

MEGAZONE WEBINAR

- Akamai 3-6-9 solution: EAA, ETP

2019. 03. 21(Thu)

Time	Contents	Speaker
14:00-14:05	1. 메가존이 제시하는 아카마이 온라인 비즈니스 솔루션 정의 및 영역 2. 비즈니스 챌린지의 정의 및 영향	신보람 (Akamai 마케팅)
14:05-15:00	1. 메가존이 바라보는 인터넷 제로 트러스트(Zero Trust) - 기업 어플리케이션 접속을 제어하고 사용자를 표적 위협으로부터 보호하는 방법 2. 고객 사례(비즈니스 챌린지) - 외부에서 접속하는 일이 많은 우리 회사의 보안 사각 지대를 어떻게 보완할 것인가? - 메일이나 그룹웨어 등을 통해 우리 회사의 구성원이 감염시키는 바이러스나 침입을 어떻게 통제할 것인가? 3. Q&A	신동준 (Akamai 영업)

메가존이 제시하는 아카마이 온라인 비즈니스 솔루션과 비즈니스 챌린지



1. What is Akamai 3·6·9 Solution?

아카마이 온라인 비즈니스 솔루션

기업이 겪고 있는 온라인 비즈니스 챌린지
(Business Challenge)에 대한 **해결책**



1. What is Akamai 3·6·9 Solution?

3

서비스 증대
Service Expansion

- Managed Service
- Premium Service&Support
- Monitoring Service

6

보안 강화
Security Enhancement

- WAF(Web Application Firewall)
- Web Application Protector
- Kona DDoS Defender
- Kona Site Defender
- Fast DNS
- ETP

9

성능 개선
Performance Improvement

<웹&모바일 가속>

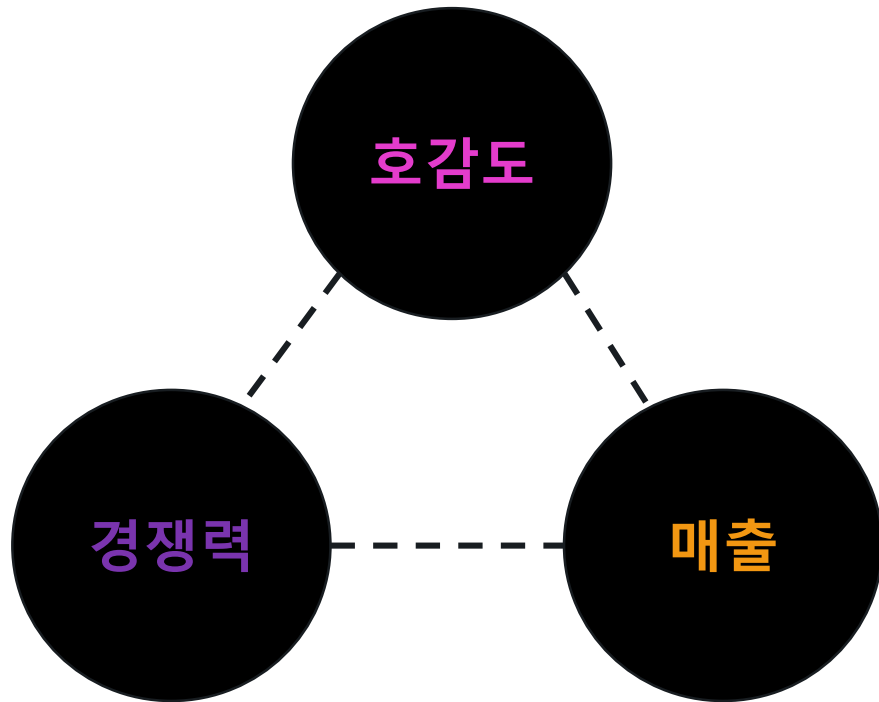
- Dynamic Site Accelerator
- Mobile Accelerator(ION)
- Load Testing(Cloudtest)
- Site Performancemanagement(mPulse)
- IP Application Accelerator

<이미지 최적화>

- Image Manager
- <DNS&트래픽>
- Application Load Balancer
- Global Traffic Management
- Fast DNS

2. What is Business Challenge?

기업이 온라인 상에서 비즈니스를 진행함에 따라 발생하는 문제상황

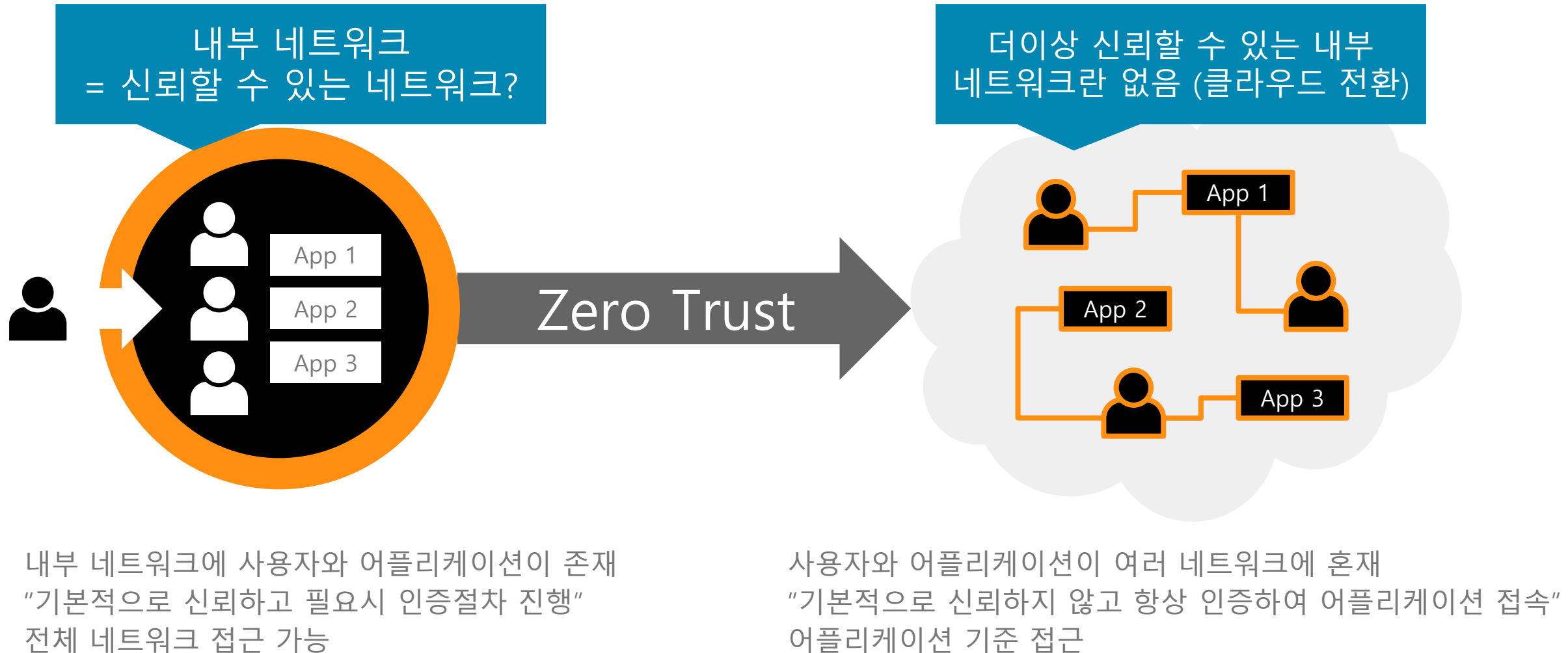


2. What is Business Challenge?



Zero Trust와 Akamai

Zero Trust란 무엇인가?



