공급망 공격 대응을 위한 제로트러스트 전략

Akamai

Akamai Korea

Hyun Do Kim

Strategic Account Executive. Sr.

Mu Kwon Lim

Solutions Engineer. Sr.

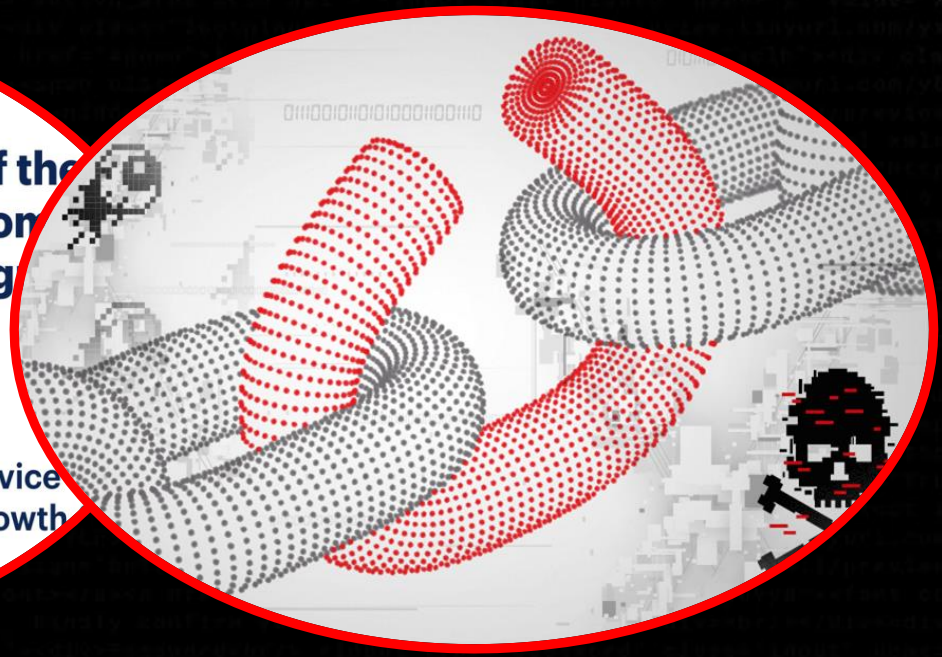
공격 표면의 급격한 증가

사이버 공격의 변화

IT 환경 변화로 인해 지능화 되어가는 사이버 공격

Social Engineering

API Attack



Supply Chain Attack

Akamai

사이버 공격의 변화

엄청난 피해를 유발하는 공급망 공격

> *시스템 제조, 개발, 공급 업체, 서비스 제공 업체를 통해 **기업의 정보 시스템에 침투하여 악용**하는 행위*

Target to pay $18.5M for 2013 data breach that affected 41 million consumers

Kevin McCoy, USA TODAY

Published 4:10 p.m. ET May 23, 2017 | Updated 6:42 p.m. ET May 23, 2017

POS 시스템 해킹

CYBERCRIME

NotPetya Operators Accessed M.E.Doc Server Using Stolen Credentials: Cisco

The group behind last week's destructive NotPetya attack was able to access M.E.Doc's update serv courtesy of stolen credentials, Cisco has discovered.

업데이트 시스템 해킹

Czech software firm Avast says CCleaner was attacked — again

This time the intrusion "was an extremely sophisticated attempt agair to leave no traces of the intruder or their purpose," the company's CISC

다운로드 서버 해킹

Massive SolarWinds hack has big businesses on high alert

By Rishi Iyengar, CNN Business

3 minute read · Published 10:14 AM EST, Sat December 19, 2020

업데이트 시스템 해킹

MALWARE & THREATS

CISA Sets 48-Hour Deadline for Removal of Insecure Ivanti Products

Zero-Day 취약점

In an unprecedented move, CISA is demanding that federal agencies disconnect all instances of Ivanti Connect Secure and Ivanti Policy Secure products within 48 hours.

ivanti Products Solutions Support Resources Partners Company Get Started

Ransomware 2021 Year End Report Reveals Hackers are Increasingly Targeting Zero-Day Vulnerabilities and Supply Chain Networks for Maximum Impact

Akamai

사이버 공격의 변화

공급망 공격 대응을 위한 노력

SBOM

- 보안 취약성 식별
- 오픈소스 사용 규정 준수
- 제품 관리 및 업데이트
- 공급망 투명성

Bug Bounty

- 보안 취약점 발견
- 보안 강화
- 보안 커뮤니티 협력
- 커뮤니케이션 강화
- 보안 인식 증진
- 취약점 경쟁력 강화

MITRE ATT&CK

- 행위 기반 지식
- 행위 표준화
- 프레임워크와 데이터소스 통합
- 통합된 분석 도구

MITER ATT&CK Framework

사이버 공격 단계를 이해하고 방어 전략 수립 필요

공격 실행 단계를 이해한 방어 전략 필요

공격자의 노력과 더 많은 노력이 필요한 방어자(?)

