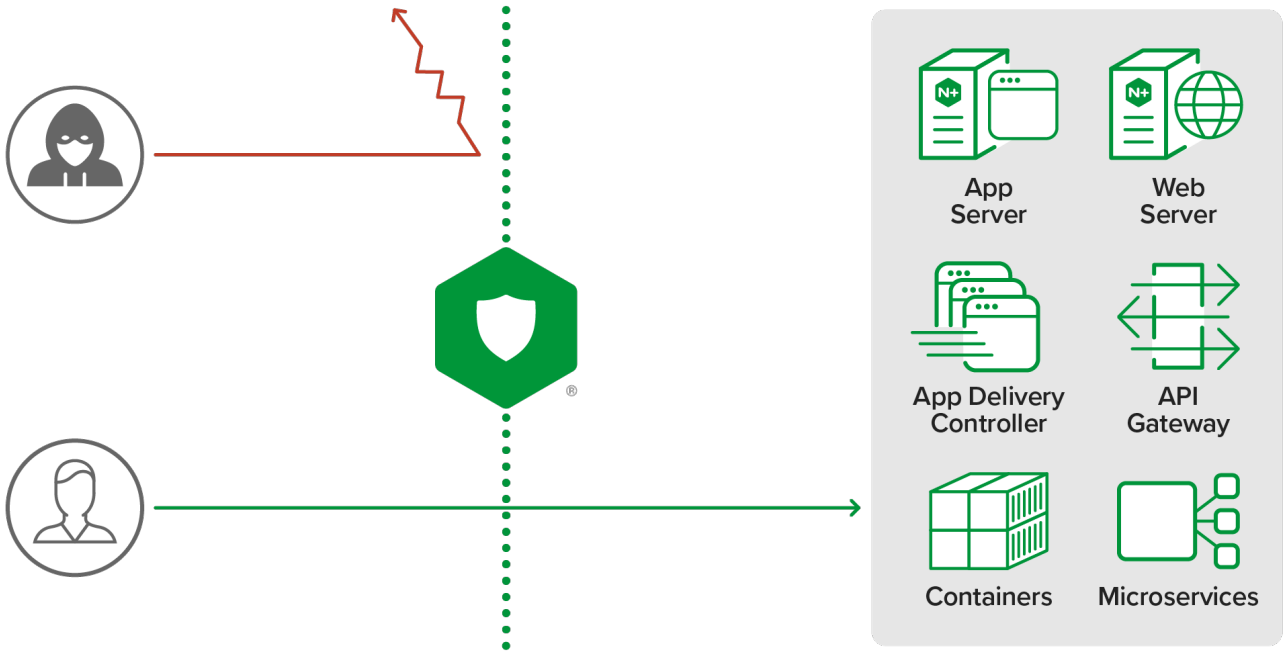
F5 NGINX App Protect 소개

V1

김재홍
CLOUD & NGINX Specialist, F5 Korea

NGINX App Protect란?

왜 NGINX APP PROTECT로의 전환이 필요할까요?



