변화하는 세상,
변화 될 애플리케이션 환경,
변하지 말아야 할 애플리케이션 보안.

이종민 부장 / F5 네트웍스

임도훈 과장 / 시큐웨이브


app
app
app
app
app
app
app
app
app
app
app
app
app
app
app
app
app
app
app
app
app


PUBLIC CLOUD
CONTAINER ENVIRONMENTS
PRIVATE CLOUD
SaaS
CO-LOCATION
ON-PREMISES
app
app
app
app
app
app

애플리케이션에 대한 다양한 보안 위협이 존재합니다.

애플리케이션 공격
L7 DoS
API Attack
Code Injection
Client-Side attack

APP 인프라 공격
DDoS
Encrypted Threat
Man-in-the-middle
DNS Spoofing

액세스 공격
Session Hijacking
Credential Theft
Brute Force
Phishing

정교한 해킹 공격
APT
Multi-cloud Threat
Malicious Bot
Threat campaigns / Malware

모든 애플리케이션은 보호되어야 합니다.

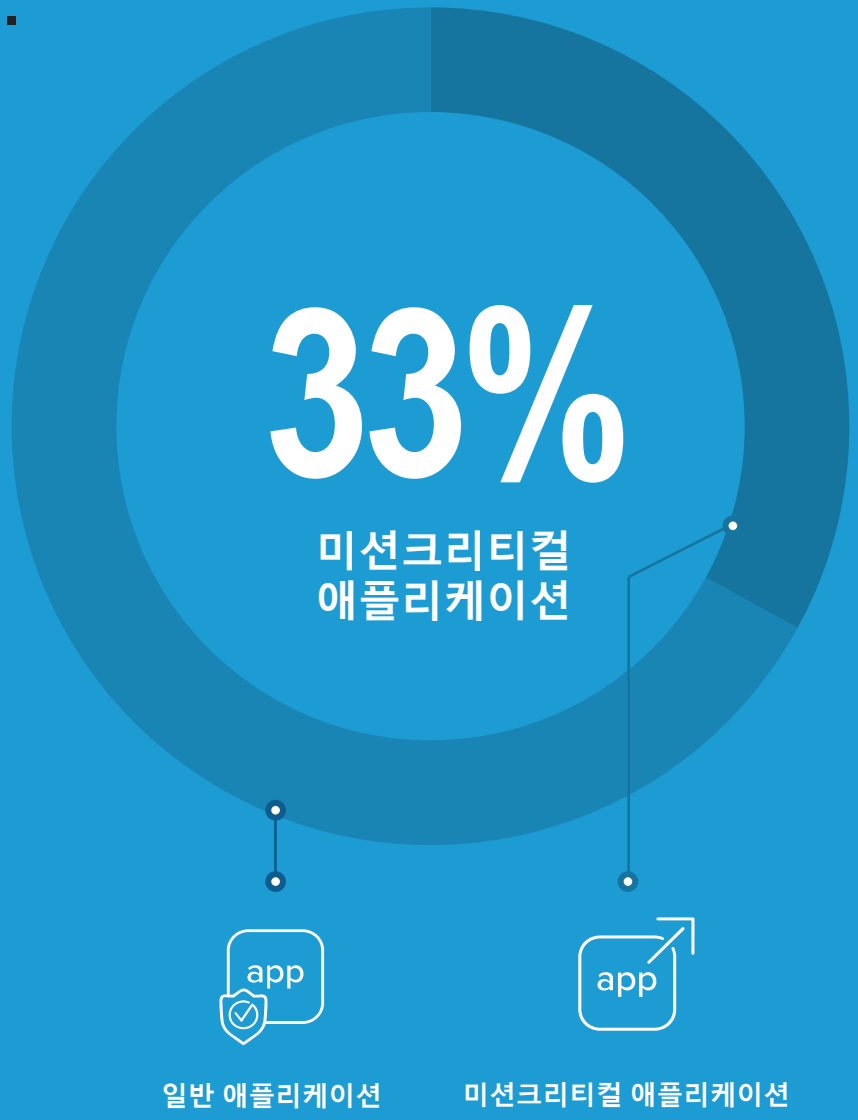
미션 크리티컬 한 애플리케이션 뿐만 아닙니다.