Akamai Zero Trust



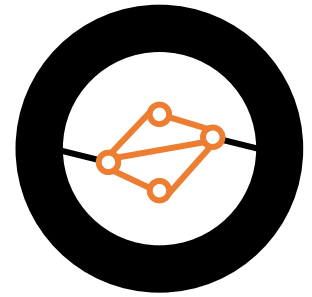
인증된 사용자 혹은
디바이스 기준으로
어플리케이션 접속
혹은 데이터 전송



멀웨어 와
데이터 탈취에 대한
선제적 대응



빠짐없는 데이터 접
근 가시성을 위해
항상 인증절차 수행

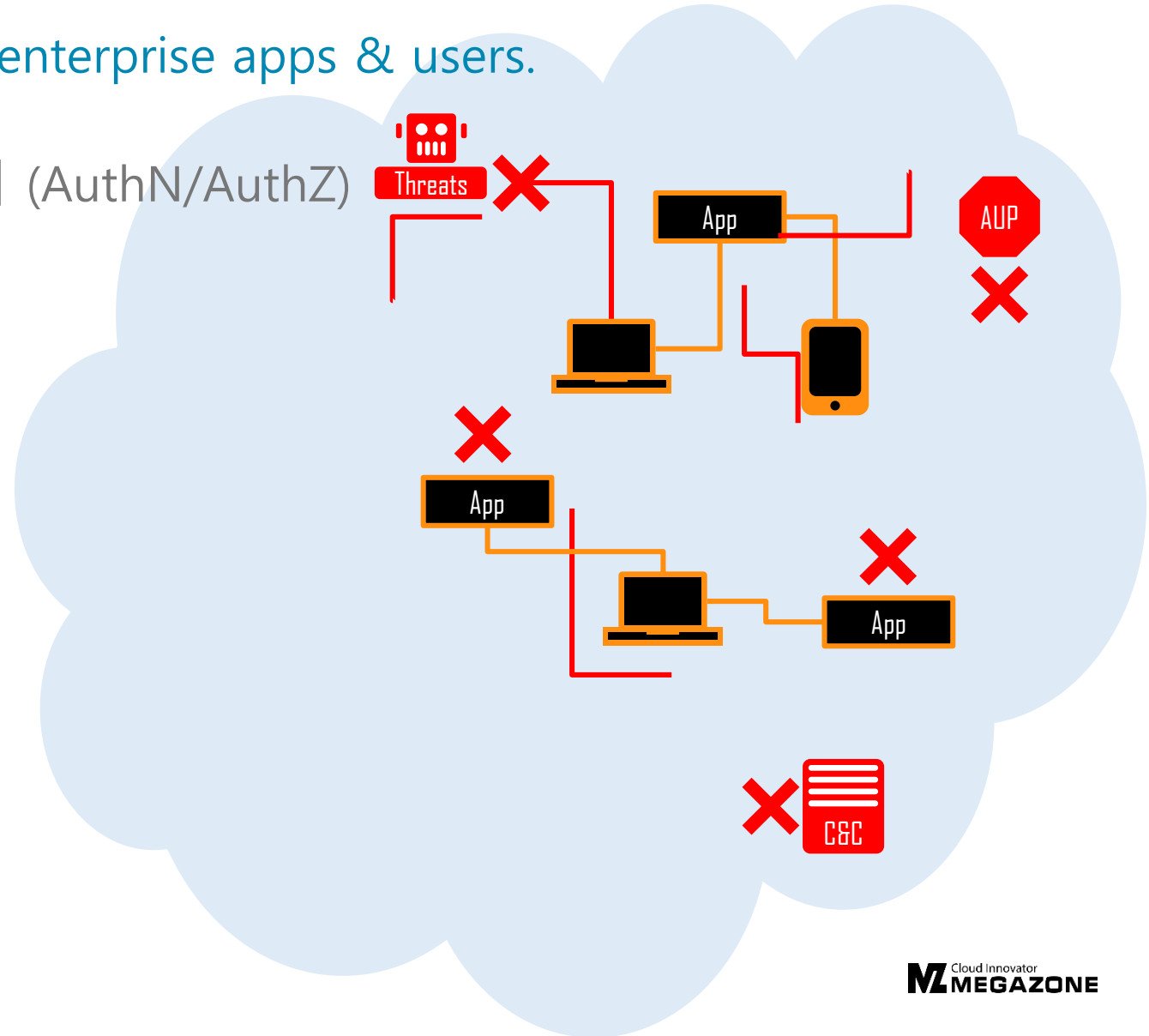


인터넷에서
기업 어플리케이션의
성능 보장

Akamai Zero Trust

Akamai Intelligent Platform to secure all enterprise apps & users.

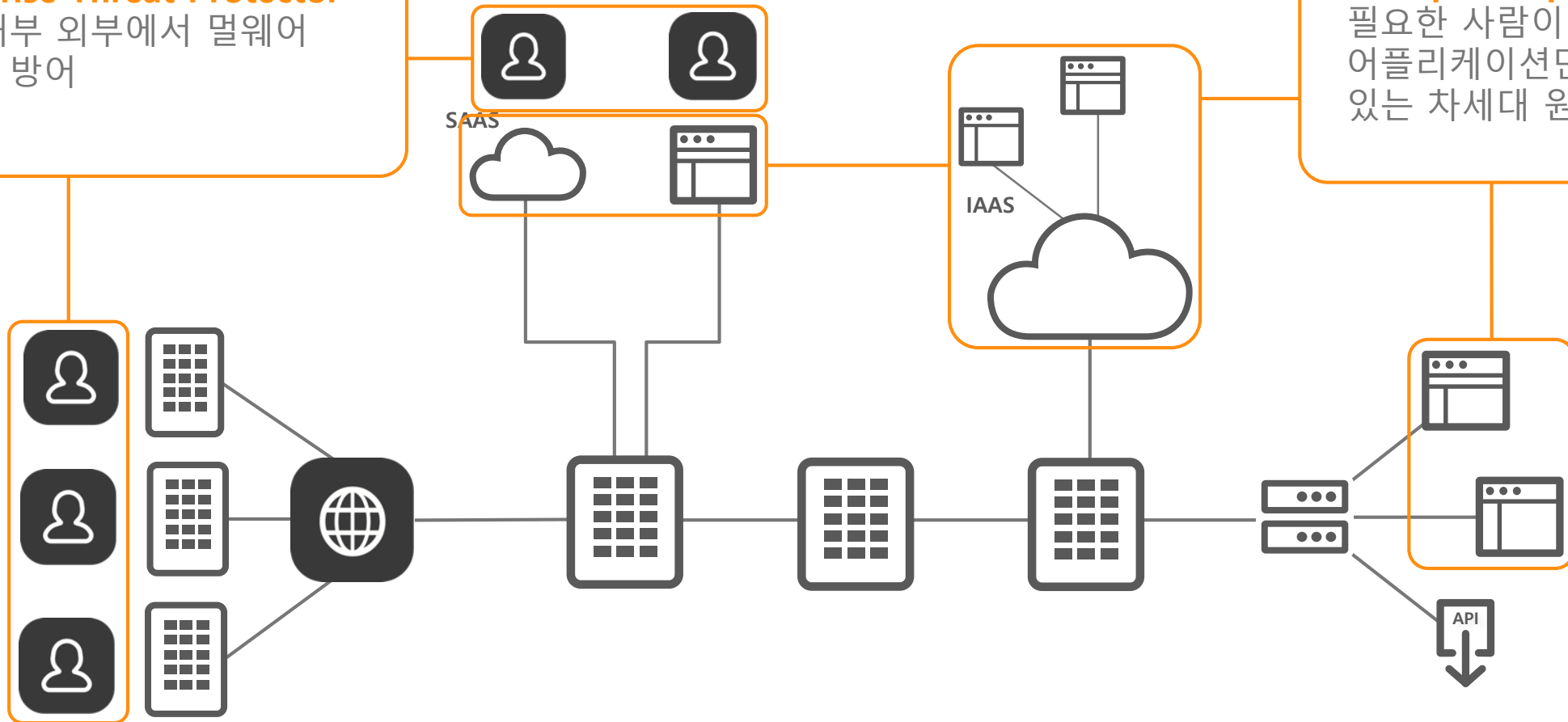
- 사용자 확인 및 어플리케이션 접근제어 (AuthN/AuthZ)
- 멀티팩터 인증을 통한 Single Sign On
- 어플리케이션의 성능 및 보안 향상
- 향상된 위협 방어
- 인라인 데이터 검사



