트너에서 제안하는 API 보안 아키텍처

Example Relationship With Other Protection Tools — 1



Gartner

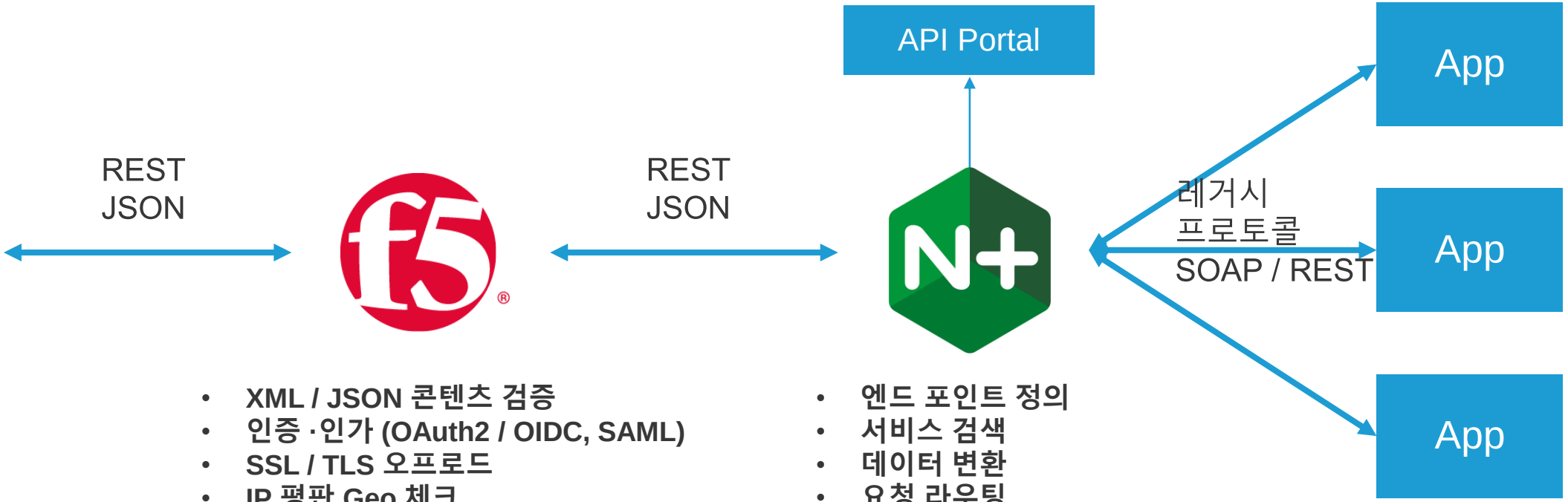
26 © 2018 Gartner, Inc. and/or its affiliates. All rights reserved.

OWASP 에서 제안하는 API 보안 체크사항



1. HTTPS
2. Access Control (인증)
3. JWT (MAC / 무결성보호)
4. API Keys (Key 보호)
5. Restrict HTTP methods
6. Input validation
7. Validate content types
8. Management endpoints (2 Factor 인증)
9. Error handling
10. Audit logs
11. Security headers
12. Sensitive information in HTTP requests
13. HTTP Return Code

F5 / Nginx 에서 제안하는 API 보안 아키텍처



- XML / JSON 콘텐츠 검증
- 인증 ·인가 (OAuth2 / OIDC, SAML)
- SSL / TLS 오프로드
- IP 평판,Geo 체크
- BOT 방어
- DDoS 방어
- 데이터 마스킹
- URL / 매개 변수 확인 및 제어
- OWASP TOP10 방어
- 레포팅

- 엔드 포인트 정의
- 서비스 검색
- 데이터 변환
- 요청 라우팅
- Microgateway 기능 (Kubenetes Ingress Controller)
- 메시지 변환
- API Key / JWT 검증
- SW 로드밸런싱
- 캐시 / 속도 제한
- API 사용 레포팅
- BASIC WAF기능

API 보안 기능 / API 제어

Access ›› API Protection : Profile ›› PetStore

Properties | Paths | Responses | Access Control

Paths

Create

Path ID	URI	Method	Server	Description	Active
1	/pet	PUT			true
2	/pet	POST			true
3	/pet/findByStatus	GET		Multiple status values can be provided with comma separated strings	true
4	/pet/findByTags	GET		Muliple tags can be provided with comma separated strings. Use tag1, tag2, tag3 for testing.	true
5	/pet/*	GET		Returns a single pet	true
6	/pet/*	POST			true
7	/pet/*	DELETE			true
8	/pet/*/uploadImage	POST			true
9	/store/inventory	GET		Returns a map of status codes to quantities	true
10	/store/order	POST			true