대규모 리테일러 고객

- 수백만 개의 고객 기록 유출
- 수십억의 손해, 시가 총액 감소, CEO 해고

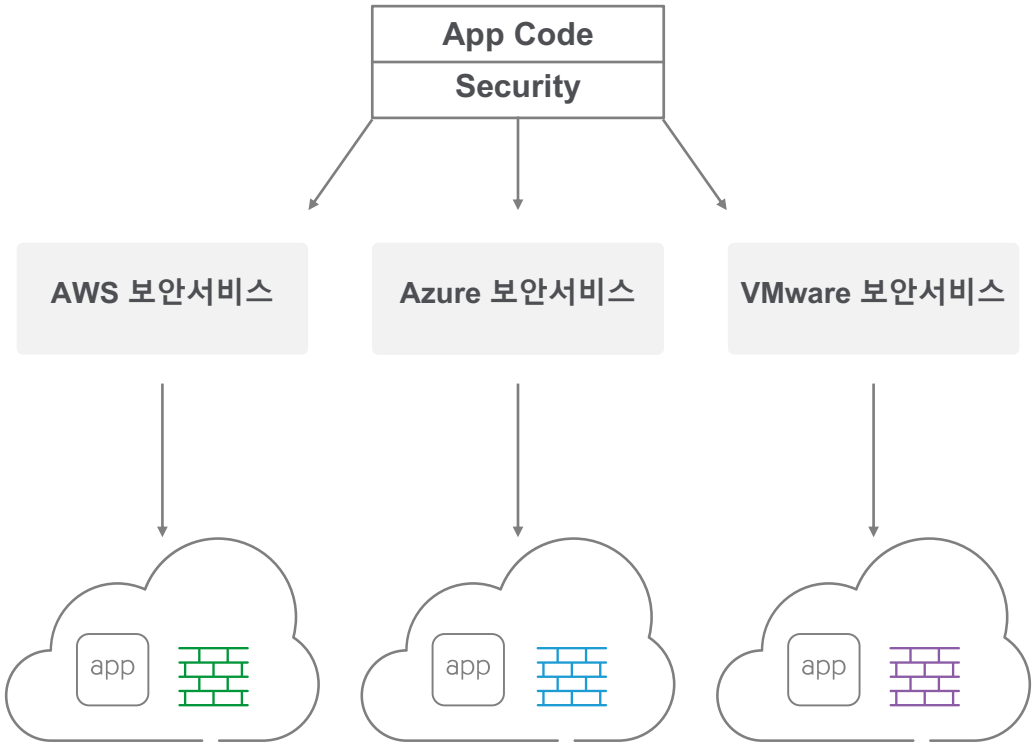
금융 고객

- 대규모 데이터 베이스 유출
- 수익성 높은 고객에 대한 위협 노출
- 디지털 해킹에 대한 중요 관문



개발자는 애플리케이션 보안에 대해 전적으로 책임을 질 수 없습니다.

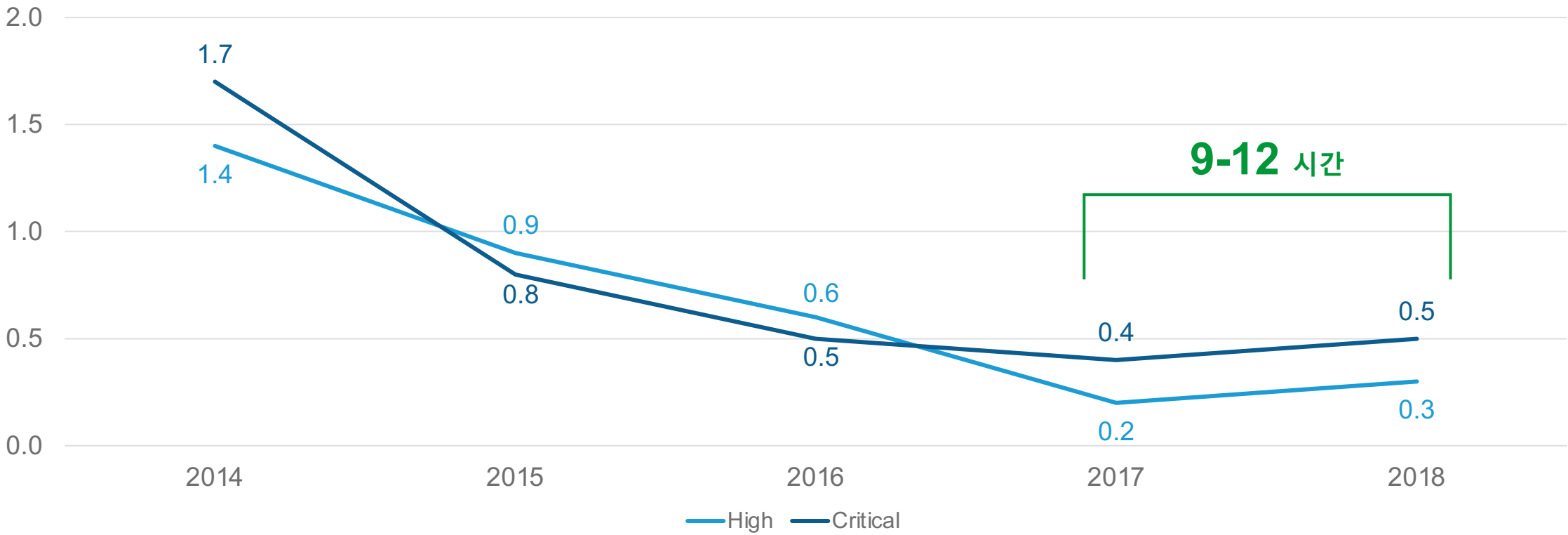
1. 개발자는 앱 코드를 보호하는 데 상당한 시간을 소비합니다.
2. 개발자는 클라우드 네이티브 보안 서비스를 개별적으로 구성합니다.
3. 개발자는 서비스를 관리하고 문제를 해결해야합니다.



Time is Gold: 개발자의 효율성 감소 및 보안 레벨 약화

보안 취약성은 보안 패치보다 더 먼저 발생됩니다.