Akamai Zero Trust

Enterprise Threat Protector

기업 내부 외부에서 멀웨어 공격을 방어



Enterprise Application Access

필요한 사람이 필요한
어플리케이션만 접근하게 할 수
있는 차세대 원격 접속 솔루션

Enterprise Application Access



기업 네트워크 사용자 보호

방화벽 또는 보안 그룹의 모든 인바운드 트래픽을 차단하고 인터넷에서 인프라를 보이지 않게 구성



엔터프라이즈 어플리케이션을 위한 Multi-factor 인증

이메일, SMS 또는 TOTP에서 MFA를 사용하여 사용자를 인증함으로써 무단 접근을 최소화



로컬 서버 로드밸런싱

다양한 부하분산 알고리즘을 사용하여 내부 인프라에 대한 트래픽 균형을 유지



중앙 집중식 보안 및 접근 제어

클라우드 및 On-Prem를 통한 사용자가 사용할 권한이 있는 특정 앱 및 접근 권한을 결정



모든 엔터프라이즈 어플리케이션의 Single sign-on 구성

Office 365, salesforce.com을 포함한 On-Prem, IaaS 및 SaaS 어플리케이션에 완벽한 접근 가능



사용자 활동의 감시

모든 사용자의 클라이언트 정보 및 수행한 작업과 위치 정보를 기록하여 HIPPA 및 PCI 준수를 보장

Enterprise Threat Protector



악의적인 목적의 도메인에 대한 접근을 식별하고 차단

Malware 또는 피싱을 목적으로 하는 사이트를 호스팅하는 것으로 알려진 악성 도메인에 대한 요청 또는 사이트와의 통신을 차단



부적절한 콘텐츠에 대한 접근 차단

기업 네트워크에서 수용 가능한 인터넷 사용 정책을 효과적이고 일관성 있게 시행



사용자와 가능한 웹 어플리케이션 보호

프로토콜, 요청제한, HTTP 정책위반, Command Injection 공격, 트로이 백도어 및 아웃바운드 콘텐츠 유출과 같이 미리 정의된 구성 가능한 응용프로그램 레벨의 방화벽 보호 컬렉션 제공



악성코드 등에 영향을 받은 장치의 통신차단

악성코드 등에 의해서 감염된 장치의 기존 연결이 악의적인 행위자의 CnC(Command and Control) 인프라로 연결되는 것을 차단



DNS 기반 데이터 추출 방지

악의적인 행위자가 DNS 프로토콜을 사용하여 민감한 기업 데이터를 추출하는 것을 방지

Enterprise Application Access

(차세대 원격 접속 솔루션)

Remote Access의 고려사항



전용 장비 / 라이선스 / S/W 설치 / 보안정책 변경 등이 필요함

Remote Access의 고려사항

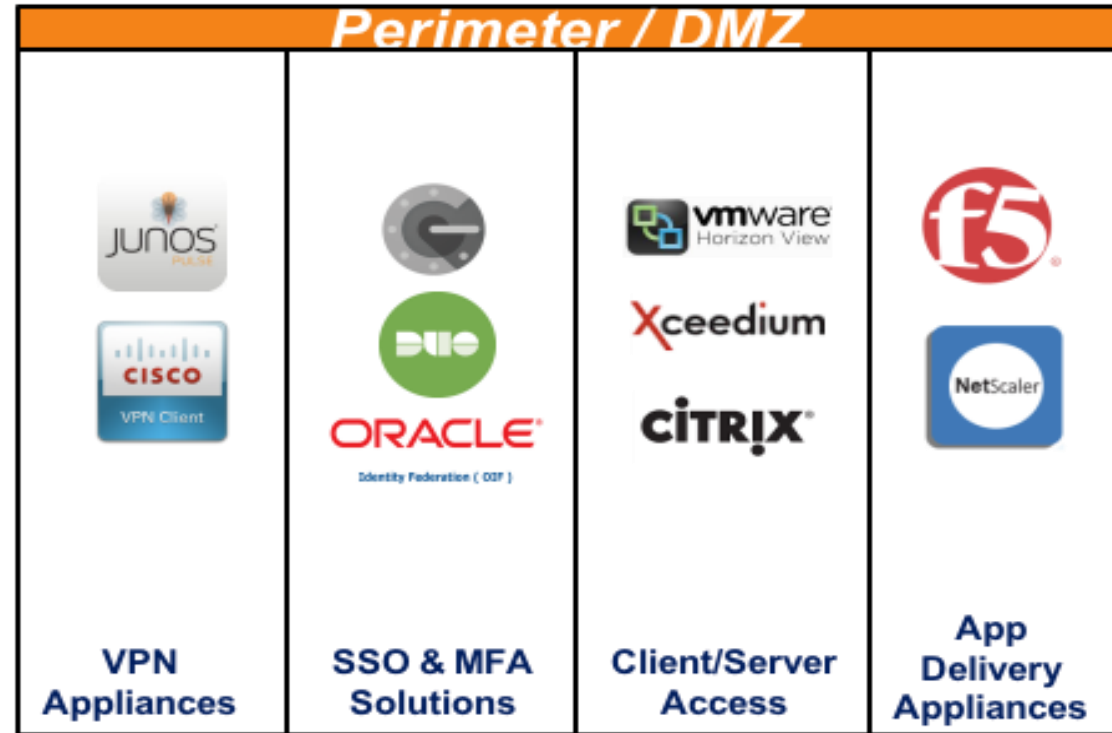
- 공개된 VPN 장비 IP 및 서비스 Port에 대한 다양한 공격
- 보안장비 운영 및 유지 보수 비용
- 보안 정책 변경 (Public IP / 서비스 Port / 접근 제어 등)
- 추가적인 사용자 인증 (대외 접속 인력)