보안

고성능의 보안

단순 Signatures 방어 이상의 다양한 기능

F5에서 검증된 신뢰할 수 있는 Signatures 사용

CI/CD

쉬운 CI/CD 통합

모던 인프라 환경에 적합한 설계

보안 개선을 위한 신속한 피드백 루프

관리

통합된 F5 선언형 인터페이스

Syslog를 통한 보안 통계

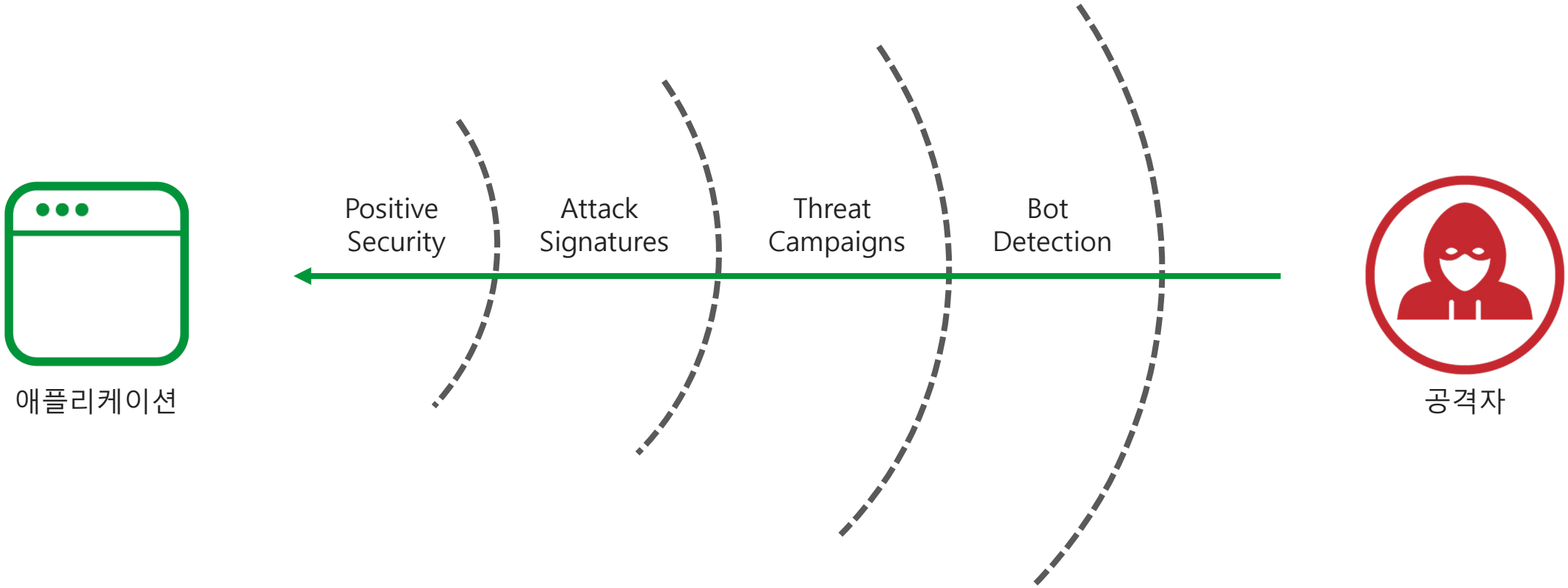
F5의 기술지원

강력한 애플리케이션 보안

F5의 advanced WAF 기술 기반으로 개발된 애플리케이션 보안 및 제어.
애플리케이션 공격의 차단 및 서비스 다운타임 감소.

강력한 애플리케이션 보안

멀티 레이어 기반의 접근방식



봇 탐지 및 방어

자동화 기반의 공격에 대한 방어를 가장 먼저 제공

- User-Agent 해더 및 URI에서 봇 패턴 기반의 기본 봇 탐지 및 방어

- 각각의 봇 시그너처는 다음의 Bot Class 범주에 포함
  - 신뢰할 수 있는 봇(Trusted Bot)
  - 신뢰할 수 없는 봇(Untrusted Bot)
  - 악의적인 봇(Malicious Bot)

- 향후 계획:
  - F5 Shape Defense 솔루션과 통합
  - 신규 기능 추가

```
{
    "policy": {
        "name": "bot_defense_policy",
        "template": {
            "name": "POLICY_TEMPLATE_NGINX_BASE"
        },
        "applicationLanguage": "utf-8",
        "enforcementMode": "blocking",
        "bot-defense": {
            "settings": {
                "isEnabled": true
            },
            "mitigations": {
                "classes": [
                    {
                        "name": "trusted-bot",
                        "action": "alarm"
                    },
                    {
                        "name": "untrusted-bot",
                        "action": "block"
                    },
                    {
                        "name": "malicious-bot",
                        "action": "block"
                    }
                ]
            }
        }
    }
}
```

위협 캠페인 - Threat Campaign

현재 확인된 ATTACK CAMPAIGNS에 대한 애플리케이션 방어

- 위협 캠페인은 위협 인텔리전스 기능
- 활성 공격 캠페인에 대한 정보가 포함된 빈번한 업데이트 피드
- 위협 캠페인의 컨텍스트 정보는 현재 확인된 공격/위협에 대한 특화됨
- False Positive 없음

예시 :

APT12 are exploiting Apache Struts2 (CVE-2018-11776) to deploy crypto-miner

NAP의 Default 정책

일관된 기본 정책을 제공

- OWASP Top 10 기반의 시그너처 & CVEs
- 회피기술(Evasion Techniques)