“HIGH” / “CRITICAL” CVE 릴리즈 후 보안 레포트 릴리즈 시간



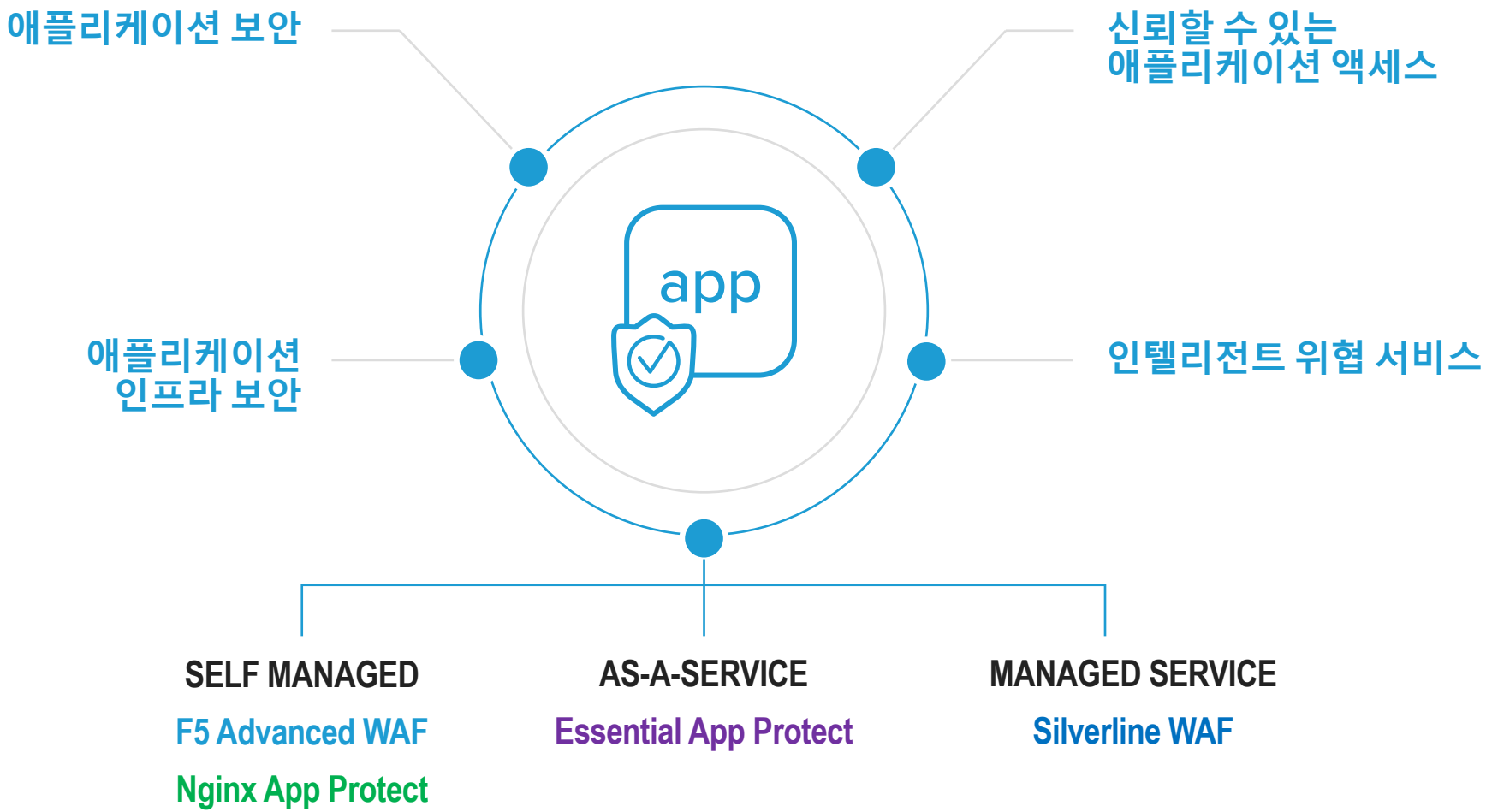
현실: 신속 하지만 불균형적인 IT 운영 구조

100	10	**1**
개발자	데브옵스	**보안**

보안이 아닌 속도를 위해 구축되었습니다.

보안 정책에 대해
클라우드 환경으로의
변환은 쉽지 않습니다.
따라서 보안 목표가
적절하게 시행이 필요합니다.

애플리케이션 배포 및 서비스 환경에 맞는 애플리케이션 보안



Advanced WAF
- Self-managed

Challenge

SecOps는 Agile 개발 모델을 따라갈 수 없습니다.

최신 애플리케이션은 마이크로 서비스가 API와 함께 배포되어 위협 노출 영역이 증가합니다.

DevOps에는 보안 제어를 적절하게 구현하는 도구가 없습니다.