전용 장비 / 라이선스 / S/W 설치 / 보안정책 변경 등이 필요함

기존 서비스 방식의 어려움

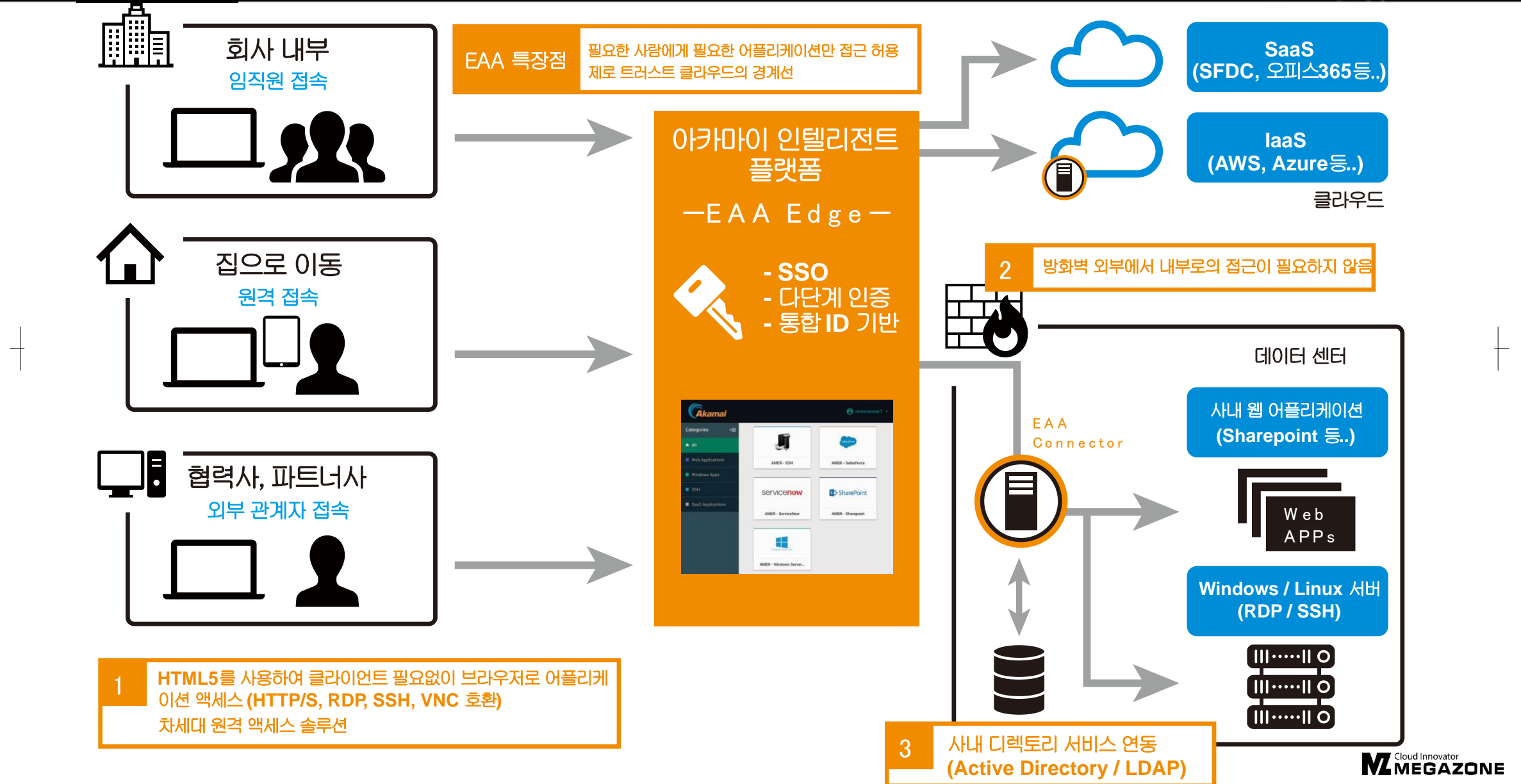
기 운영중인 환경에 대한 변경이 필수적

- 사용자 및 애플리케이션 사이징
- 장애 대비 추가 장비 및 네트워크 구성
- 물리적 장비의 설치
- 네트워크 구성 변경 및 설치
- 다양한 인증 방식지원을 위한 추가 구성
- 보안 설정 및 네트워크 변경이 필요
- 정책 관리 및 데이터 관리 필요
- 서비스에 따라 별도의 S/W 설치 필요
- 기타



구성 및 운영 소요기간 : 수 주일에서 수 개월

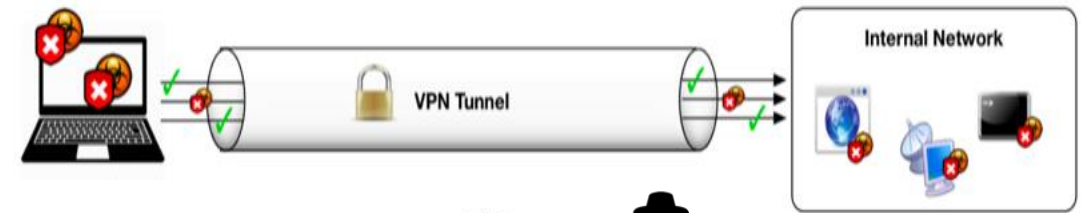
EAA(Enterprise Application Access)



기존 VPN 기반 방식과의 차이점

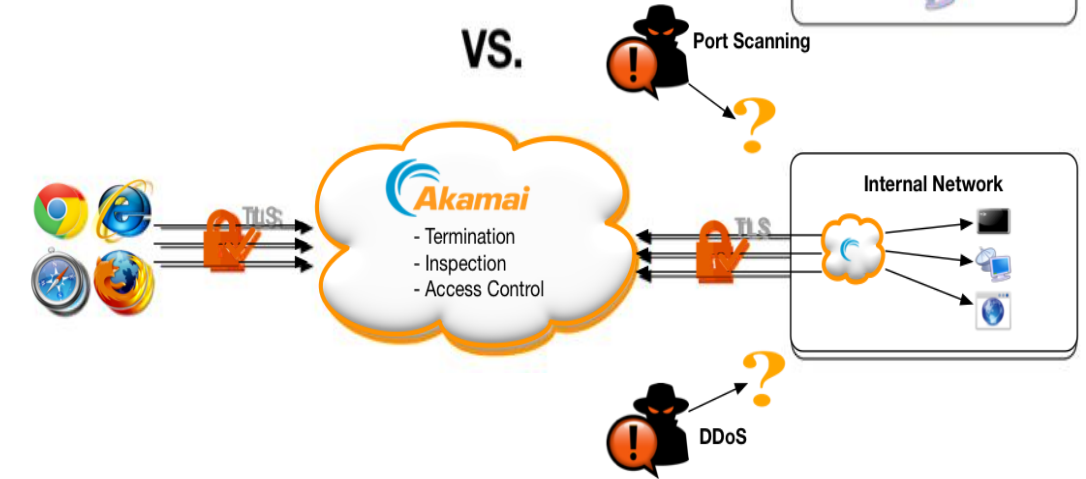
기존의 VPN Tunnel 구조

- VPN 접속을 위한 별도 장비 및 보안 정책 추가 설정 필요
- VPN tunnel 접속 후 모든 내부 네트워크에 대한 접근 가능
- 유해 트래픽에 감염된 End User로 인한 내부 네트워크 위협 증가
- 외부에 공개된 IP 및 서비스 Port로 각종 공격의 대상이 됨

