앱 및 API 보안을 위한 모범 사례

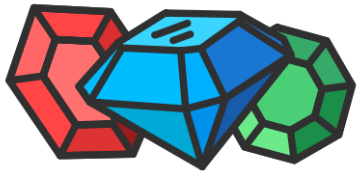
신민수
Networking Solutions Engineer
Citrix

2020년 11월

citrix

애플리케이션 및 API는

우리는 앱 및 API 세상속에서 살고 있습니다.



가장 중요하지만

가장 위험한 자산입니다

위협은 점점 더 정교해지고 있습니다.
멀티 클라우드로의 앱 전환은 복잡성과 단편화를 가중시킵니다.

하이브리드, 멀티 클라우드 환경에서의 CISO 과제

DevOps 및 SecOps
속도 불일치

API 관리 모델의 부족,
미지에 대한 두려움

인프라에서 앱 보안까지
기술 및 예산의 변화

앱, API 및 멀티 클라우드 전반에
걸친 일관된 보안 태세 부족

위협
앱 및 API
보안 태세

더욱 정교해지고 자동화된 앱 및
API 중심의 위협, 항상 한발 앞서가는 해커

정적인 규칙의 한계,
인공지능 및 머신러닝 필요

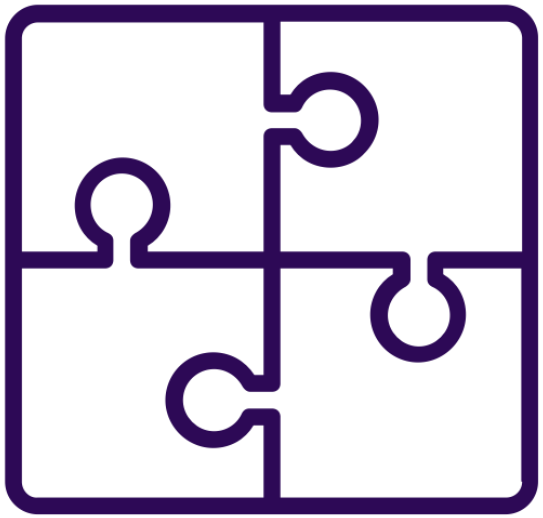
암호화된 트래픽에 숨겨진 멀웨어,
더 암호화된 웹 트래픽

멀티 클라우드에서 앱 및 API 보안
태세에 대한 전체적인 가시성 부족

citrix

앱 및 API 보안에 필요한 사항

전체적이고 검증된
계층화된 보호



멀티 클라우드로의
더 빠른 전환

규정 준수 및 관리를
위한 구축

DevOps 속도로
SecOps 활성화

모든 클라우드를 위한 단일 플랫폼

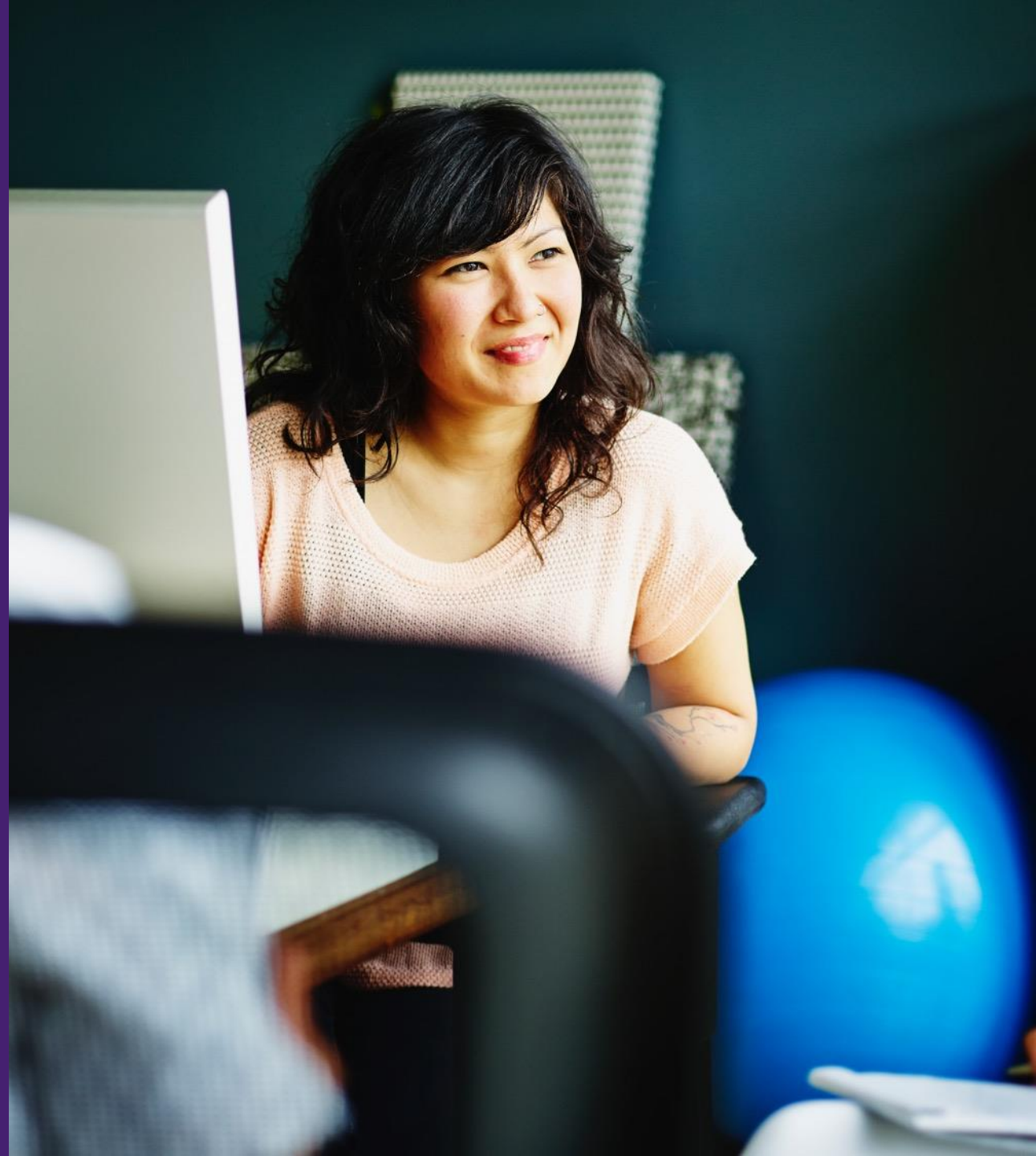