Delete

Page 1 of 2

Servers

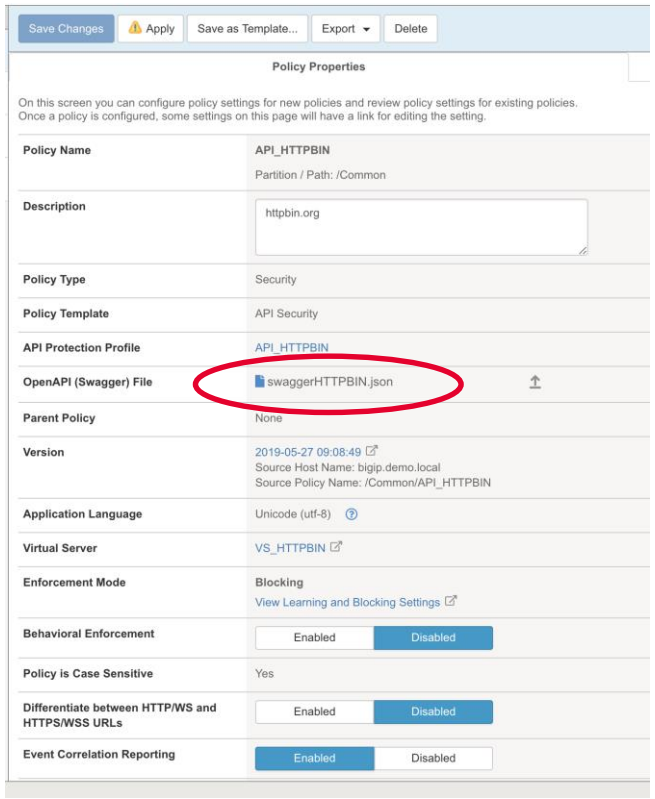
Create

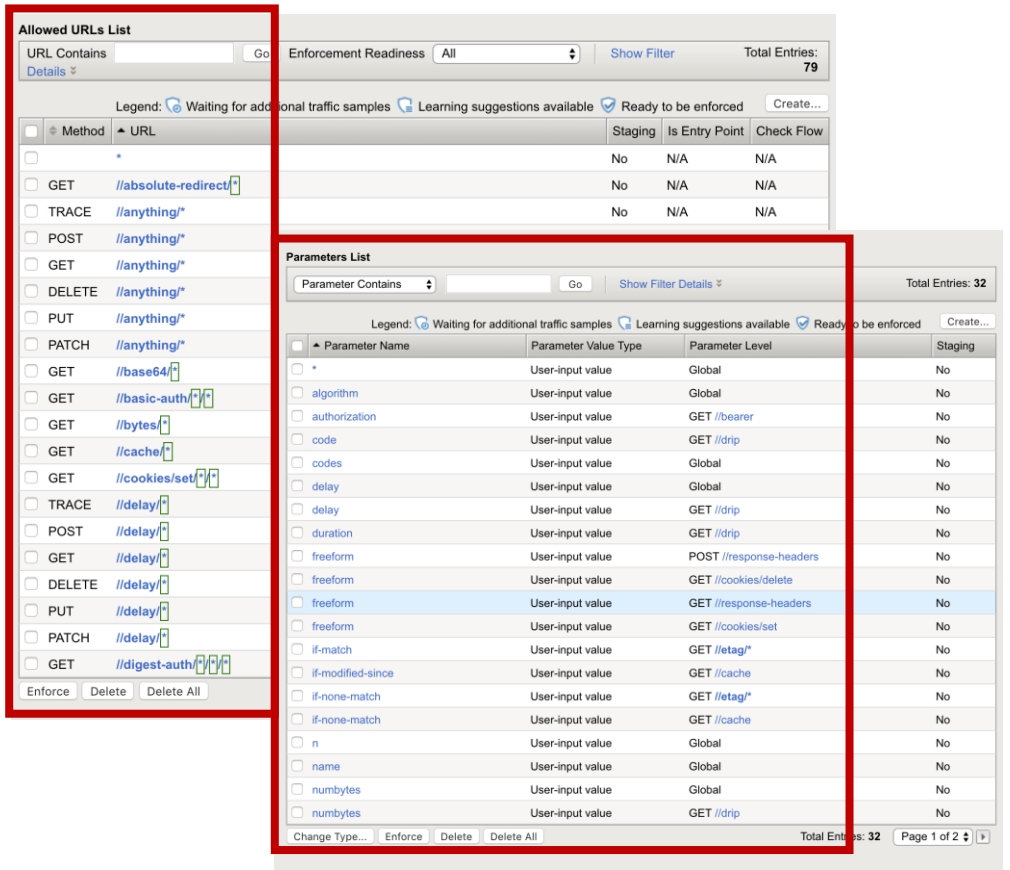
Name	URL	SSL Profile	Description
PetStore_server1	https://petstore.swagger.io/v2	/Common/apm-default-serverssl	
PetStore_server2	http://petstore.swagger.io/v2		