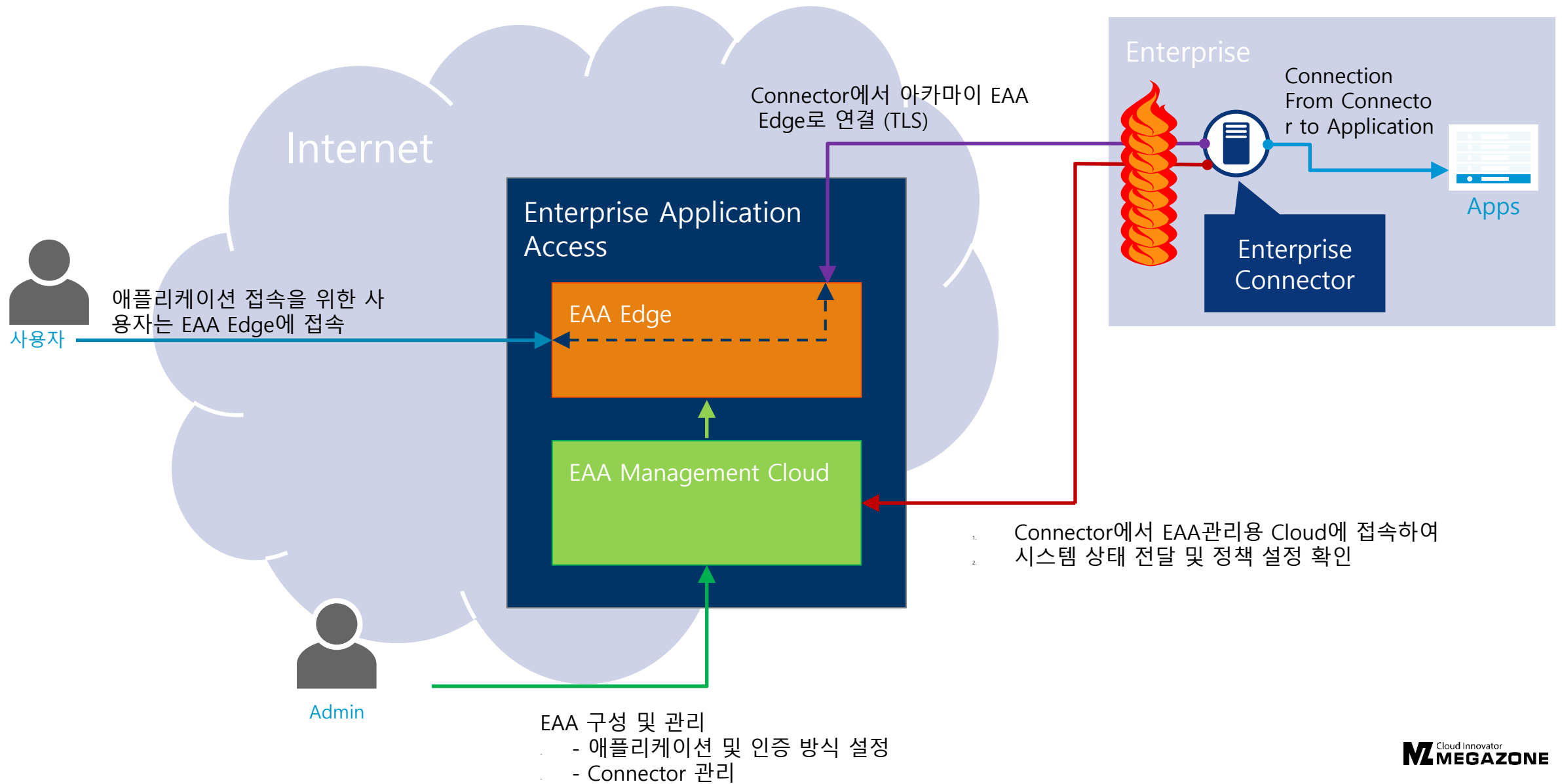


EAA 서비스 구조

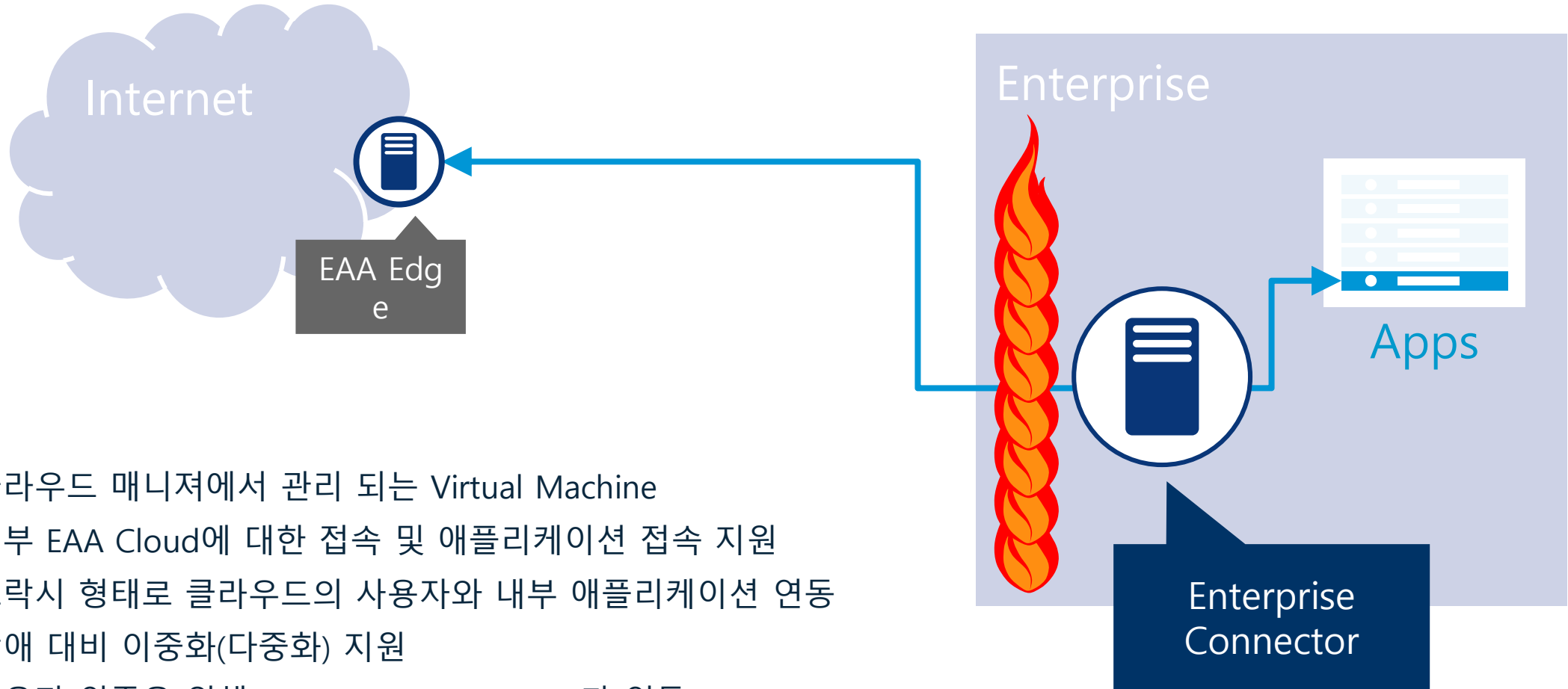
- 내부에 설치된 VM에 Proxy 로 동작하는 S/W 만을 탑재, 전용 장비의 구매 및 보안정책 추가 설정 불필요
- End User에 허용된 APP 에만 접속을 허용, 보안 위협 최소화
- Browser 를 통한 HTTP/S 만을 사용함으로 End User로 인한 보안 위협이 내부 서비스에 전파 되는 것을 방지
- 외부로 공개된 서비스 Port 가 없음으로 각종 공격의 대상에서 제외됨



구성방식



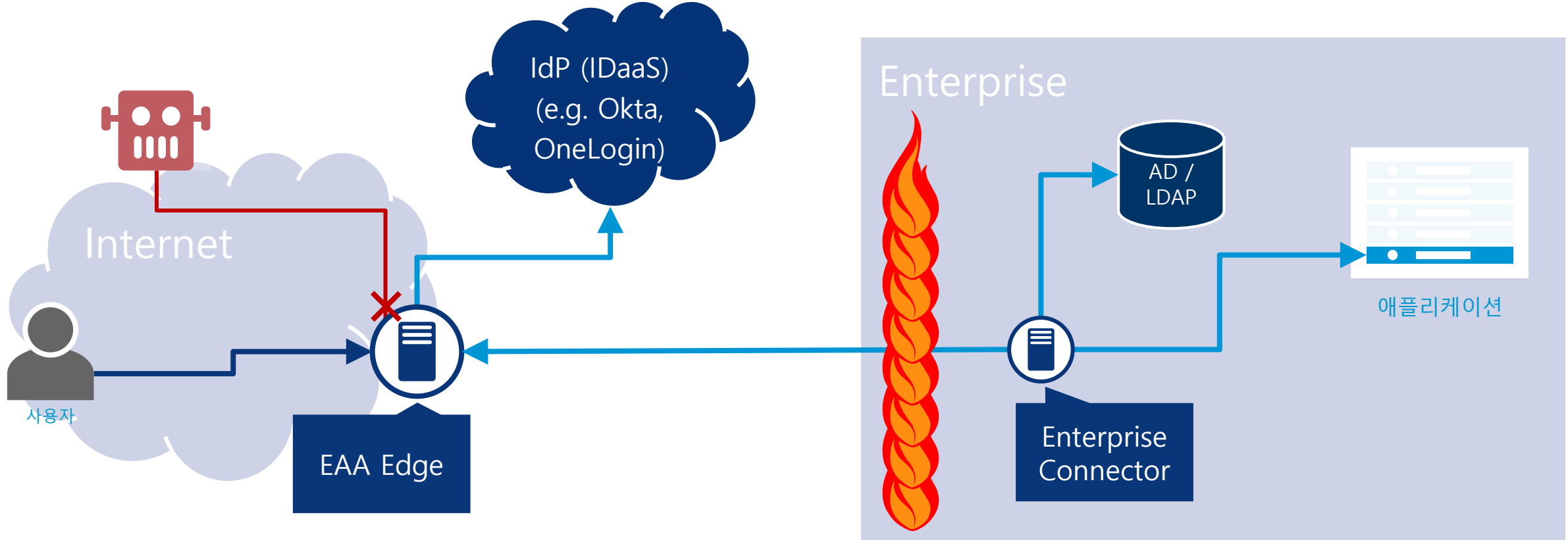
Enterprise Connector의 역할



- 클라우드 매니저에서 관리 되는 Virtual Machine
- 외부 EAA Cloud에 대한 접속 및 애플리케이션 접속 지원
- 프락시 형태로 클라우드의 사용자와 내부 애플리케이션 연동
- 장애 대비 이중화(다중화) 지원
- 사용자 인증을 위해 Active Directory/LDAP과 연동
- 다양한 ADC 기능 지원 (load balancing, custom headers, path based routing, and authentication bridging 등)