citrix

포괄적인 앱 및 API 보안 솔루션

citrix

모범 사례 체크리스트

- 인프라 보안
- OWASP Top 10, Zero-day Attack 및 CVE로 부터 웹 어플리케이션 보호
- Bot Management 및 위험 완화
- API Protection
- 정책 기반만이 아닌 행동 양식 기반의 인공 지능 및 머신 러닝
- 단일 및 마이크로서비스 앱 보호
- 일관성 있고 표준화된 보안 정책
- 포괄적인 가시성 및 분석



계층화된 Protection 기능 구축

citrix

동급 최고의 WAF로 웹 애플리케이션 보호

취약점의 92%가 네트워크가 아닌 애플리케이션에 있다고 보고되었습니다 — NIST 보고서

견고한 보안

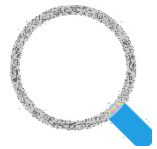
NSS Labs 권장
100% 공격 차단,
더 나은 **가격 대비 성능**,
PCI-DSS 규정 준수

알려진 공격과 미지의 공격으로부터 보호

OWASP Top 10: XSS, SQL Injection
알려진 위협에 대한 **Signatures**
제로 데이 공격 보호
애플리케이션 학습모드

배포 용이성

추가 장치 없음: Citrix ADC Premium Edition License
스캐닝 툴 통합: IBM Qualys, Cenzic, Rapid7, WhiteHat
동적 프로파일링: 학습된 rule에 의한 자동화된 정책 구축
이전 가능한 정책: WAF 정책을 개발 및 테스트 장비에서 실장비로 쉽게 내보내기