누가 승자인가?

랜섬웨어 공격

공급망 공격

피싱 공격

AI 기반 공격

사회공학 공격

피해손실
$103억+

일 피해불만
2,175+

년 피해불만
651,800+

5년간 신고 건
730만+

클라우드 확산

원격 근무 증가

애플리케이션 증가

비즈니스 환경 변화

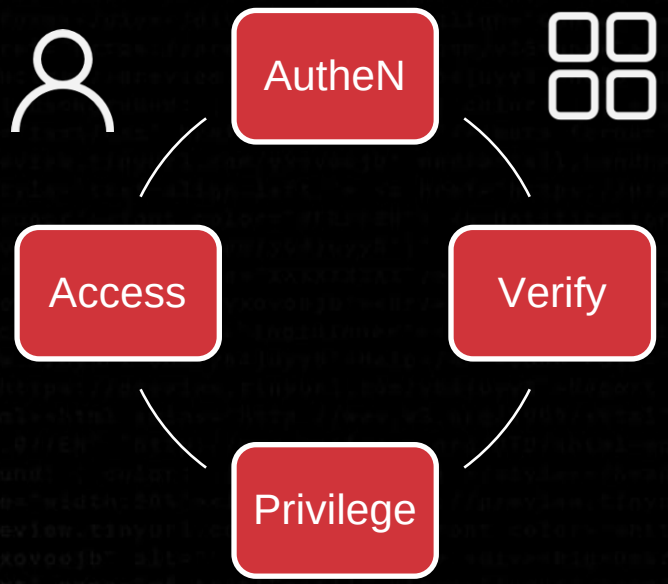
마이크로서비스 아키텍처

> *공격 표면*을 최대한 줄이고 *전문가 서비스* 필요

제로트러스트로의 관심

공격 대응을 위해 새로운 대안이 필요

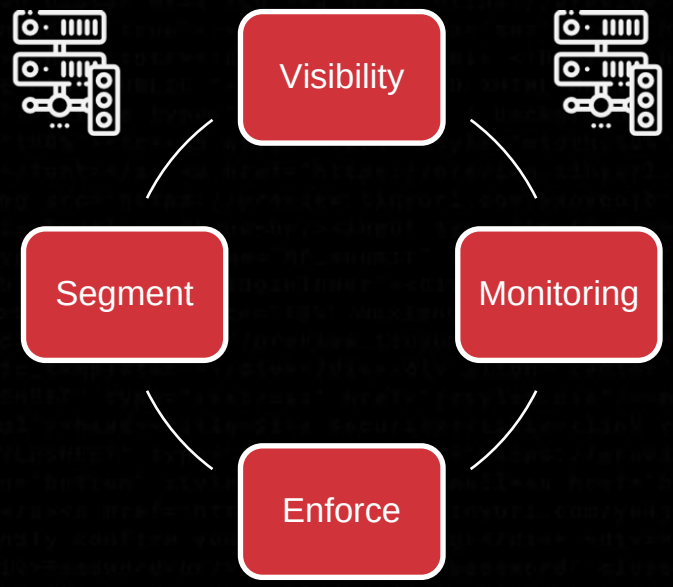
Zero Trust Network Access



- 접속자는 강력한 인증 필요
- 접속 장치는 항상 검증
- 사용자는 최소 권한으로 리소스에 접속