사용자 인증 및 권한관리

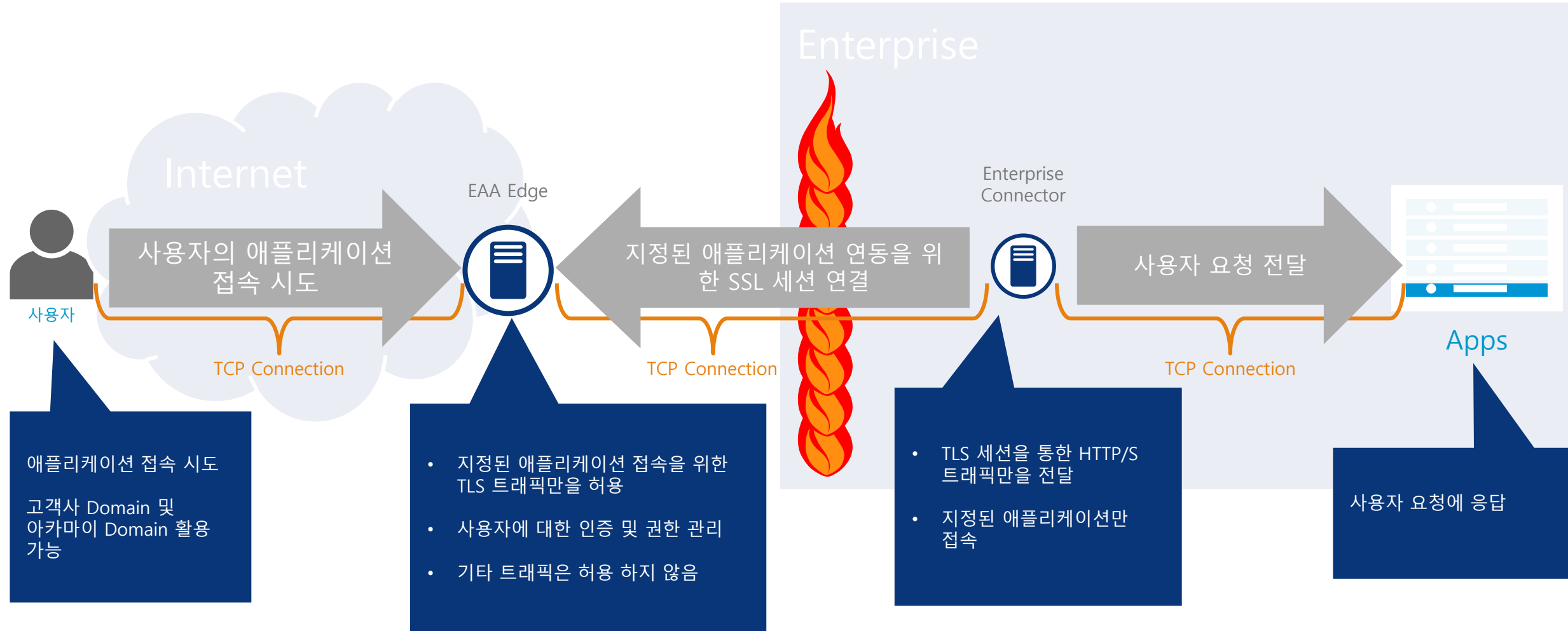
인증 및 권한관리 간편화 - 기존 운영 중인 인증 구조 활용 가능



- EAA Edge 에서 사용자 인증 will authenticate the user
- 싱글사인온 기능 지원
- 다중 인증 방식 지원 및 다양한 인증 지원
 - SAML 2.0 Identity providers (IdP) 지원
 - NTLM, Kerberos, SAML, Header based Auth

다양한 인증 방식 지원 가능

트래픽 플로우



지원 서비스 세부 내용

애플리케이션

- HTTP/S Enterprise Web Apps, such as
 - SharePoint
 - Jira
 - Jenkins
 - Oracle - JD Edwards
 - Oracle - Business Intelligence
 - Oracle - ERP
 - SAP - Inbox
 - SAP - Business Intelligence
- SSH, VNC
- Remote Desktop Access

애플리케이션 위치

- On-Premise (Datacenter)
- Cloud Providers, such as AWS, Google Cloud, Microsoft Azure, Rackspace

다양한 인증 지원

- Enterprise Active Directory
 - NTLM v1 & v2 / Kerberos
- SAML
 - Okta, Ping, OneLogin, other SAML 2.0 IdPs
- Custom HTTP Headers
- Basic and Forms-based Auth
- 2 Factor Authentication (Email, SMS, TOTP)

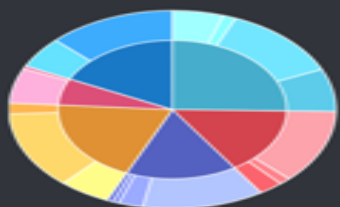
Connector 설치환경

- VMware
- Microsoft Hyper-V
- Amazon AWS EC2/VPC
- Microsoft Azure
- Google GCE
- IBM SoftLayer
- Openstack or KVM
- VirtualBox
- Docker Container



30 days ▾

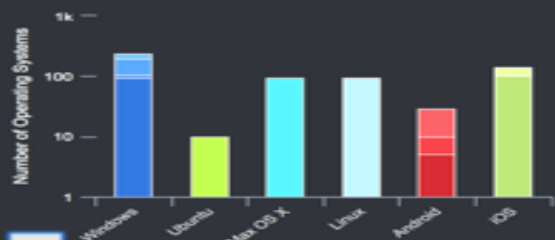
Refresh



● Chrome 200
● Firefox 123
● Safari 124
● Internet ... 154
● Edge 49
● Opera 140

Last

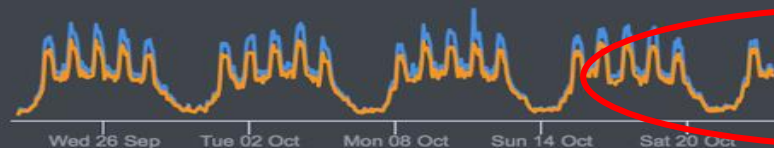
OPERATING SYSTEMS



USER LOCATIONS



ACTIVITY



Active sessions

46077

Unique users

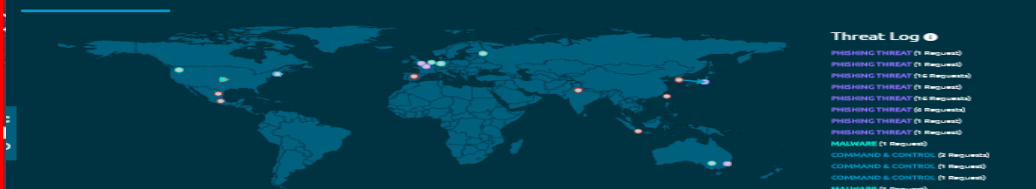
6575

TOP APPLICATIONS

incidents.akam.ai	49.47%
zulip.akam.ai	15.49%
collaborate.akamai.com	10.82%
aoalogin.akamai.com	5.19%
akamaiocsp.akamai.com	3.37%

340+ Applications
6500+ Users

ENTERPRISE THREAT MONITOR



Threat Log

PHISHING THREAT (1 Request)
PHISHING THREAT (1 Request)
PHISHING THREAT (1 Request)
PHISHING THREAT (1 Request)
PHISHING THREAT (1 Request)
PHISHING THREAT (1 Request)
MALWARE (1 Request)
COMMAND & CONTROL (1 Request)
COMMAND & CONTROL (1 Request)
COMMAND & CONTROL (1 Request)