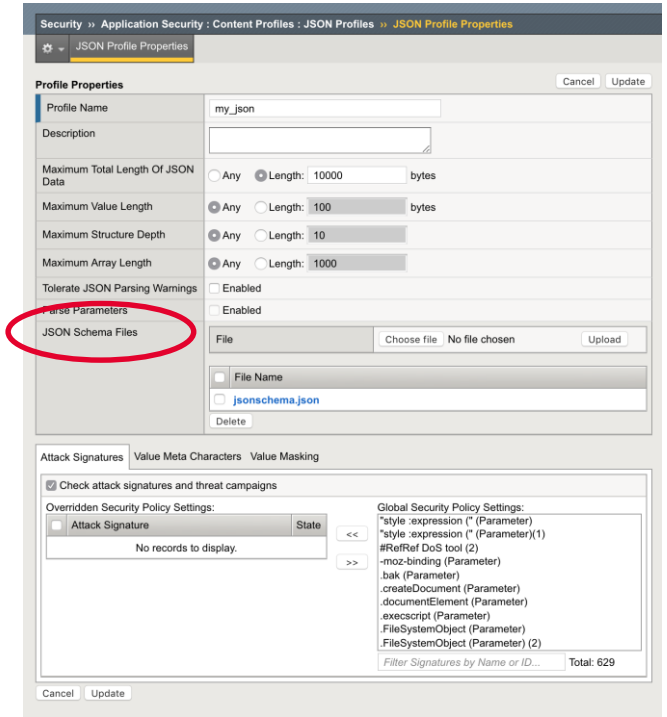


Path / Request, Responses / Method / Authentication, Authorization 제어

API 보안 기능 / API 제어

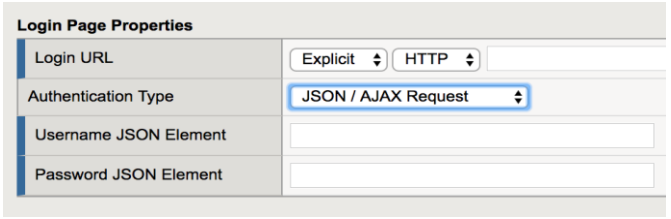






URI / Parameter / Method 제어

API 보안 기능 / Brute Force 방어