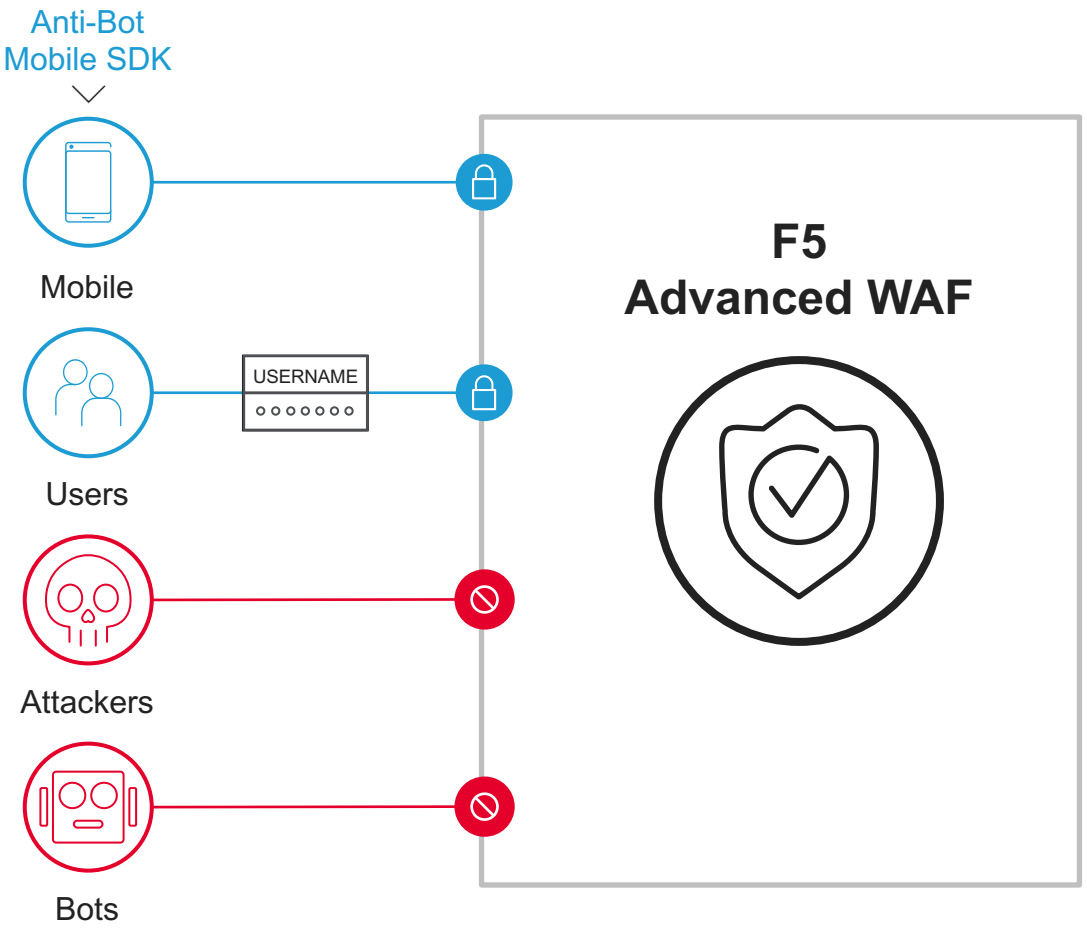
Key Benefit

마이크로 서비스 및 다양한 클라우드 확장에 맞는 단순화 된 구성 및 세분화 된 보안 정책

보안 관리를 위한 전용 API 보안 대시 보드

선언적 API 기반 구성 지원으로 DevOps 프로세스가 자동화 된 보안 구현을 위해 SecOps 관리 형 보안 정책 사용

Advanced WAF



고전적 WAF

- OWASP Top 10
- SSL/TLS 탐지
- 스크립팅 공격 방어

Advanced WAF

- 봇 공격 방어
- 크레덴셜 해킹 방어
- Layer 7 DDoS, API 공격 방어

NGINX App Protect
- Self-managed

Challenge

모던 애플리케이션 아키텍처에 대한 보안 부족

다중 클라우드 환경에서 일관되지 않은 보안 정책 해결

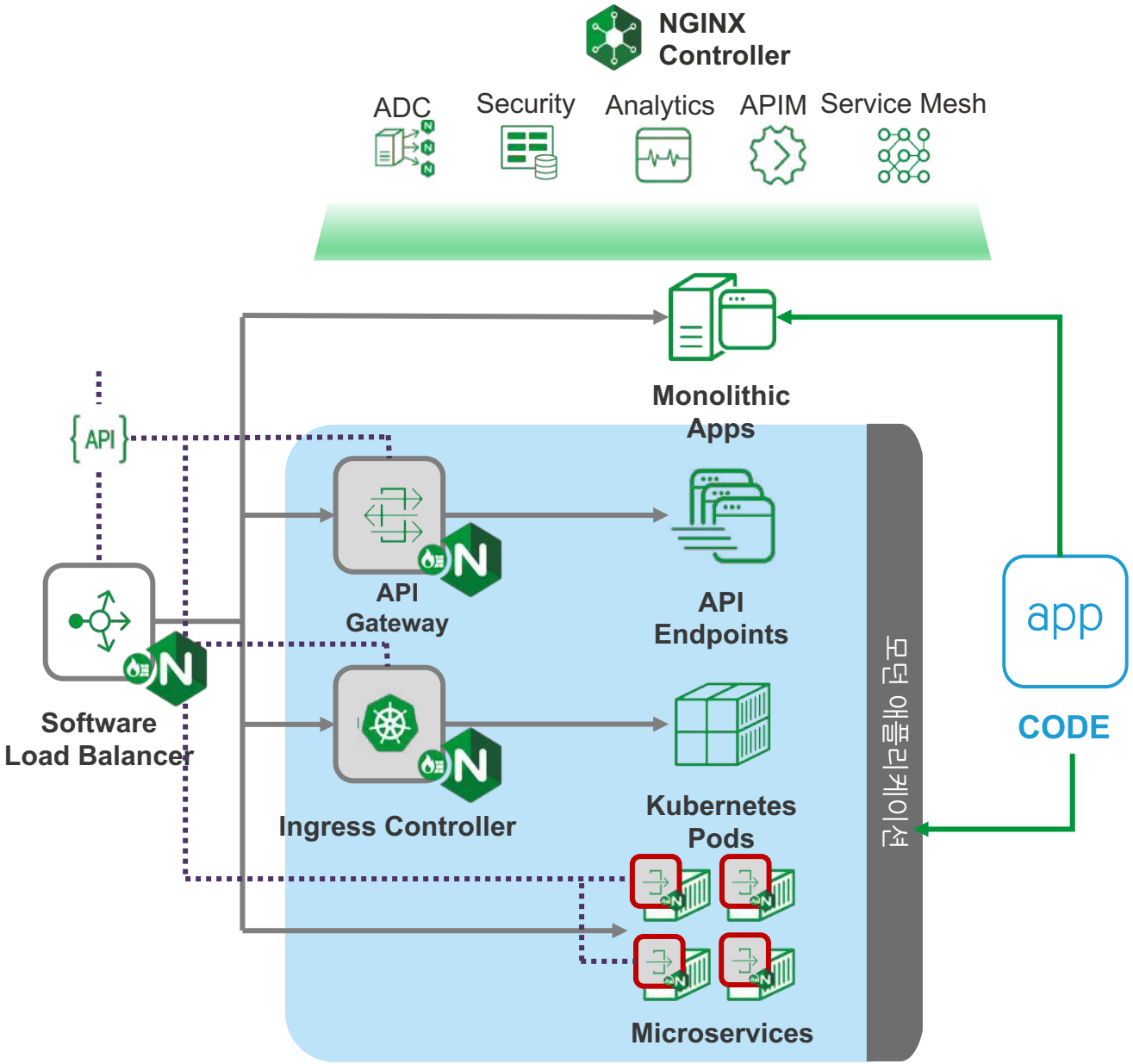
성능에 대한 제약

Key Benefit

최신 애플리케이션 아키텍처 (예 : 컨테이너 및 마이크로 서비스) 를 위한 강력한 보안 제어 자동화

CI / CD 파이프 라인으로의 통합을 통한 신속한 배포를 위해 설계된 최소 설치 공간

모던 애플리케이션 아키텍처에서의 대용량 보안 성능 제공



모던 앱 구축

성능과 확장성을 갖춘 고성능 보안

#1 웹 애플리케이션 플랫폼으로의 원활한

- 유연한 NGINX 통합
- 고성능
- 다양한 구성옵션
- OWASP Top 10 및 API 보안
- ModSecurity 대비 20배 이상의 성능
- 경량화 솔루션

https://web.microsoftstream.com/video/f091bb45-6a02-4187-b8bf-e47d02057b19

Essential App Protect
- WAF as a Service

Challenge

네이티브 클라우드 인프라에서의 애플리케이션 보안에는 애플리케이션 보호를 위한 적절한 보안이 부족합니다.

정교한 애플리케이션 제어로 인한 운영상의 문제가 발생될 가능성이 존재합니다.

IT 보안은 앱 배포에 병목 현상을 일으킬 수 있습니다.