더 빠른 문제 해결을 위한 Insight

위반: 유형 및 볼륨
애플리케이션: 무엇이, 어디로부터 위협 받고 있는지
통합 모니터링: Citrix ADM

멀티 클라우드를 위한 유연한 옵션: On-Prem, Physical, Virtual, Private Cloud, Public Clouds

citrix

봇 공격으로부터 비즈니스 보호

상향된 Bot Management : 포괄적이고 통합된 인공지능 및 머신 러닝 기반

- Content Scraping
- L7 DDoS 공격
- 계정 탈취, 가짜 A/C
- 광고 사기 및 데이터 왜곡
- 신용 카드 Stuffing
- Inventory Hoarding

- 악성 IP 및 지역 차단
- 화이트리스트/블랙리스트 IP 지정
- IP 신뢰도 필터
- 3500개 이상의 Bot Signatures
- Device Fingerprinting
- 행동양식 분석, AI/ML
- Rate Limit, Redirect, CAPTCHA

TCO 절감
계층화된 보안을 위한 간편한 삽입
ADC 및 WAF와 통합

citrix

마이크로서비스 기반 애플리케이션 보호

Citrix를 이용하여 마이크로서비스 간 트래픽 (E-W) 사각 지대를 제거 합니다.

일관된 보안 태세
단일 및 마이크로서비스

더 신속한 문제 해결
전체적인 관측성 및 Citrix ADM

S-N 트래픽 보호
Citrix Ingress Proxy

API Protection
통합 Citrix API Protection

E-W 트래픽 보호
Service Mesh/Lite 아키텍처

Sidecar로 선택 보안 기능 적용
Sidecar 형태의 Citrix CPX

오픈 소스 Control Plane 수용
Citrix - Istio Citadel 통합

citrix

API Protection

2021년, API 사용으로 웹 지원 애플리케이션의 90%에서 더 넓은 범위의 공격대상을 형성할 것이다. - Gartner, 2019년 10월

포괄적인 보호 기능

단일 및 마이크로 서비스 기반 앱
Runtime 보호: 인증, 권한 부여, Rate Limit, TLS, WAF, Bot, 콘텐츠 라우팅, IP 화이트리스트 및 블랙리스트

API Analytics

사용량, 인증 성공 및 실패, Errors, Latency, TLS Cipher,
Key Strength, API Call Geo Location
상향된 분석을 위한 진화중인 로드맵

통합 싱글 패스의 장점

통합 WAF+Bot+API 보호의 단순성
성능 향상 및 TCO 절감

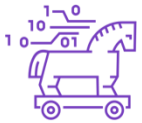
더 빠른 배포

개발자 도구 통합 - OAS/Swagger
Cloud Native 배포를 위한 CRD
Citrix ADM

WAF 및 BOT Protection으로 API Lifecycle 관리 Tool 보완

citrix

암호화된 트래픽에 숨겨진 공격으로부터 보호
TLS 리더십: 향상된 보호, 향상된 TCO, 향상된 관리



암호화된 트래픽에 숨겨진 멀웨어, 대부분 암호화 된 웹 트래픽

많은 비용이 발생하는 반복적이고 복잡한 TLS termination

TLS 프로토콜, Cipher 및 인증서의 관리 및 가시성 부족

CITRIX SSL

최신 TLS 프로토콜 및 암호 지원
TLS 1.3, ECC, FIPS 140-2

암호화된 트래픽 증가를 위한 TLS 확장
Citrix ADC - 동급 최고의 TLS 확장 및 가격 대비 성능
TLS를 Citrix ADC로 Offload하고 서버, 방화벽, IDS 및 AV 비용 절감
Citrix ADC로 TLS Offload를 함으로써 간편해진 중앙 집중식 인증서 관리

가시성 및 관리를 위한 심층 분석
프로토콜 및 Cipher (예: TLS 1.3/1.2, AES 256)
Keys strengths (예: 2048 vs 1024 bit, 만료된 인증서)