Threat Breakdown - Last Hour



Threat Trends



Breakdown by Threat Type

Average Threats Per Hour Trends



7 days ago ▶

Access Map

Recent Activity

Bandwidth Usage

Date

Application Name

Browser

Username

OS

IP

Location

Dec 7th 2016, 15:47 (PST)

ion-sandbox-sp.projectwikiwiki.com

other

anon-user

other

165.254.48.163

New York,US

Dec 7th 2016, 15:55 (PST)

ion-sandbox-sp.projectwikiwiki.com

other

anon-user

other

67.131.44.157

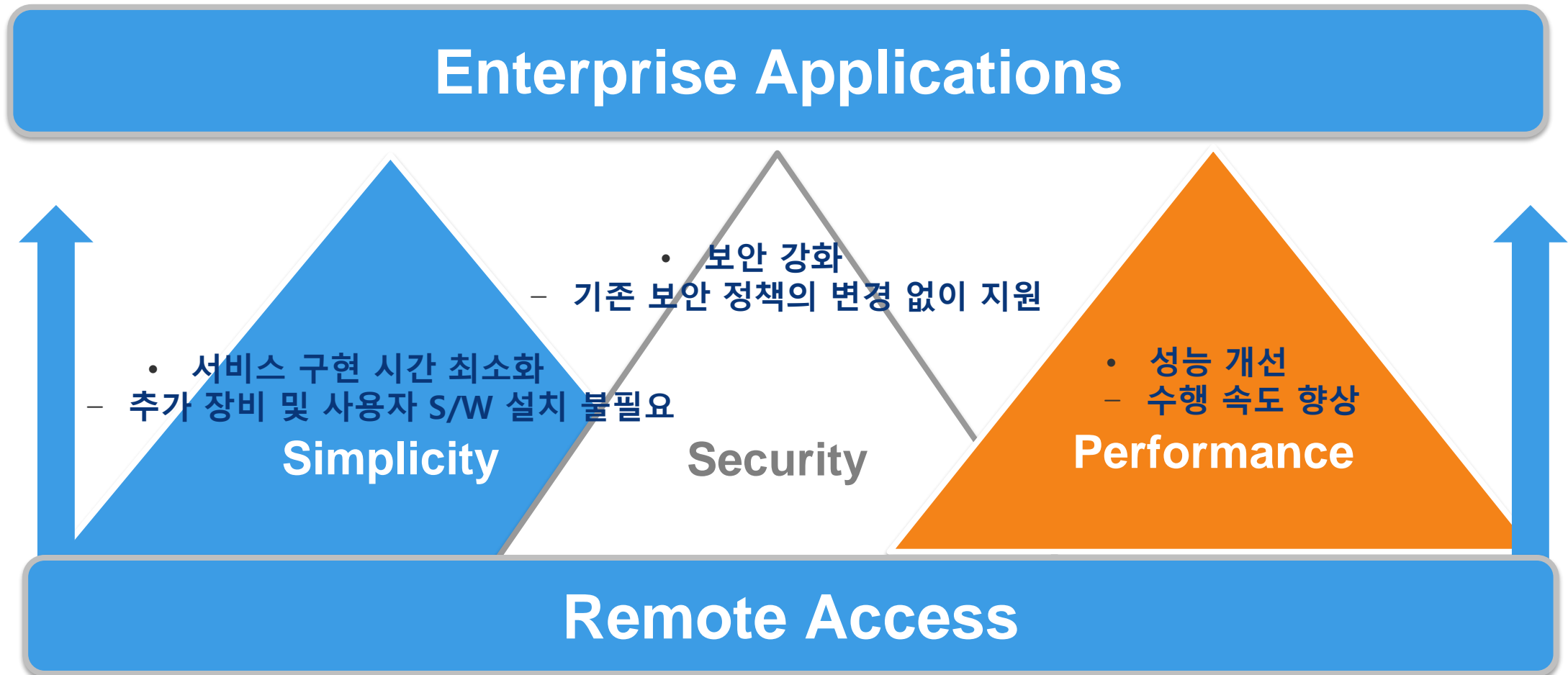
undefined,US

Wednesday, December 7th 2016, 4:28 pm

67.131.44.156 ion-sandbox-sp.projectwikiwiki.com partner GET text/html 200 ion-sandbox-sp.projectwikiwiki.com/Lists/Team%20Discussion/AllItems.aspx windows-7 windows-7-desktop gomeza

Wednesday, December 7th 2016, 4:28 pm

67.131.44.156 ion-sandbox-sp.projectwikiwiki.com partner GET text/html 200 ion-sandbox-sp.projectwikiwiki.com/Lists/Team%20Discussion/AllItems.aspx windows-7 windows-7-desktop gomeza



- 다양한 인증 지원: AD, LDAP, Cloud Directory 등 다양한 인증 활용 가능

EAA 고객 사례 – 항공사

1. 고객 이슈

- 세계적인 규모의 항공사는 제한 된 인원으로 구성된 개발팀에게 애플리케이션 접속 권한을 부여

2. 요구 사항

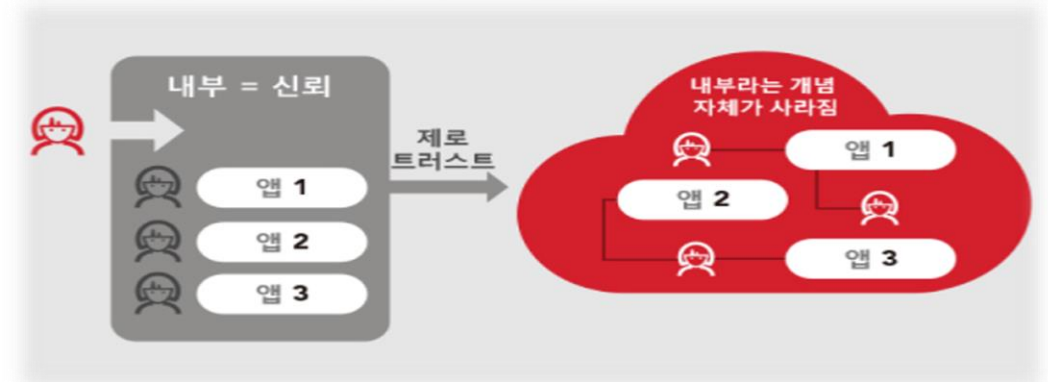
- 내부 개발자와 외부 개발자가 엔터프라이즈 애플리케이션에 접속할 수 있어야 함
- AWS 및 점프 서버 SSH 접속이 호환되어야 함

3. 솔루션 도입 과정

- 솔루션 도입 과정 며칠 안에 구축이 완료되었고 IT 팀에서는 2달 동안 Enterprise Application Access에 대한 테스트와 평가에 전념할 수 있었습니다.
- 기존 솔루션 단점 : 사용자 친화적인 인터페이스를 제공하지 않으며 전문가급 지식 필요, DMZ 기능이 존재하기 때문에 기존의 시스템에서 애플리케이션에 대한 접속 권한을 설정의 어려움.
- EAA 장점 : 클라우드 환경을 오픈할 필요가 없고 DMZ 인프라도 필요하지 않아 애플리케이션 컨텍스트 라우팅 기능을 포함한 애플리케이션을 몇 분 안에 퍼블리싱 가능