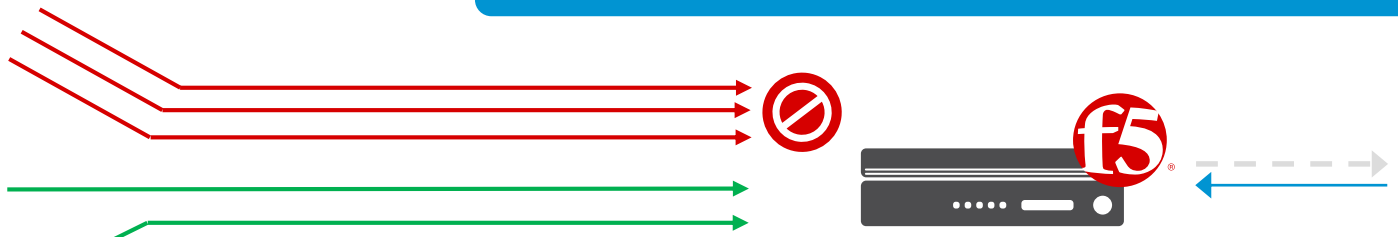
JSON / AJAX Request에 대한 검증 제공

정상 봇, 비정상 봇, 정상 사용자 구분 / 검증









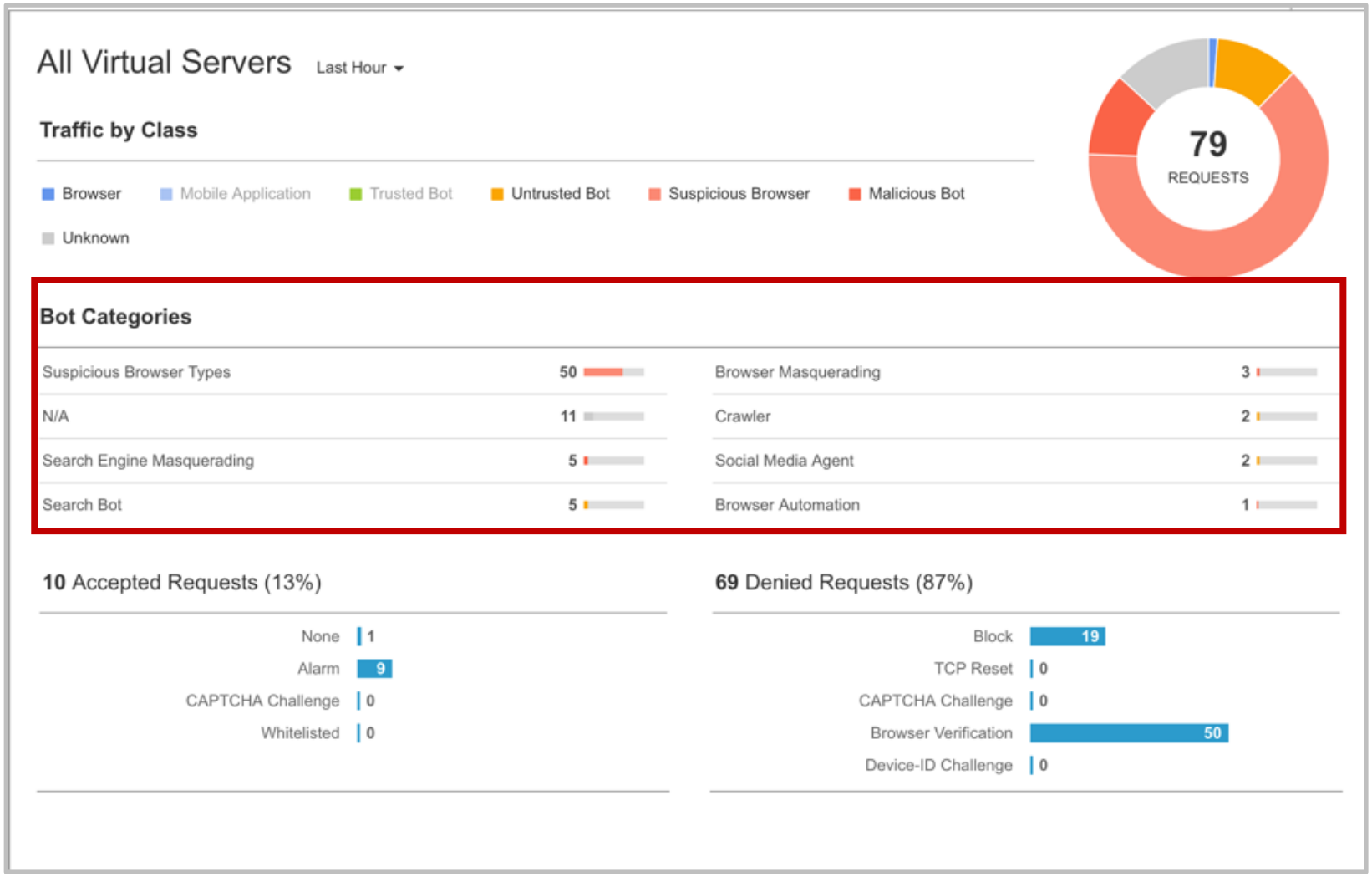


Scraping 과 Brute force 공격 방어

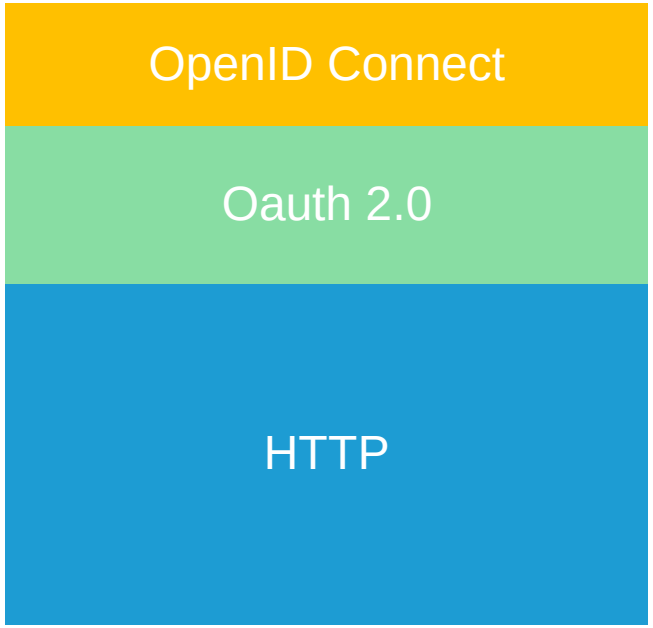
Real time challenge 제공 (java script / captcha)