암호화 트래픽 사각지대 제거, 확장성 개선 및 비용 절감

citrix

앱과 API 보안에 대한 가시성 및 분석 확보

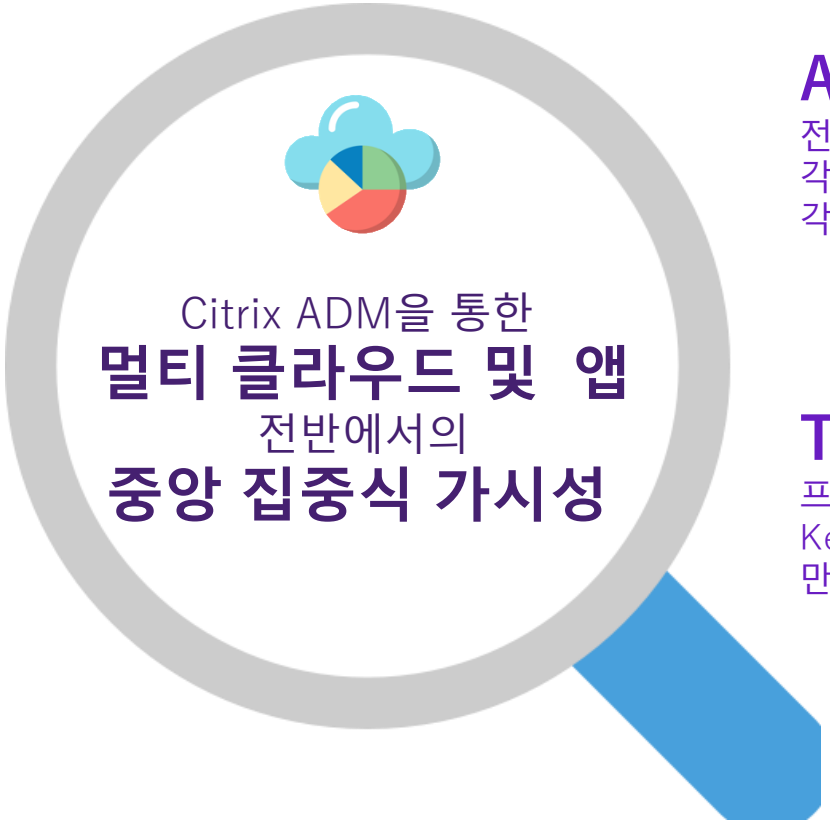
클라우드 전반에 걸친 전체적이고 직관적인 통합 관리

애플리케이션 공격

위반 횟수 및 유형 (예: SQL injection, CSS)
Top origin IP 및 Geolocations
주요 애플리케이션 공격, Zero-day attacks

봇 공격

Top origin IP 및 Geolocations
봇 유형 및 심각도 (예: 계정 탈취)
BI를 정규화 하는 전체 트래픽의 %로 표시되는 봇(Bot) 트래픽



API Insights

전체 트래픽 통계 (예: 요청, 응답, 데이터)
각 API에 대한 성능, 지연 시간, 인증 성공/실패
각 API에 대해 수행된 Rate limiting 작업

TLS Insights

프로토콜 및 Cipher (예: TLS 1.3/1.2, AES 256)
Keys strengths (예: 2048 vs 1024 bit)
만료된 인증서