SEGMENTATION

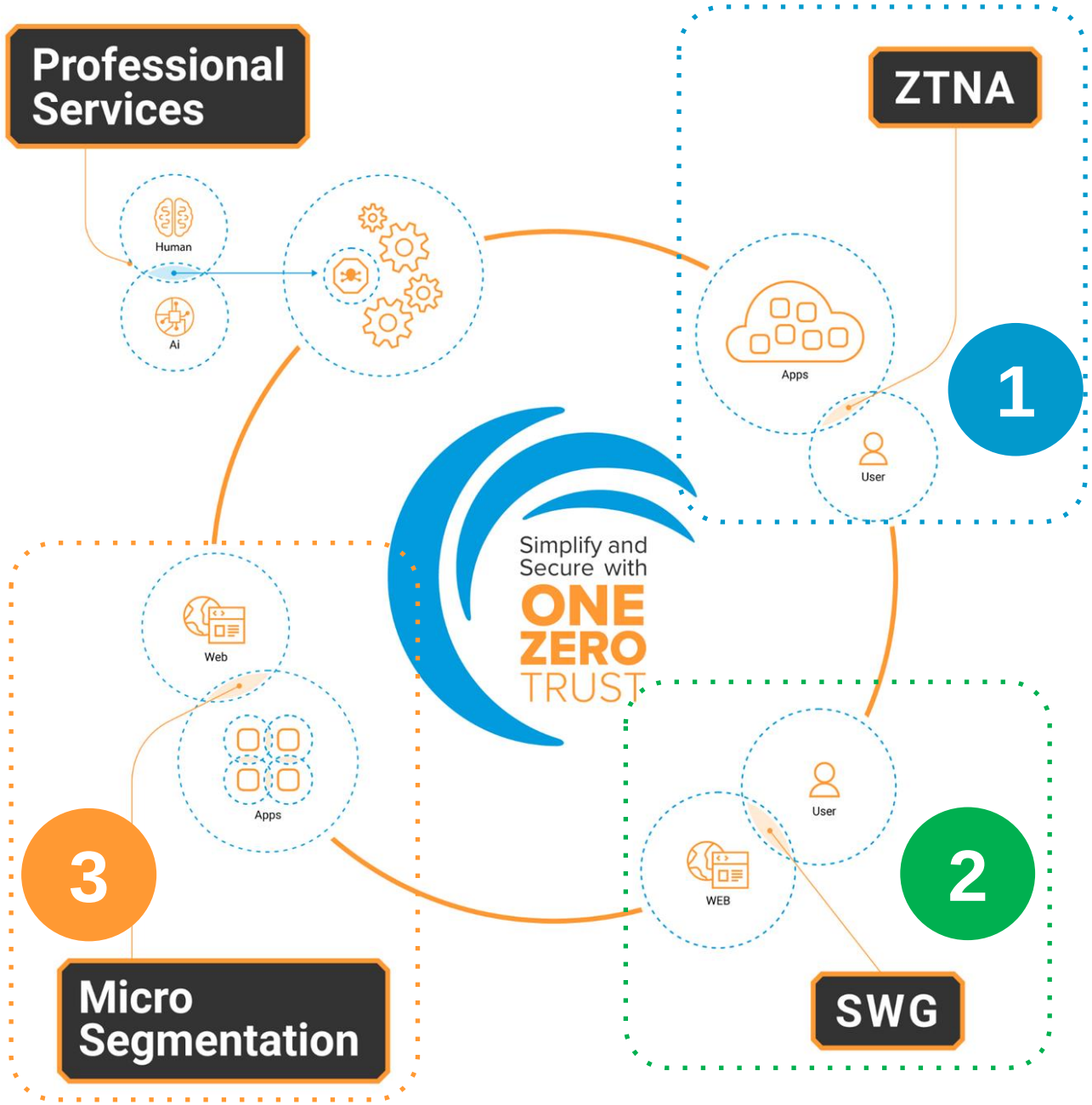
Micro - Segmentation



- 모든 통신은 식별되고 모니터링
- 권한이 없는 워크로드로 접근은 차단
- 확인되지 않은 횡 이동은 차단

Akamai

아카마이 제로트러스트



Never Trust / Always Verify / Least Privilege

1
- *강력한 Akamai MFA*
- *접속 단말의 상태 검증*
- *안전한 암호 통신 유지*
- *최소한의 APP 접근 권한 유지*

2 — *모든 사용자 인터넷 접속 안전 유지*

3 — *모든 자산은 세분화되어 관리*

Akamai

MITER ATT&CK Framework

단계별 방어가능한 수준을 제공합니다.