Negative Model

- Meta Characters 확인
- HTTP Protocol Compliance
- Disallow file type(bin, cgi, cmd, dll, exe, msi, sys 등)
- Cookie Integrity Check
- JSON & XML Check
- Sensitive parameters & Data Guard

Positive Model

NAP – Attack Signatures

애플리케이션 방어에 적용되는 공격 패턴

기본 제공되는 Signatures Sets:

- All Response Signatures
- All Signatures
- Generic Detection Signatures
- Generic Detection Signatures(High Accuracy)
- Generic Detection Signatures(High/Mid Accuracy)
- High Accuracy Signatures
- Low Accuracy Signatures
- Medium Accuracy Signatures
- OWA Signatures
- WebSphere Signatures

또는 80개 이상의 서버 기술로 앱 보호 정책을 사용자 정의로 사용:

Sharepoint, Python, Vue.JS, GraphQL, NodeJS, Angular, React, Express.JS,

Wordpress, Linux, XML, PHP, Windows … 등

NAP – Positive Model

애플리케이션의 잠재 공격에 대한 제로데이 방어를 사용

Positive Security Model을 사용하여 보안 정책을 강화:

- **데이터가드** – 응답에 포함된 민감 정보 보호
- **File 유형** – 허용 또는 차단할 파일 유형 선택
- **HTTP 메소드** – 허용 또는 차단할 HTTP 메소드
- **HTTP 응답코드** – 허용할 응답 코드
- **HTTP 파라메터** – 파라메터의 탐지 및 제어
- **HTTP URL** – 허용 또는 차단할 URL 정의
- **Content Profile** – JSON, XML 등

```
{
    "entity": {
        "name": "/vulnerabilities/sqli*"
    },
    "entityChanges": {
        "signatureOverrides": [
            {
                "signatureId": 200002147,
                "enabled": false
            },
            {
                "signatureId": 200002835,
                "enabled": false
            },
            {
                "signatureId": 200002476,
                "enabled": false
            }
        ]
    },
    "entityType": "url",
    "action": "add-or-update"
}
```

또는 Signatures 예외 정책과 함께 사용

NAP – Positive Model

애플리케이션의 잠재 공격에 대한 제로데이 방어를 사용

```
{
    "policy": {
        "name": "json_form_policy_external_schema",
        "template": {
            "name": "POLICY_TEMPLATE_NGINX_BASE"
        },
        "json-validation-files": [
            {
                "fileName": "person_schema.json",
                "link": "file://person_schema.json"
            }
        ],
        "json-profiles": [
            {
                "name": "reg_form_prof",
                "defenseAttributes": {
                    "maximumArrayLength": "any",
                    "maximumStructureDepth": "any",
                    "maximumTotalLengthOfJSONData": 10
                    "maximumValueLength": "any",
                    "tolerateJSONParsingWarnings": fal
                },
                "validationFiles": [
                    {
                        "isPrimary": true,
                        "jsonValidationFile": {
                            "fileName": "person_schema.json"
                        }
```

```
{
    "policy": {
        "name": "petstore_api_security_policy",
        "description": "NGINX App Protect API Security Policy for the Petstore API",
        "template": {
            "name": "POLICY_TEMPLATE_NGINX_BASE"
        },
        "open-api-files": [
            {
                "link": "http://127.0.0.1:8088/myapi.yaml"
            }
        ],
        "violations": [
            {
                "block": true,
                "description": "Disallowed file upload content detected in body",
                "name": "VIOL_FILE_UPLOAD_IN_BODY"
            },
            {
```


NGINX Part of F5

NAP – False Positive 관리

FALSE POSITIVE의 관리에 도움

- 각각의 요청별 Violation Rating을 제공하여 관리자가 False Positive를 쉽게 관리할 수 있도록 지원
- Attack Signatures False Positive Mode(기본설정) 사용을 통해 Violation Rating 점수 기반의 차단을 제공

method	uri	violations	violation_rating	request_status
GET	/login.php	HTTP protocol compliance failed	3	alerted
GET	/manager/html	HTTP protocol compliance failed, Bot Client Detected	3	alerted
GET	/wp-login.php	HTTP protocol compliance failed, Bot Client Detected	3	alerted
POST	/_ignition/execute-solution	HTTP protocol compliance failed, Illegal meta character in value	2	alerted
POST	/vendor/phpunit/phpunit/src/Util/PHP/eval-stdin.php	HTTP protocol compliance failed, Illegal meta character in value, Illegal meta character in parameter name, Attack signature detected, Violation Rating Threat detected	4	blocked
GET	/	HTTP protocol compliance failed	3	alerted