API 보안 기능 / L7 DoS 방어



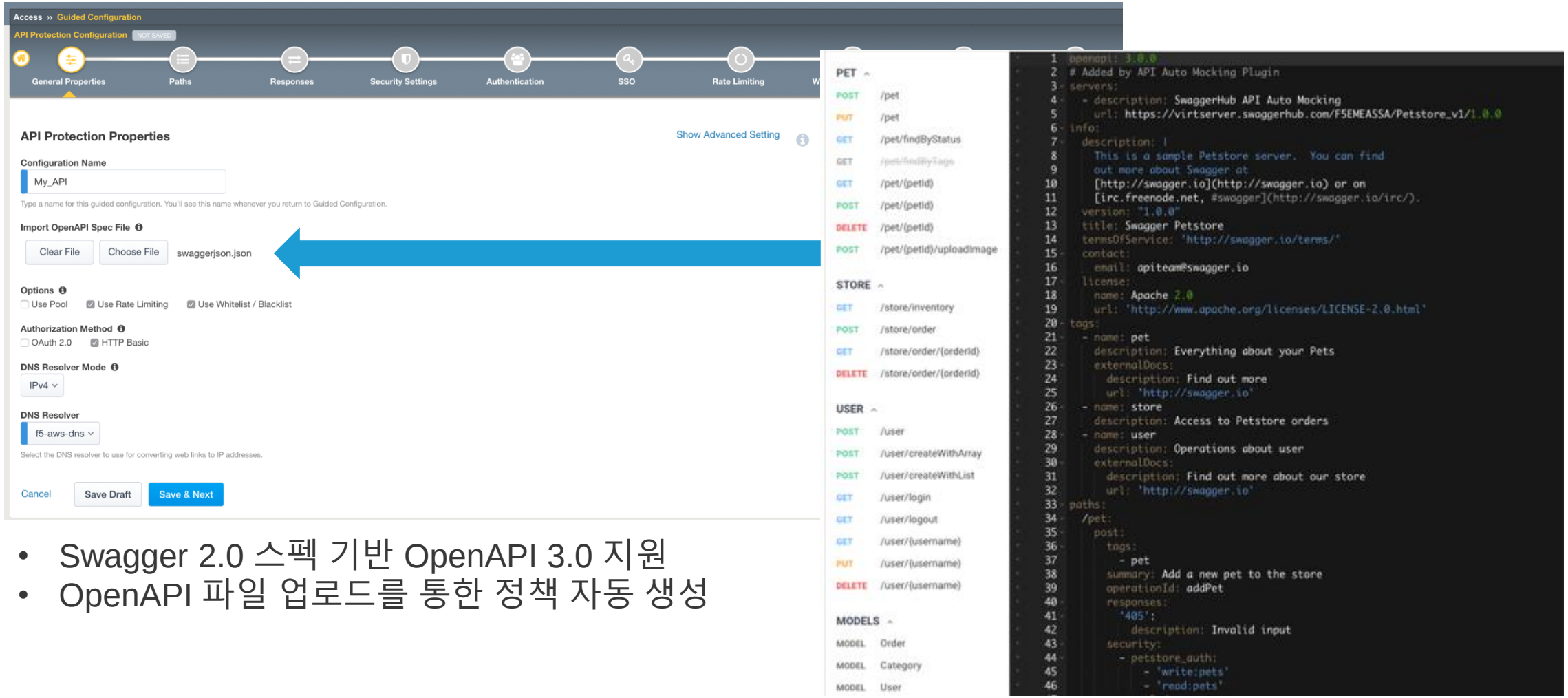
API 보안 기능 / AuthN 제공



- 인증을 위한 OpenID connect 제공
- 권한을 위한 OAuth 2.0 제공
- 기본 인증을 위한 BASIC 인증 제공

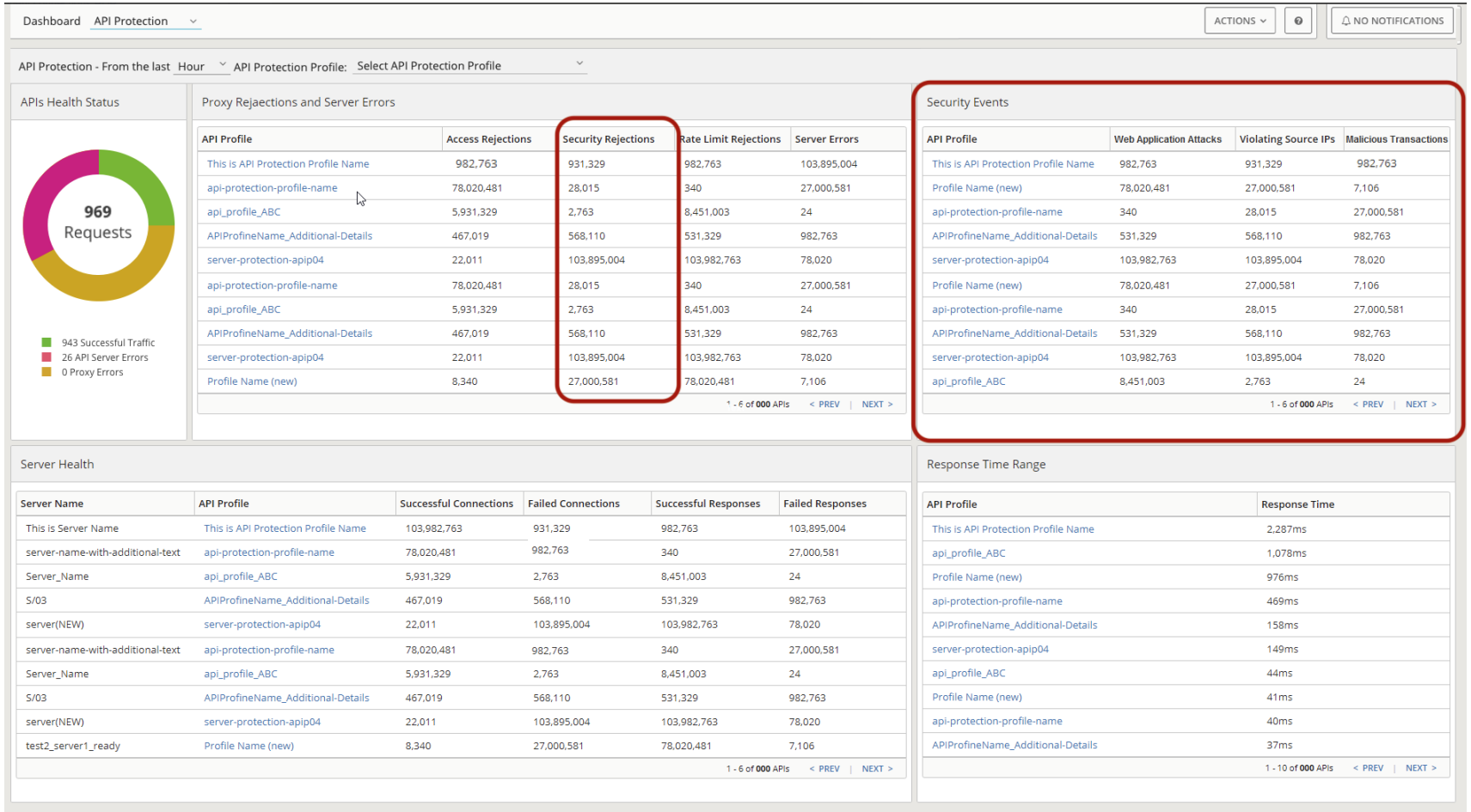
API 보안 기능 / 템플릿 지원

V15

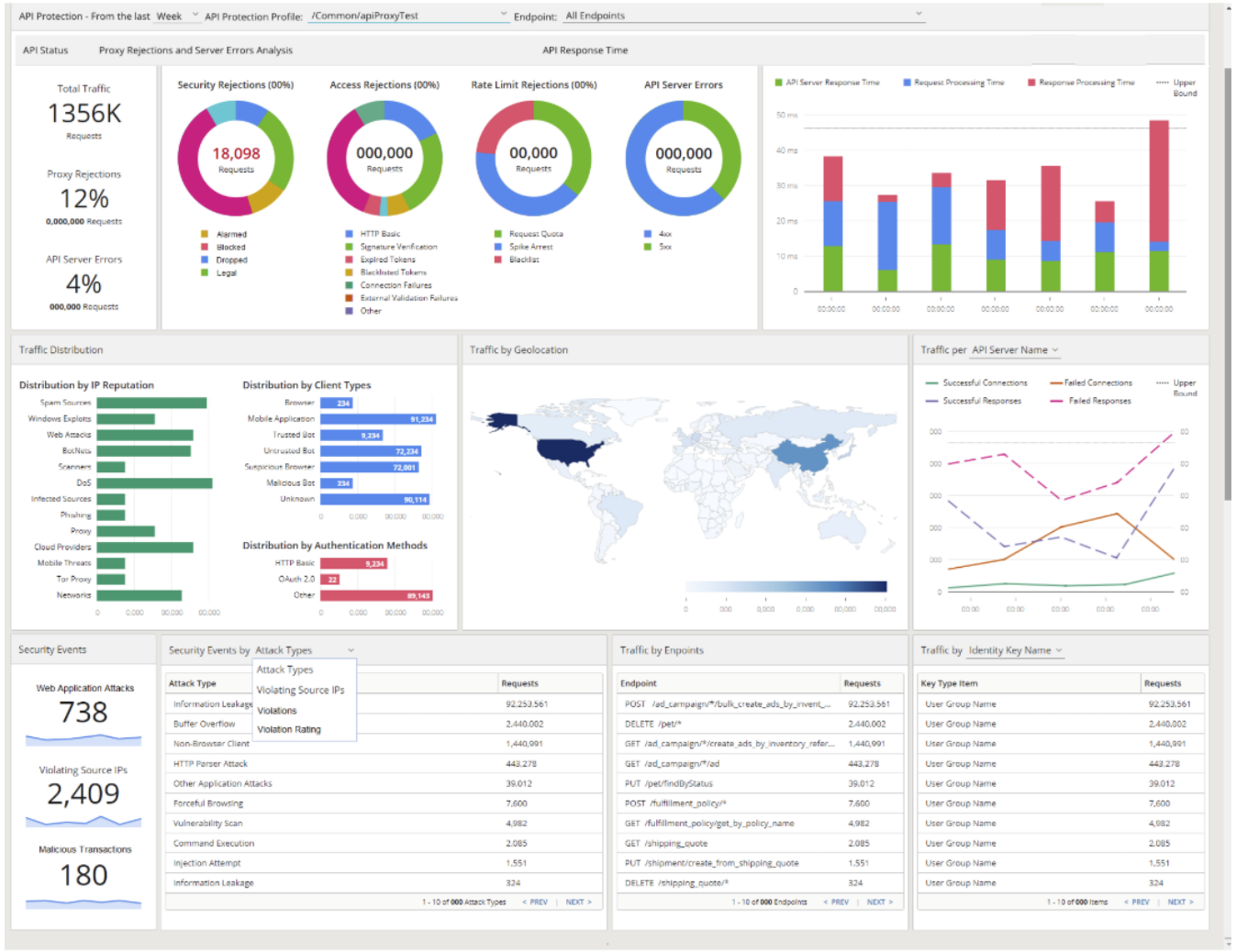


- Swagger 2.0 스펙 기반 OpenAPI 3.0 지원
- OpenAPI 파일 업로드를 통한 정책 자동 생성

API 보안 기능 / 레포팅

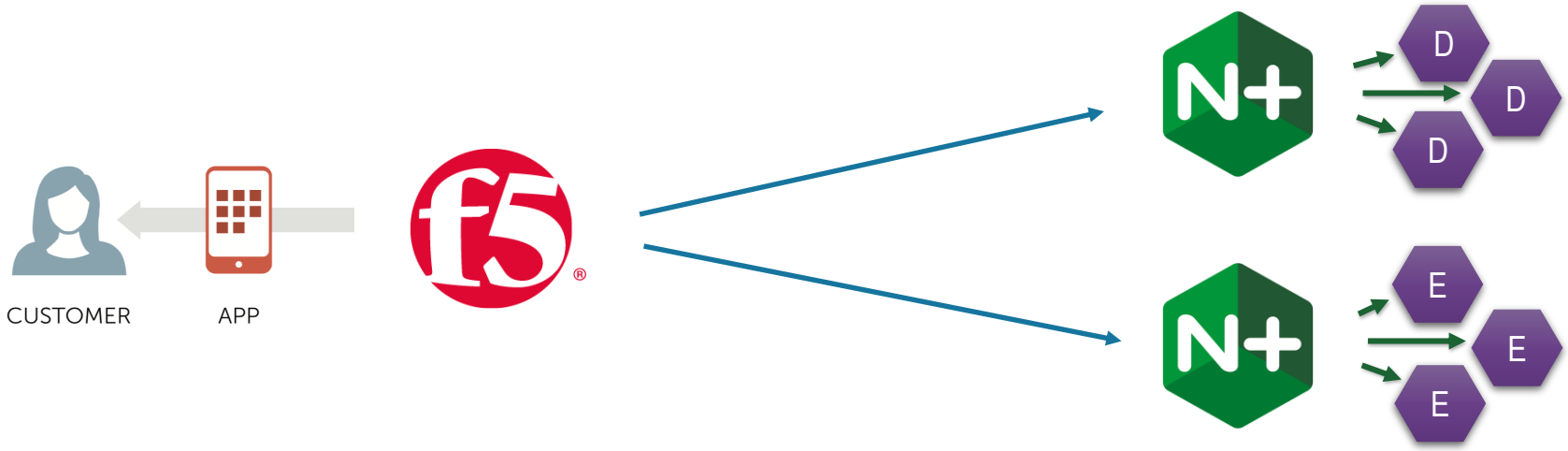

Dashboard API Protection
ACTIONS
NO NOTIFICATIONS
API Protection - From the last Hour API Protection Profile: Select API Protection Profile
APIs Health Status
969 Requests
943 Successful Traffic
26 API Server Errors
0 Proxy Errors
Proxy Rejaections and Server Errors
API Profile | Access Rejections | Security Rejections | Rate Limit Rejections | Server Errors
This is API Protection Profile Name | 982,763 | 931,329 | 982,763 | 103,895,004
api-protection-profile-name | 78,020,481 | 28,015 | 340 | 27,000,581
api_profile_ABC | 5,931,329 | 2,763 | 8,451,003 | 24
APIProfineName_Additional-Details | 467,019 | 568,110 | 531,329 | 982,763
server-protection-apip04 | 22,011 | 103,895,004 | 103,982,763 | 78,020
api-protection-profile-name | 78,020,481 | 28,015 | 340 | 27,000,581
api_profile_ABC | 5,931,329 | 2,763 | 8,451,003 | 24