Akamai는 각 단계를 이해하고 방어 전략을 제공합니다

전통적인 보안 시스템의 한계

공급망 자체가 공격 벡터 중 하나로 자리 잡히고 있습니다

BUSINESS

- 하이브리드 환경의 ***유연성 부족***
- 리소스 요구에 따른 ***확장성 부족***
- 환경 변화에 따른 ***시장 요구 대응 지연***

COST

- 시스템 운영관리에 따른 ***인건비***
- 시스템 유지 ***관리 비용*** 증가
- 시스템 변경관리에 따른 ***노력비용***

SECURTY

- 메인 코드에 ***오래된 소스코드*** 사용
- 시스템 ***아키텍처 변경*** 없이 형상 유지
- ***취약점 관리*** 소홀

Akamai 가 고객에게 제공하는 숨은 노력

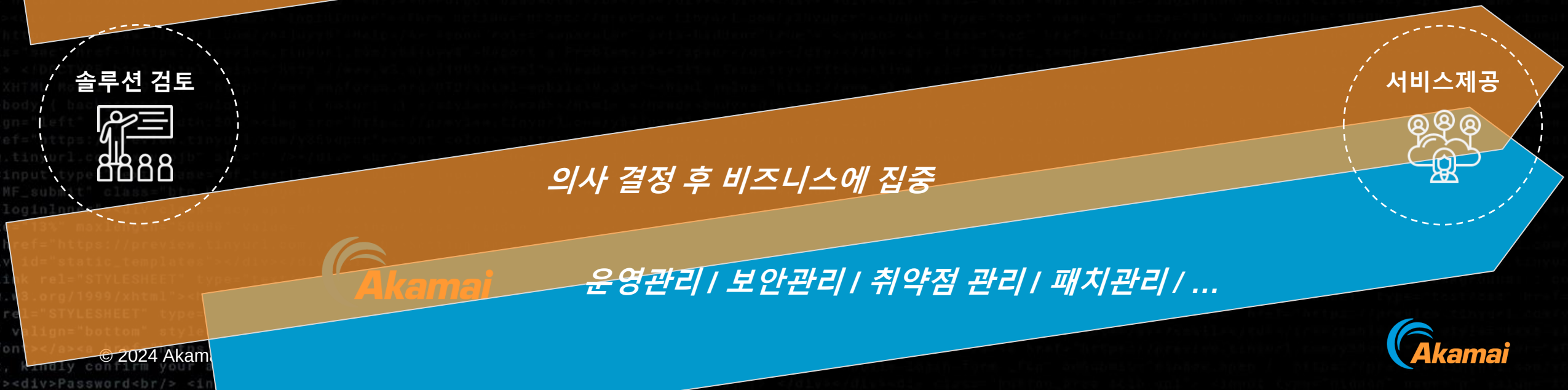
- On-Prem, Cloud, Hybrid ***쉬운 배포***
- ***100% 서비스 보장***을 위한 처리 능력
- 요구 변화에 ***즉각 대응가능한 유연성***

- 시스템 ***운영 비용 Zero***
- 시스템 ***관리 비용 Zero***
- 아키텍처 변경관리 ***노력비용 Zero***

- 주기적인 ***시스템 취약점 점검***
- 지속적인 ***시스템 Hardening***
- FedRamp, PCI, SOC II 등과 같은 ***인증 유지***

신규 솔루션 도입에 대한 피로

On-Prem 방식과 Cloud 방식의 도입



아카마이 고객 사례

수많은 기업들이 아카마이를 선택합니다

“Crowd-Sourced Platform”

Challenge

- 전세계 분산된 직원들의 ***안전한 원격 접속*** 필요

Requirement

- 안전하고 ***간편하며 편리한 원격 보안 접속*** 솔루션 필요
- ***데이터 무결성, 개인 정보 보호, 애플리케이션 보안*** 보장 필수
- ***사용자별 지정된 App만 액세스***할 수 있어야 함
- 설정, 구성, 변경이 쉬우면서 높은 수준의 보안 보장필요
- ***규정 준수, 보안, 고가용성 및 저렴한 비용***의 솔루션 필요

고객은 **Akamai ZTNA** 선택하여 안전하게 서비스 하고 있습니다.

“Fire Equipment Manufacture”

Challenge

- ***Ransomware 대응*** 필요

Requirement

- ***Ransomware 사고 경험***
- Micro-Segmentation 적용한 시스템만 피해 없음
- 전사 시스템에 Micro-Segmentation 적용 요구
- ***네트워크 구성 변경, 시스템 다운타임 없이 적용***해야 함
- 이원화된 관리 포인트를 ***하나로 통합***해야 함

고객은 **Akamai Micro-Seg**을 선택하여 랜섬웨어로 부터 자산을 보고하고 있습니다.


Akamai