0	No Violation
1	False Positive
2	False Positive
3	Needs Examination
4	Threat
5	Threat

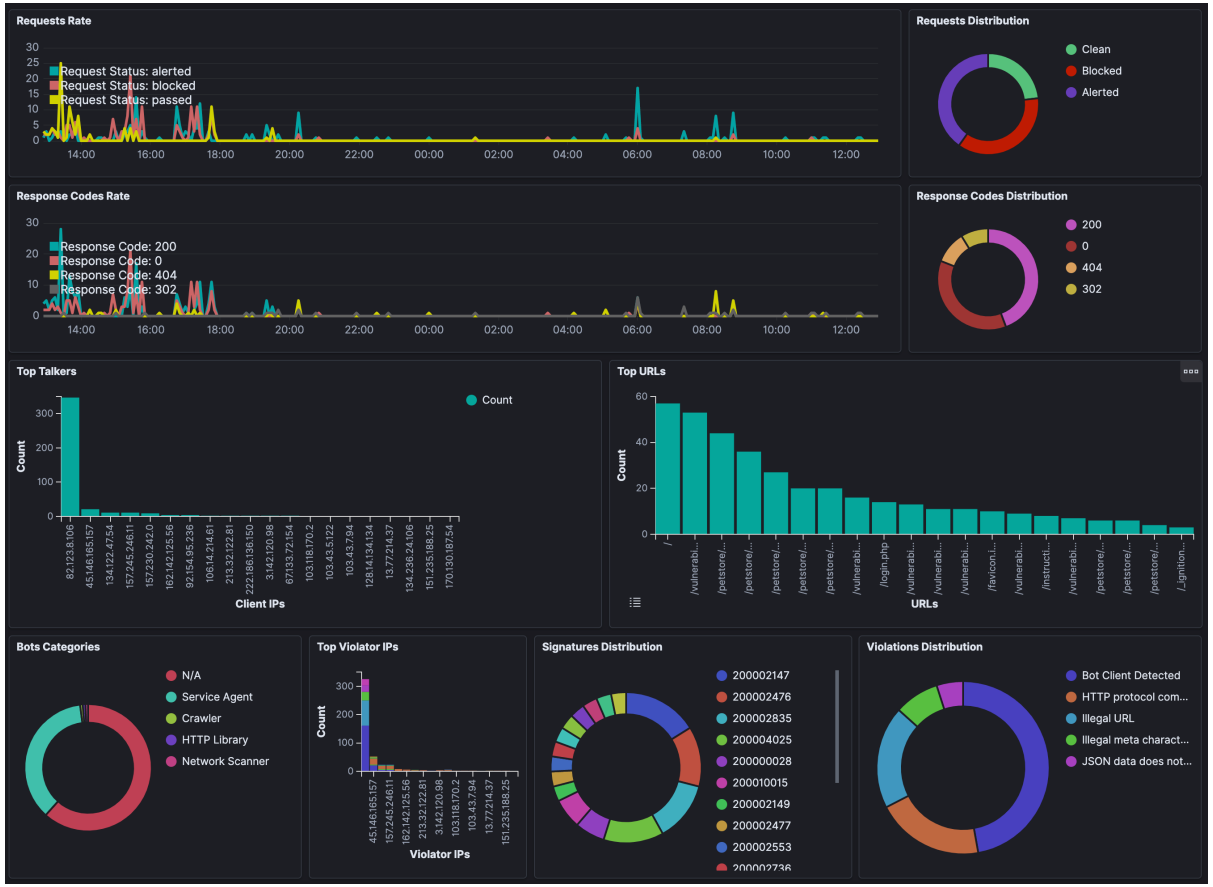
NAP – 보안 가시성

트래픽, 위반 및 차단에 대한 전체 가시성을 제공

Security Log는 아래의 정보를 포함:

- **HTTP request/response**에 대한 상세정보
- NGINX App Protect의 트래픽 처리 상태
- 설정된 정책 파라메터 기반의 차단 내용
- 그리고 관련 로그 정보의 추출
  - Stderr, Files, Syslog

```
app_protect_security_log "/etc/app_protect/conf/log_default.json" syslog:server=localhost:5144;
app_protect_security_log "/etc/app_protect/conf/log_default.json" /var/log/app_protect/security.log;
app_protect_security_log "/etc/app_protect/conf/log_default.json" stderr;
```



ELK Dashboard 제공:

https://github.com/f5devcentral/f5-waf-elk-dashboards

모던 앱을 위한 보안

성능 및 확장성을 제공하는 고성능 보안

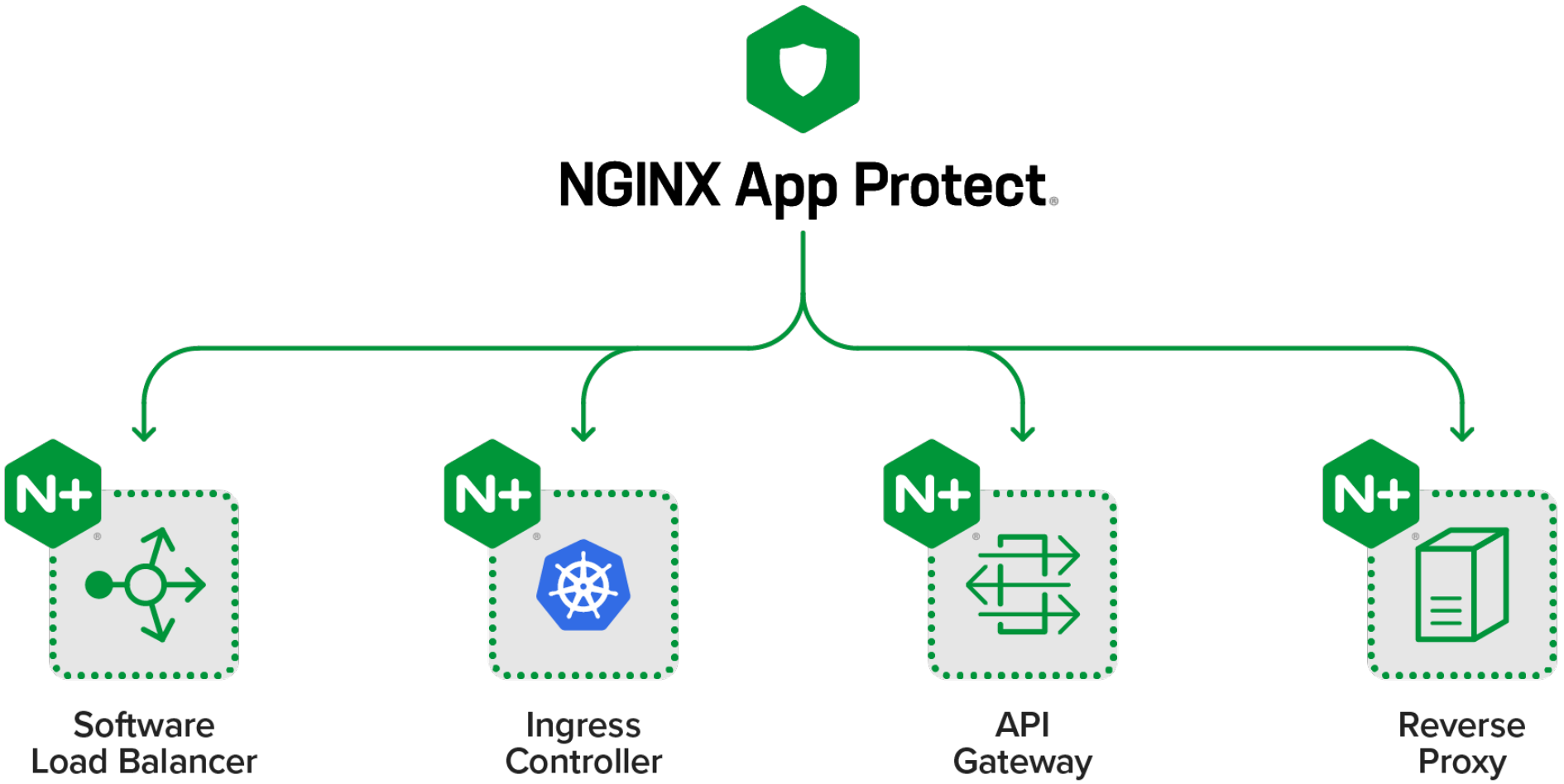
모던 앱을 위한 보안

NGINX에 NATIVE 통합

```
http {
    include       /etc/nginx/mime.types;
    default_type  application/octet-stream;
    sendfile        on;
    keepalive_timeout  65;

    app_protect_enable on; # This is how you enable NGINX App Protect in the relevant context/bloc
    app_protect_policy_file "/etc/nginx/NginxDefaultPolicy.json"; # This is a reference to the pol
    app_protect_security_log_enable on; # This section enables the logging capability
    app_protect_security_log "/etc/app_protect/conf/log_default.json" syslog:server=127.0.0.1:515;

    server {
        listen       80;
        server_name  localhost;
        proxy_http_version 1.1;

        location / {
            client_max_body_size 0;
            default_type text/html;
            proxy_pass http://172.29.38.211:80$request_uri;
        }
    }
```