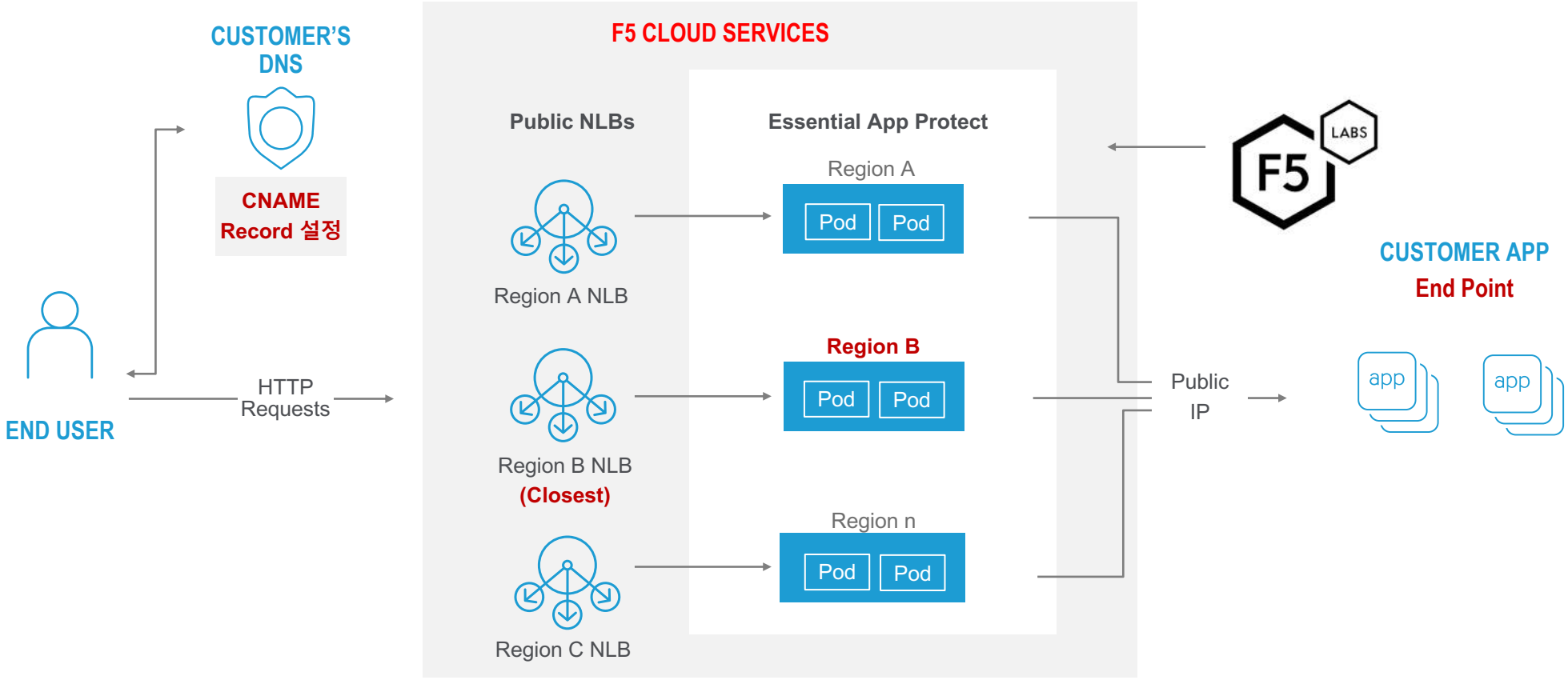
Key Benefit

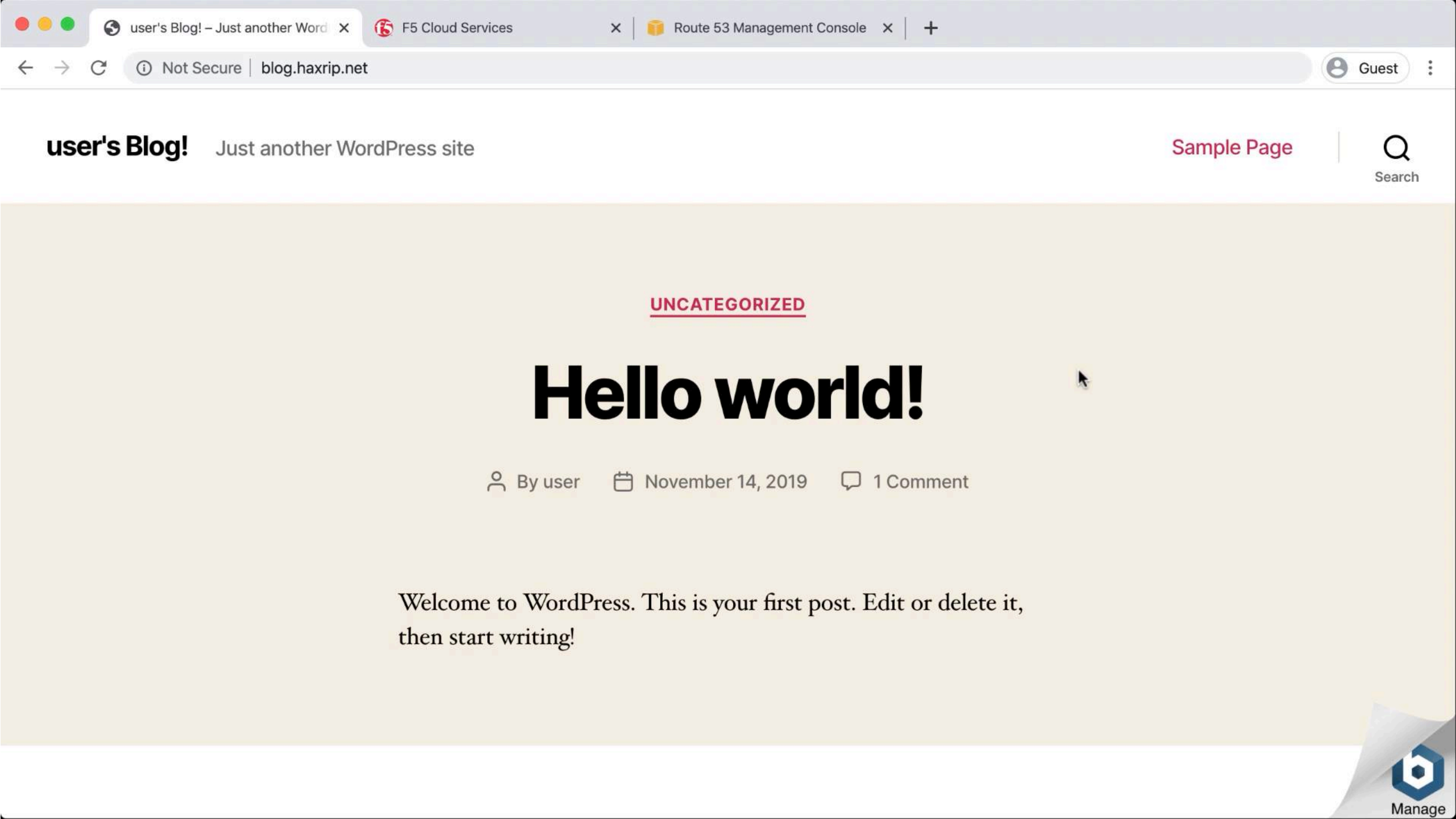
일반적인 웹 익스플로잇, 악성 IP 및 조정 된 공격 유형으로부터 신속하고 즉시 사용 가능한 보호