APIProfineName_Additional-Details | 467,019 | 568,110 | 531,329 | 982,763
server-protection-apip04 | 22,011 | 103,895,004 | 103,982,763 | 78,020
Profile Name (new) | 8,340 | 27,000,581 | 78,020,481 | 7,106
1 - 6 of 000 APIs < PREV | NEXT >
Security Events
API Profile | Web Application Attacks | Violating Source IPs | Malicious Transactions
This is API Protection Profile Name | 982,763 | 931,329 | 982,763
Profile Name (new) | 78,020,481 | 27,000,581 | 7,106
api-protection-profile-name | 340 | 28,015 | 27,000,581
APIProfineName_Additional-Details | 531,329 | 568,110 | 982,763
server-protection-apip04 | 103,982,763 | 103,895,004 | 78,020
Profile Name (new) | 78,020,481 | 27,000,581 | 7,106
api-protection-profile-name | 340 | 28,015 | 27,000,581
APIProfineName_Additional-Details | 531,329 | 568,110 | 982,763
server-protection-apip04 | 103,982,763 | 103,895,004 | 78,020
api_profile_ABC | 8,451,003 | 2,763 | 24
1 - 6 of 000 APIs < PREV | NEXT >
Server Health
Server Name | API Profile | Successful Connections | Failed Connections | Successful Responses | Failed Responses
This is Server Name | This is API Protection Profile Name | 103,982,763 | 931,329 | 982,763 | 103,895,004