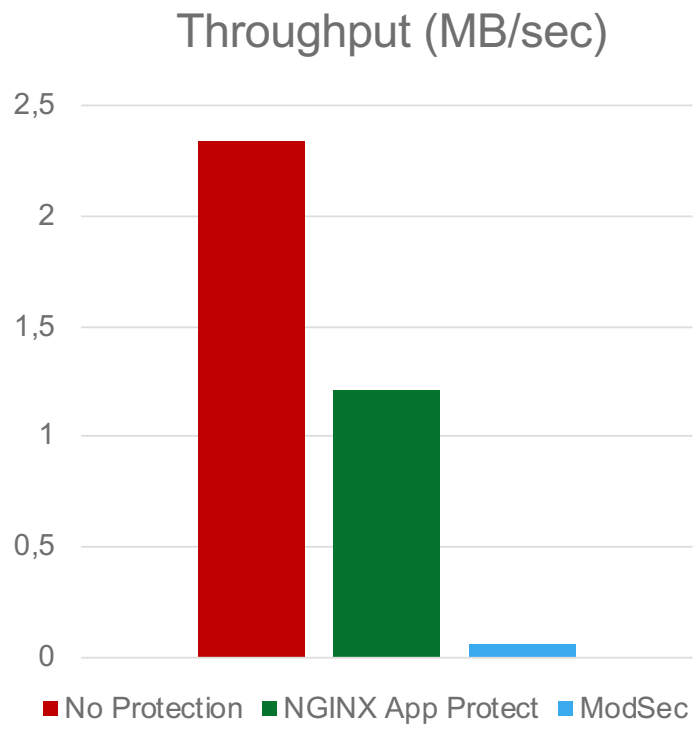
모던 앱을 위한 보안

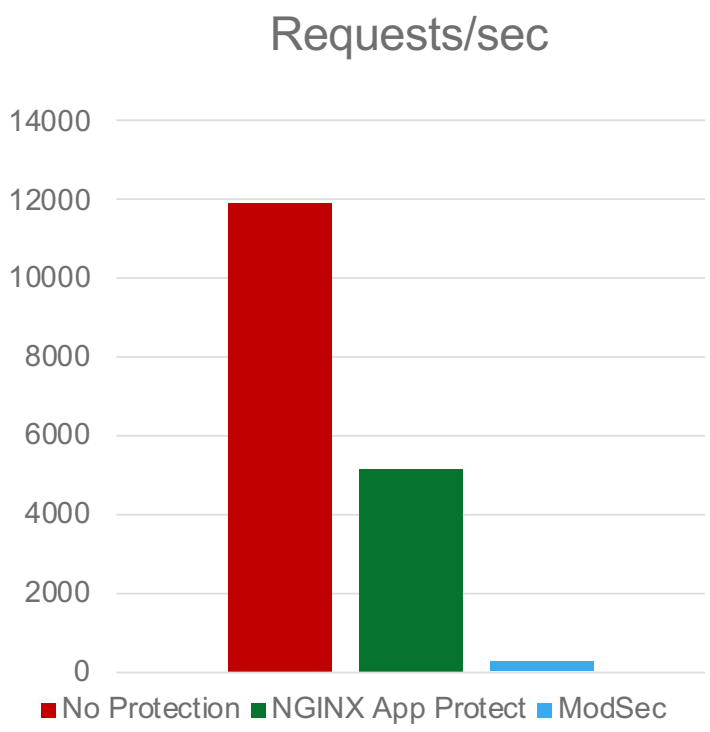
제공하는 배포/구성 옵션

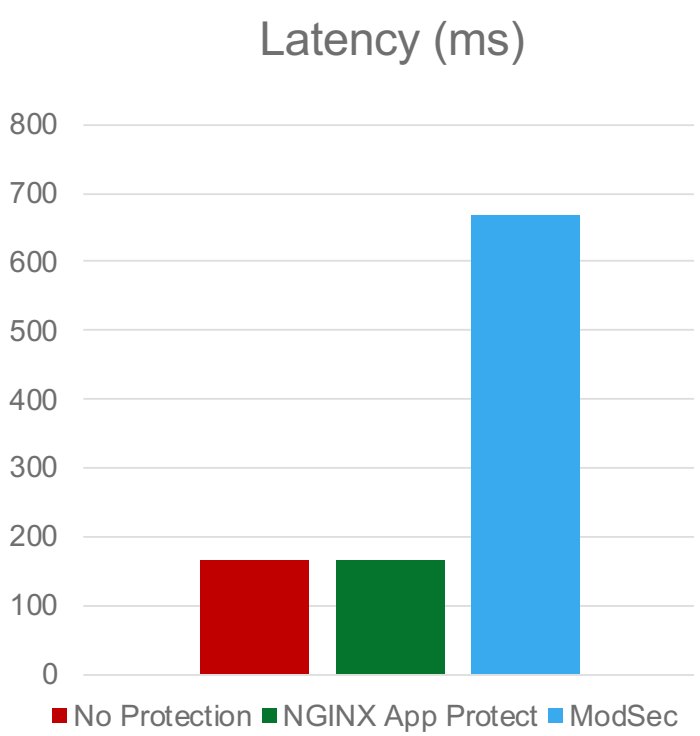


모던 앱을 위한 보안

고성능 및 낮은 지연율로 보안을 제공







- ModSec Configuration: OWASP Top 10 (enable all CRS 3v rules)
- NGINX App Protect Configuration: OWASP Top 10 (Enable signatures), Evasion technique, Data Guard, Disallowed file types, HTTP protocol compliance

CI/CD 친화적

보안이 DevOps의 이니셔티브와 보조를 맞출 수 있도록 지원

NAP – CI/CD 친화적

선언형 정책

1 기본 템플릿 제공

사전 정의된 템플릿 또는 외부 참조

```
http {
    include       /etc/nginx/mime.types;
    default_type  application/octet-stream;
    sendfile        on;
    keepalive_timeout  65;

    app_protect_enable on; # This is how you enable NGINX App Prote
    app_protect_policy_file "/etc/nginx/NginxDefaultPolicy.json";
    app_protect_security_log_enable on; # This section enables the
    app_protect_security_log "/etc/app_protect/conf/log_default.jso

    server {
        listen       80;
        server_name  localhost;
        proxy_http_version 1.1;

        location / {
            client_max_body_size 0;
            default_type text/html;
            proxy_pass http://172.29.38.211:80$request_uri;
        }
    }
```

```
{
    "policy": {
        "name": "signature_modification_entitytype",
        "template": { "name": "POLICY_TEMPLATE_NGINX_BASE" },
        "applicationLanguage": "utf-8",
        "enforcementMode": "blocking",
        "signature-sets": [
            {
                "name": "All Signatures",
                "block": true,
                "alarm": true
            }
        ]
    },
    "modifications": [
        {
            "entityChanges": {
                "enabled": false
            },
            "entity": {
                "signatureId": 200001834
            },
            "entityType": "signature",
            "action": "add-or-update"
        }
    ]
}
```