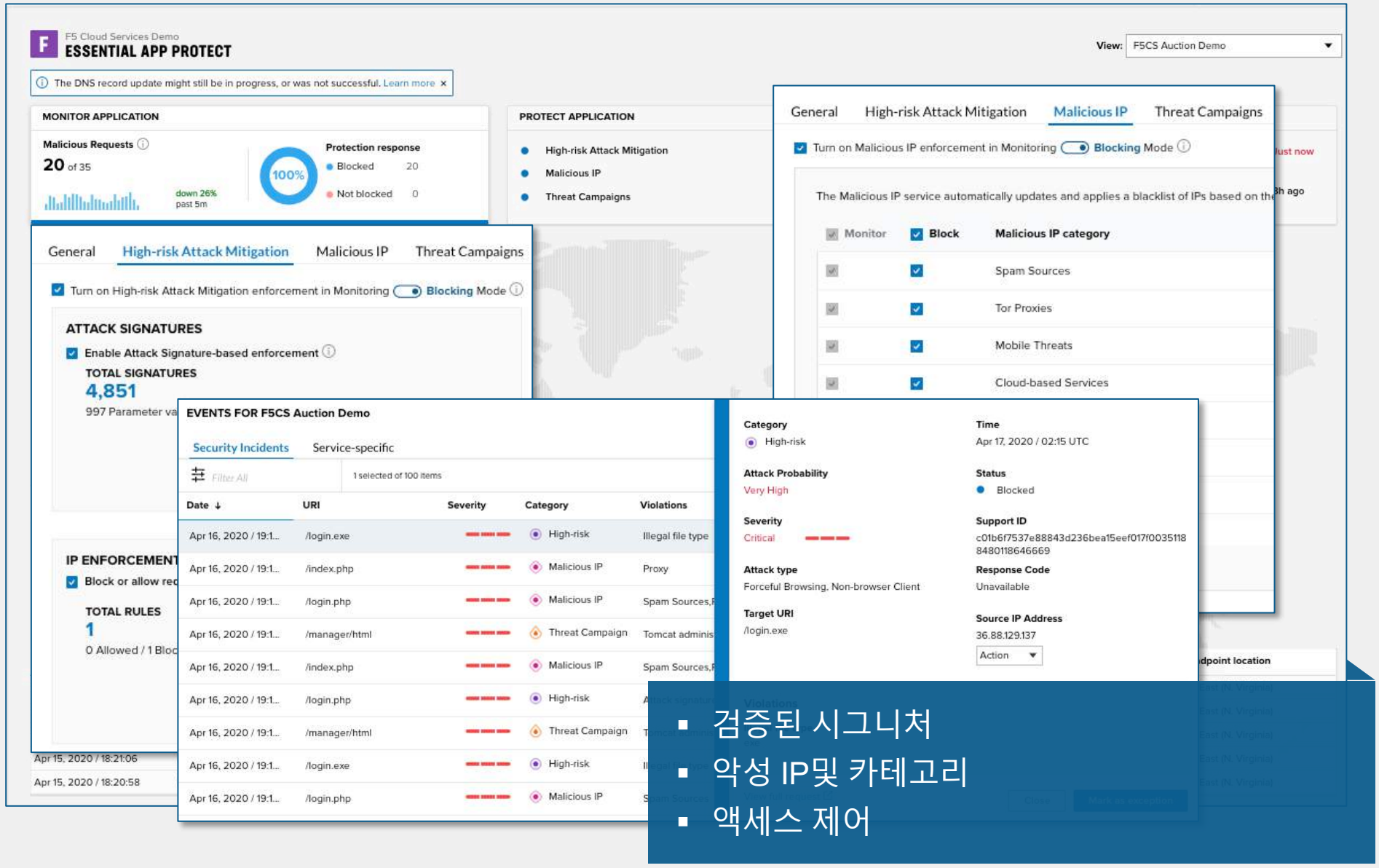
어디서나 모든 클라우드에서 대한 간단한 클라우드 기반 애플리케이션 보호

위협 환경 및 자동 완화에 대한 상시 가시성

Essential App Protect 아키텍처




user's Blog! – Just another Word
F5 Cloud Services
Route 53 Management Console
Not Secure
blog.haxrip.net
Guest
user's Blog!
Just another WordPress site
Sample Page
Search
UNCATEGORIZED
Hello world!
By user
November 14, 2019
1 Comment
Welcome to WordPress. This is your first post. Edit or delete it, then start writing!
Manage



- 검증된 시그니처
- 악성 IP및 카테고리
- 액세스 제어

원 클릭 적용

단계별 안내를 통한 간편한 프로비저닝

이전의 보안 전문 지식이 필요하지 않은 간단한 운영

공격 동향에 대한 시각적 맵과 해킹 방어 정보에 대한 손쉬운 액세스

- Cache 서버 연동을 통한 속도 개선

CDN 연동

애플리케이션 보안을 캐시 가능한 콘텐츠와 결합

글로벌 CDN 네트워크 활용

DevOps가 단일 소스에서 API를 통해 애플리케이션 제공 및 보안을 정의 할 수 있습니다.