server-name-with-additional-text | api-protection-profile-name | 78,020,481 | 982,763 | 340 | 27,000,581
Server_Name | api_profile_ABC | 5,931,329 | 2,763 | 8,451,003 | 24
S/03 | APIProfineName_Additional-Details | 467,019 | 568,110 | 531,329 | 982,763
server(NEW) | server-protection-apip04 | 22,011 | 103,895,004 | 103,982,763 | 78,020
server-name-with-additional-text | api-protection-profile-name | 78,020,481 | 982,763 | 340 | 27,000,581
Server_Name | api_profile_ABC | 5,931,329 | 2,763 | 8,451,003 | 24
S/03 | APIProfineName_Additional-Details | 467,019 | 568,110 | 531,329 | 982,763
server(NEW) | server-protection-apip04 | 22,011 | 103,895,004 | 103,982,763 | 78,020
test2_server1_ready | Profile Name (new) | 8,340 | 27,000,581 | 78,020,481 | 7,106
1 - 6 of 000 APIs < PREV | NEXT >
Response Time Range
API Profile | Response Time
This is API Protection Profile Name | 2,287ms
api_profile_ABC | 1,078ms
Profile Name (new) | 976ms
api-protection-profile-name | 469ms
APIProfineName_Additional-Details | 158ms
server-protection-apip04 | 149ms
api_profile_ABC | 44ms
Profile Name (new) | 41ms
api-protection-profile-name | 40ms
APIProfineName_Additional-Details | 37ms
1 - 10 of 000 APIs < PREV | NEXT >