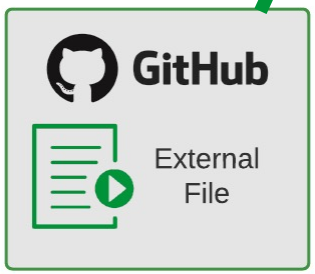

NGINX Part of F5

NAP – CI/CD 친화적

선언형 정책 – 외부 참조

로컬 파일 시스템, HTTP(s) 웹서버/리포지토리

```
{
    "name": "external_resources_file_types",
    "template": {
        "name": "POLICY_TEMPLATE_NGINX_BASE"
    },
    "applicationLanguage": "utf-8",
    "enforcementMode": "blocking",
    "blocking-settings": {
        "violations": [
            {
                "name": "VIOL_FILETYPE",
                "alarm": true,
                "block": true
            }
        ]
    },
    "filetypeReference": {
        "link": "http://domain.com:8081/file-types.txt"
    }
}
```

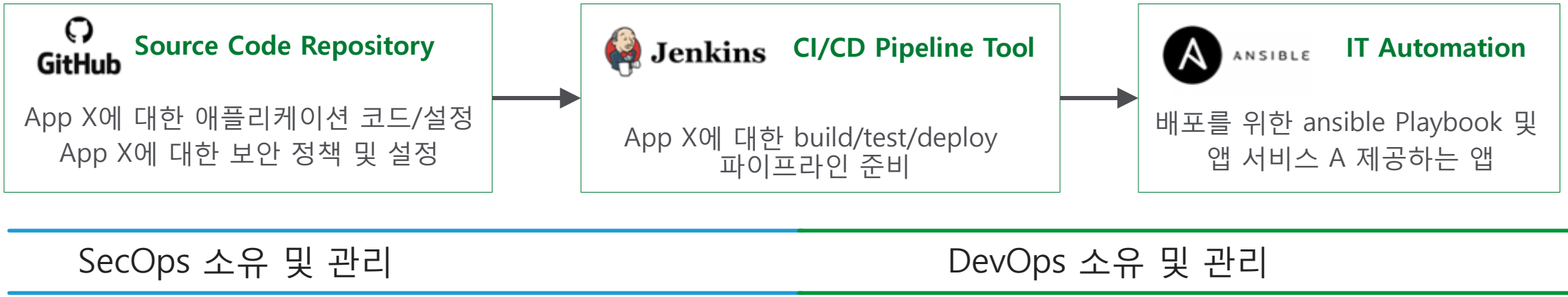



```
[
    {
        "name": "*",
        "type": "wildcard",
        "allowed": true,
        "checkPostDataLength": false,
        "postDataLength": 4096,
        "checkRequestLength": false,
        "requestLength": 8192,
        "checkUrlLength": true,
        "urlLength": 2048,
        "checkQueryStringLength": true,
        "queryStringLength": 2048,
        "responseCheck": false
    },
    {
        "name": "pat",
        "allowed": false
    },
    {
        "name": "mat",
        "allowed": false
    }
]
```


NGINX Part of F5

NAP – CI/CD 친화적

DEVSECOPS 및 보안의 코드화 설정




```
{
  "entityChanges": {
    "type": "explicit"
  },
  "entity": {
    "name": "bak"
  },
  "entityKind":
"tm:asm:policies:filetypes:filetypestate",
  "action": "delete",
  "description": "Delete Disallowed File Type"
}
```

F5 NGINX App Protect

강력한
애플리케이션
보안

모던 앱을 위한
보안

CI/CD
친화적

F5의 애플리케이션 계층 위협 솔루션

F5는 다양한 애플리케이션 계층 위협에 효율적으로 대응하기 위한 솔루션 라인업 및 포트폴리오를 제공

애플리케이션 계층 위협 솔루션

	셀프-관리형	부분 관리형 (SaaS)	전체 관리형 W/SOC
고급 사용 사례 사기 및 남용 방지 (고부가가치 B2C 앱)			**Shape Enterprise Defense**
고급 제어 표적 공격 및 고급 위협 행위자 (기본 제어 포함)	**BIG-IP Advanced WAF** (하드웨어, 소프트웨어, 클라우드)	**프로모션 솔루션** (Shape + Behavioral App Protect + Fraud Protection Solution)	**Silverline Shape Defense** **Silverline WAF**
기본 제어 소프트웨어 취약점 및 일반적인 공격 벡터 (공통의 웹 또는 모던 앱 서비스)	**NGINX App Protect** (NGINX 플러스)	**F5 클라우드 서비스 Essential App Protect**	

Silverline®

NGINX Part of F5