Silverline WAF
- Full-Managed

Challenge

온 프레미스 / 클라우드 / 하이브리드에 걸쳐 점점 더 복잡 해지는 아키텍처 웹 / 앱 / 서버 기술의 급격한 변화

지속적으로 진화하는 위협 및 변화하는 비즈니스 속도에 따라 민첩한 보안 전략 필요

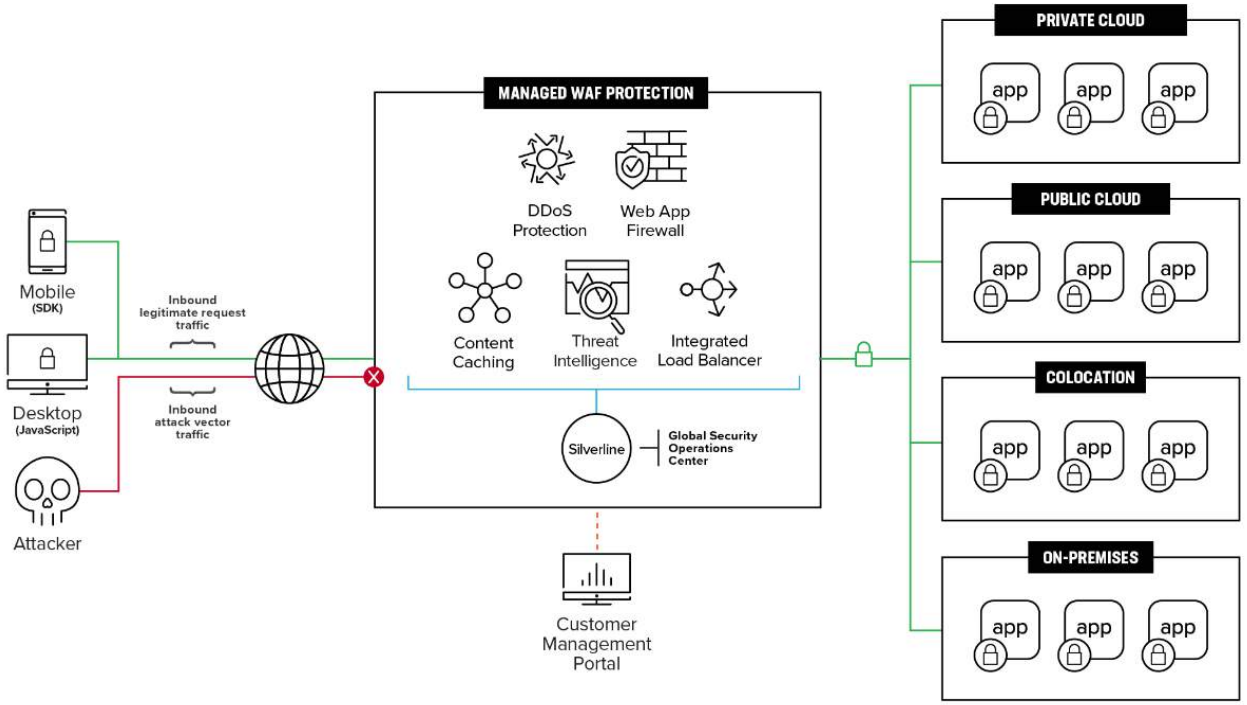
Key Benefit

L7 공격, 제로 데이 공격, OWASP Top 10 및 Credential Stuffing 등의 공격으로부터 보호

24x7 서비스에 WAF 전문가 지원

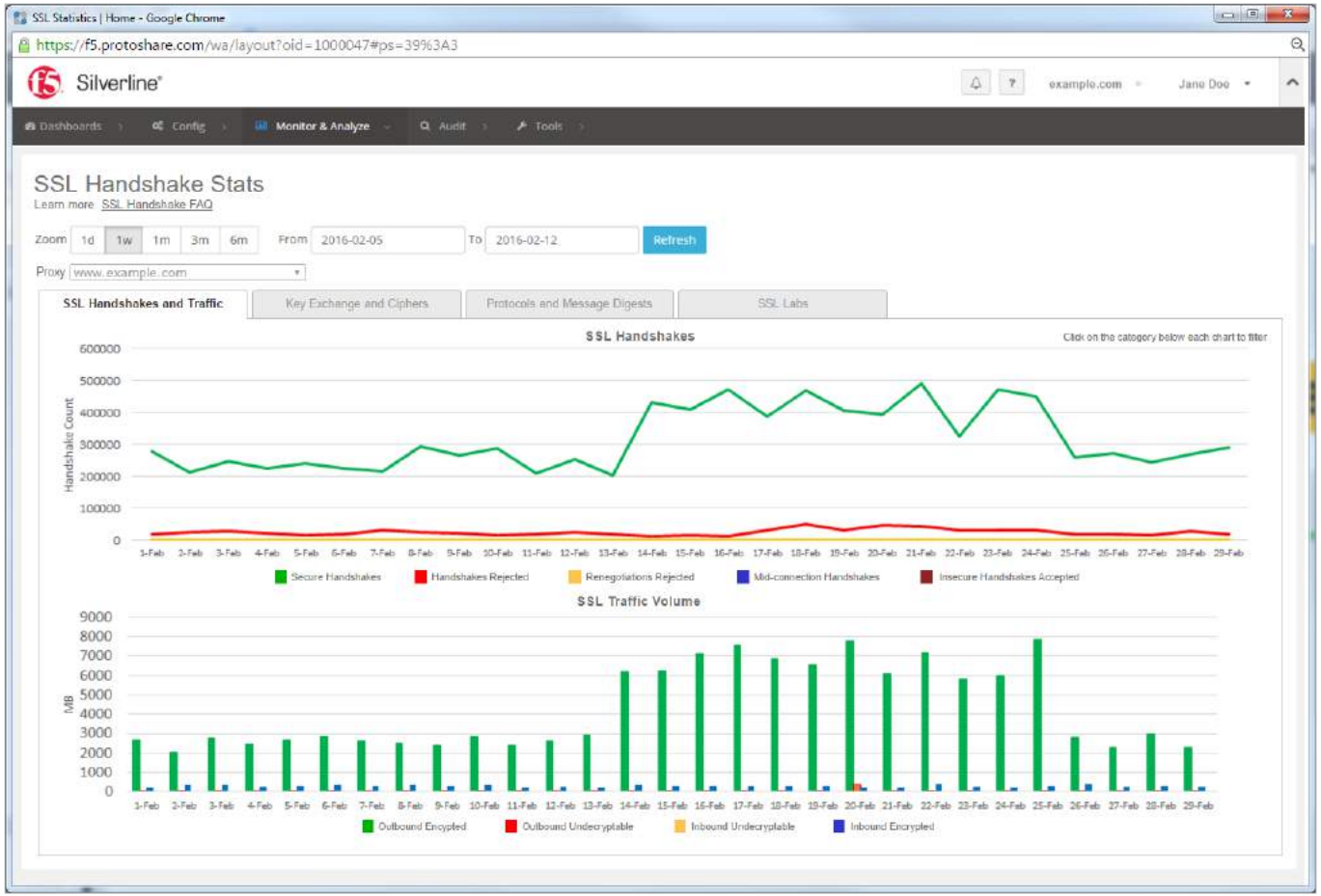
실시간 공격 데이터에. 액세스하고 앱을 보호하기. 위해 외부 인텔리전스 통합

WAF 관리 복잡성 제거, 정책 배포 속도 향상, 운영 비용 절감



F5 Silverline Portal Visibility: SSL

현재 어떤 CIPHER SUITE가 사용되고 있나요?



애플리케이션 /. SSL 가시성 확보

지원되는 SSL Cipher 를 변경할 계획이십니까?

- 암호가 사용되는 경험적 데이터 제공
- 사용중인 키 교환에 대한 통찰력 제공

애플리케이션 배포 및 서비스 환경에 맞는 애플리케이션 보안