API 보안 기능 / 레포팅


API Protection - From the last Week
API Protection Profile: /Common/apiProxyTest
Endpoint: All Endpoints
API Status
Proxy Rejections and Server Errors Analysis
API Response Time
Total Traffic
1356K
Requests
Proxy Rejections
12%
0,000,000 Requests
API Server Errors
4%
000,000 Requests
Security Rejections (00%)
18,098
Requests
Alarmed
Blocked
Dropped
Legal
Access Rejections (00%)
000,000
Requests
HTTP Basic
Signature Verification
Expired Tokens
Blacklisted Tokens
Connection Failures
External Validation Failures
Other
Rate Limit Rejections (00%)
00,000
Requests
Request Quota
Spike Arrest
Blacklist
API Server Errors
000,000
Requests
4xx
5xx
API Server Response Time
Request Processing Time
Response Processing Time
Upper Bound
Traffic Distribution
Distribution by IP Reputation
Spam Sources
Windows Exploits
Web Attacks
BotNets
Scanners
DoS
Infected Sources
Phishing
Proxy
Cloud Providers
Mobile Threats
Tor Proxy
Networks
Distribution by Client Types
Browser
Mobile Application
Trusted Bot
Untrusted Bot
Suspicious Browser
Malicious Bot
Unknown
Distribution by Authentication Methods
HTTP Basic
OAuth 2.0
Other
Traffic by Geolocation
Traffic per API Server Name
Successful Connections
Failed Connections
Upper Bound
Successful Responses
Failed Responses
Security Events
Web Application Attacks
738
Violating Source IPs
2,409
Malicious Transactions
180
Security Events by Attack Types
Attack Types
Violating Source IPs
Violations
Violation Rating
Attack Type
Requests
Information Leakage
92,253,561
Buffer Overflow
2,440,002
Non-Browser Client
1,440,991
HTTP Parser Attack
443,278
Other Application Attacks
39,012
Forceful Browsing
7,600
Vulnerability Scan
4,982
Command Execution
2,085
Injection Attempt
1,551
Information Leakage
324
1 - 10 of 000 Attack Types
< PREV
NEXT >
Traffic by Enpoints
Endpoint
Requests
POST /ad_campaign/*/bulk_create_ads_by_invent_...
92,253,561
DELETE /pet/*
2,440,002
GET /ad_campaign/*/create_ads_by_inventory_refer...
1,440,991
GET /ad_campaign/*/ad
443,278
PUT /pet/findByStatus
39,012
POST /fulfillment_policy/*
7,600
GET /fulfillment_policy/get_by_policy_name
4,982
GET /shipping_quote
2,085
PUT /shipment/create_from_shipping_quote
1,551
DELETE /shipping_quote/*
324
1 - 10 of 000 Endpoints
< PREV
NEXT >
Traffic by Identity Key Name
Key Type Item
Requests
User Group Name
92,253,561
User Group Name
2,440,002
User Group Name
1,440,991
User Group Name
443,278
User Group Name
39,012
User Group Name
7,600
User Group Name
4,982
User Group Name
2,085
User Group Name
1,551
User Group Name
324
1 - 10 of 000 Items
< PREV
NEXT >

요약

API Gateway 와 API 보안의 통합 아키텍처



익숙한 인터페이스, 원할한 기술지원

API 처리에 대한 비용절감

API Gateway 의 대용량 성능 지원

F5 와의 통합을 통한 All-in-one 보안 지원