가능한 조치: 주요 원인에 대한 신속한 파악, 규정 준수 및 관리 시행

citrix

단순성 및 유연성: 구매 및 배포 옵션

작업 시간 단축

유연한 라이선스 옵션

Perpetual & Subscription 옵션
필요한 곳으로 옮길 수 있는 Pooled Capacity Licensing

Premium Edition Citrix ADC에 대한 라이선스

ADC+ 모든 보안 기능

구입 및 관리할
추가 장치가 없는 단순함

통합 포트폴리오의 강력함: 기능의 일관성

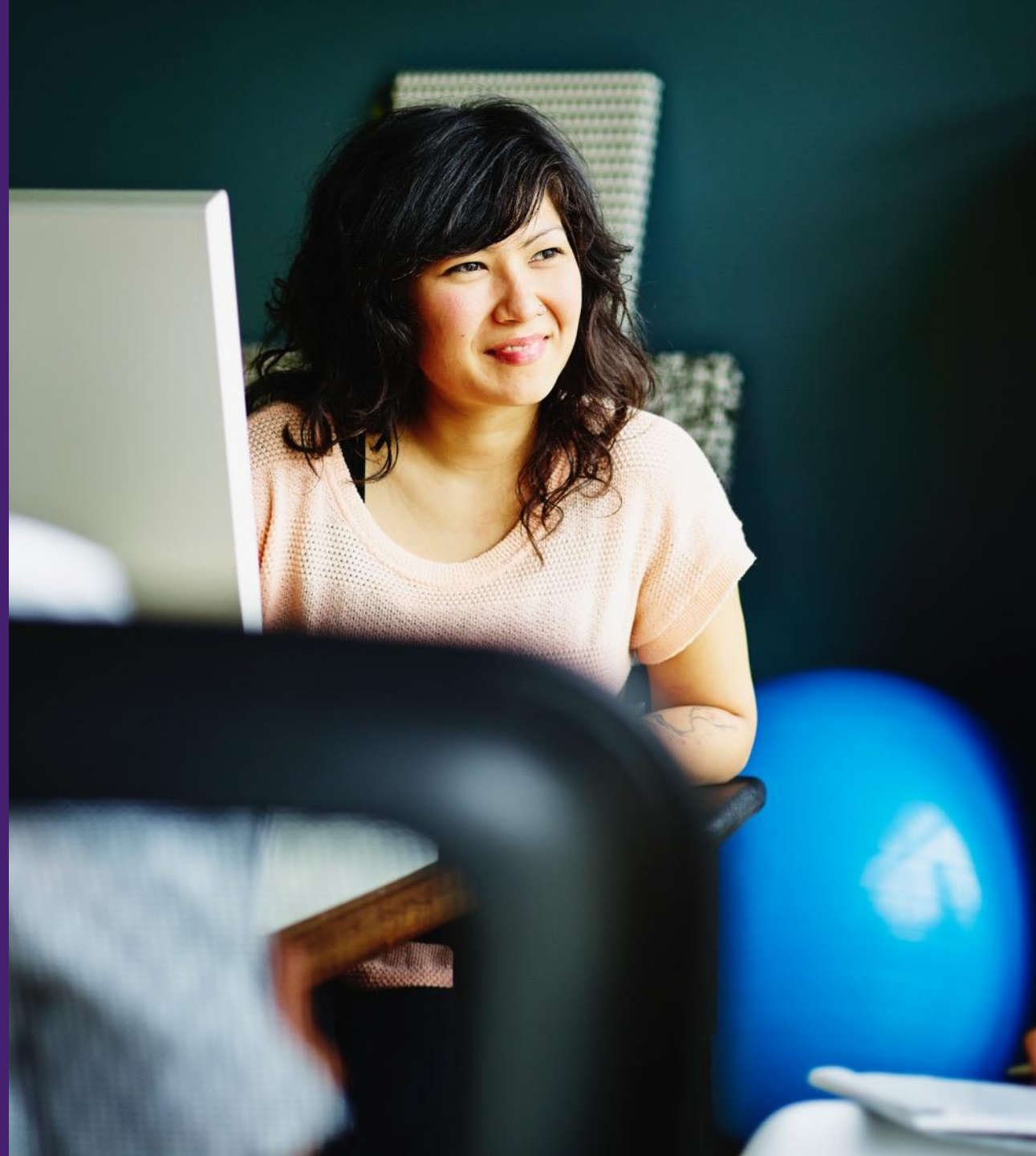
ADC: 모든 Form Factor, 모든 클라우드
ADM: 통합 모니터링

단일 라이선스 : All You Can Eat Protection

citrix

모범 사례 체크리스트

- ✓ 인프라 보안
- ✓ OWASP Top 10, Zero-day Attack 및 CVE로 부터 웹 앱 보호
- ✓ Bot Management 및 위험 완화
- ✓ API Protection
- ✓ 정책 기반만이 아닌 행동 양식 기반의 인공 지능 및 머신 러닝
- ✓ 단일 및 마이크로서비스 앱 보호
- ✓ 일관성 있고 표준화된 보안 정책
- ✓ 포괄적인 가시성 및 분석



앱 및 API 보안 파트너로서의 Citrix

고객의 목표

전체적이고 검증된
계층화된 보호

규정 준수와 관리를
위한 구축

멀티 클라우드로의
더 빠른 전환

DevOps 속도로
SecOps 활성화

Citrix 솔루션

모든 클라우드를 위한 단일 플랫폼