4. 결과

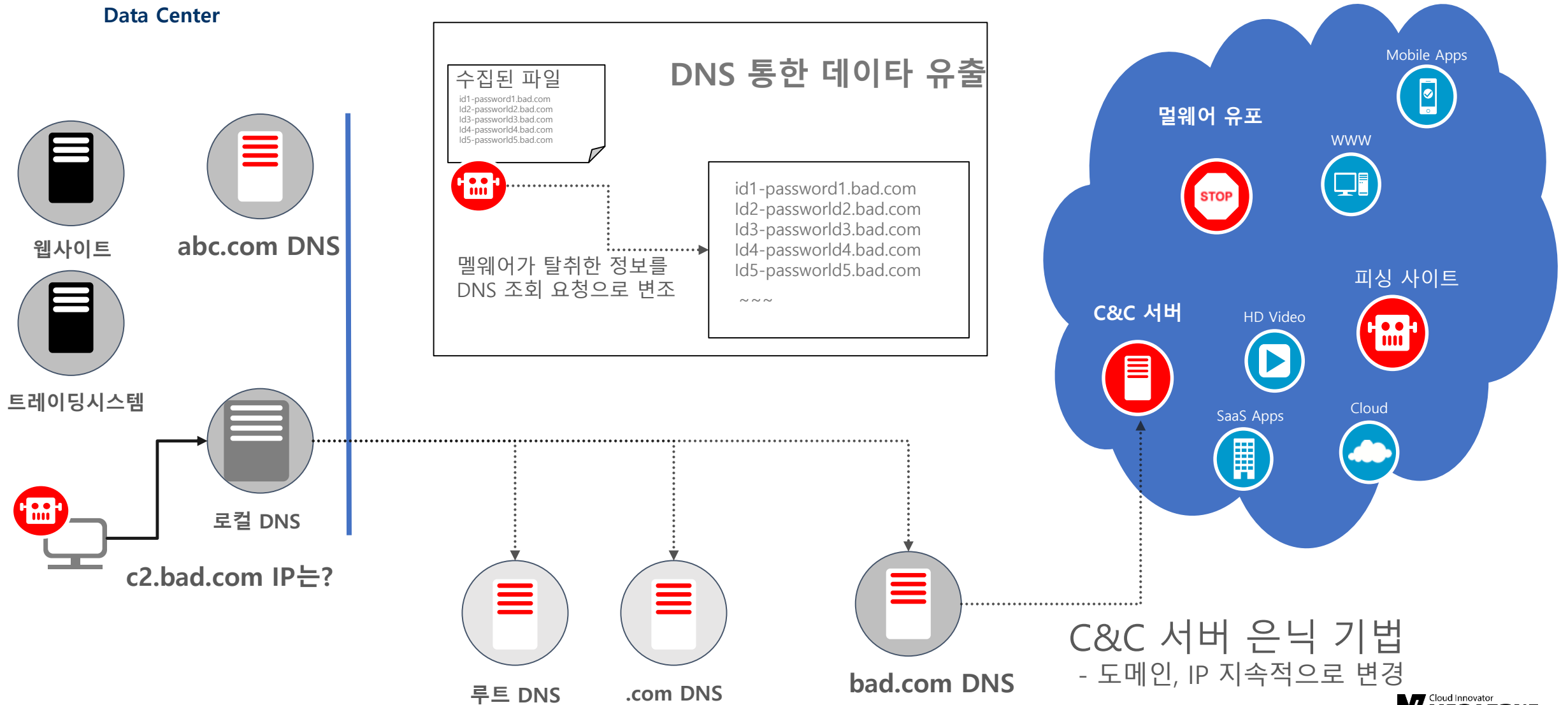
- 보안 개선 : Akamai 클라우드에 있는 사용자들을 검증한 뒤 애플리케이션 접속 권한 부여
- 민첩성 개선 : 단순화된 아키텍처를 통해 며칠이 걸리던 애플리케이션 퍼블리싱을 몇 분 단축, 동시에 기존의 ADFS 시스템과 통합을 유지하면서 네트워크 구성 요소에 복잡한 변화를 주지 않음.
- 가시성 보완 : EAA는 모든 접속 활동을 기록하며 유리창과 같은 투명성을 보장.



Enterprise Threat Protector

(멀웨어에 대한 선제적 대응)

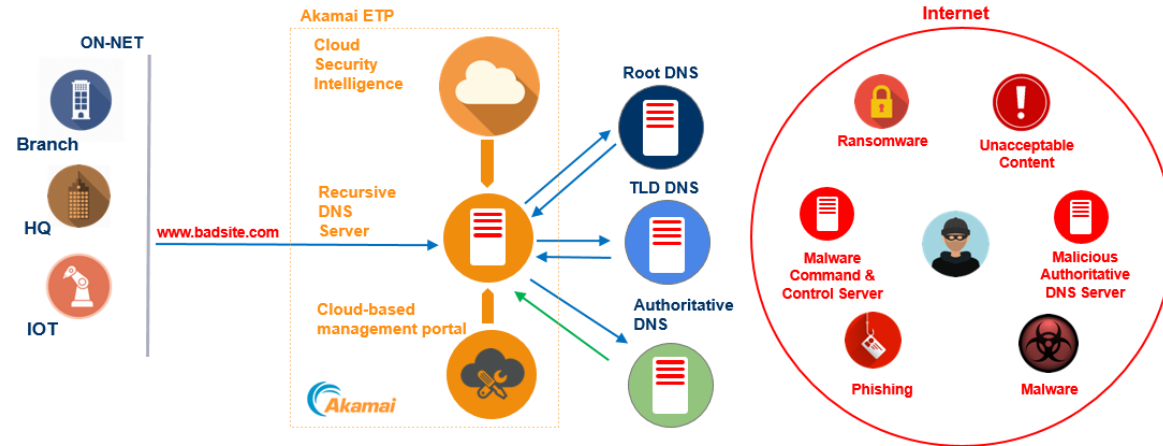
모든 요청은 DNS 질의로 시작 - 멀웨어도 DNS 사용



Malware와 Ransomware의 92%가 DNS를 이용해 C&C 서버와 통신 시도

아카마이 ETP(Enterprise Threat Protector) 개요

DNS 를
보안의
한계층으로
활용



아카마이 보안 정보

전체 웹트래픽의 30% 처리
1500억건의 DNS 쿼리 처리

3rd 파티 정보

Raw threat data
Premium threat

PUBLIC 보안 정보

WHOIS data
Registrar data

수집된 데이터의 자동화된 통계,
추세 및 패턴 분석



아카마이 데이터 엔지니어링
팀에서 실행 가능한 위협 정보를
위해 데이터를 검토, 정리 및
검색 합니다.

실시간, 빅데이터 기반의
클라우드 보안 인텔리전스

Machine Learning과
Human 다층 분석

기업 트래픽 및 소비자
트래픽에 의해 공격 패턴
정보 수집

3rd 파티 및 고객이 직접
입력한 공격 패턴으로 보강

ETP 특징

DNS를 활용해 내부 보안 강화

- 내부 사용자의 멀웨어, 랜섬웨어, 피싱사이트 접근을 사전에 차단
- DNS 쿼리로 위장한 내부 기밀 데이터 유출 차단
- 비 업무 사이트 접속 통제 및 모니터링 제공

인프라 추가 없이 솔루션 도입 가능

- 내부 DNS 설정 변경만으로 편리하게 도입
- 클라우드 기반으로 별도의 장비 도입 없음
- 인프라 환경 변경 불필요

손쉬운 관리

- 아카마이 빅데이터 기반 자동화 된 보안 데이터 제공
- 직관적이고 편리한 웹 UI 제공
- 수분내 보안 정책 변경 및 적용 가능

DGA (Domain Generation Algorithm)

C&C 서버를 숨기기 위해 사용되는 도메인 생성 기법 입니다.

- 도메인 기반 방화벽에 탐지를 회피 하기 위해 사용합니다.
- 미리 설정된 알고리즘 및 salt를 기반으로 도메인을 끊임 없이 생성 합니다.
- 사람이 봤을 때 한번에 파악 가능 하지만 장비는 쉽게 찾아내지 못합니다.

아카마이 ETP 대응

- 행위 기반 비정상 도메인 탐지 기법 사용
- 단기간에 생성 되고 소멸되는 도메인 탐지
- 다수의 NxDomain 에 대한 DNS Query 탐지
- 도메인 이름의 어휘 분석

Compromised System



HASH

Seed

+

Date

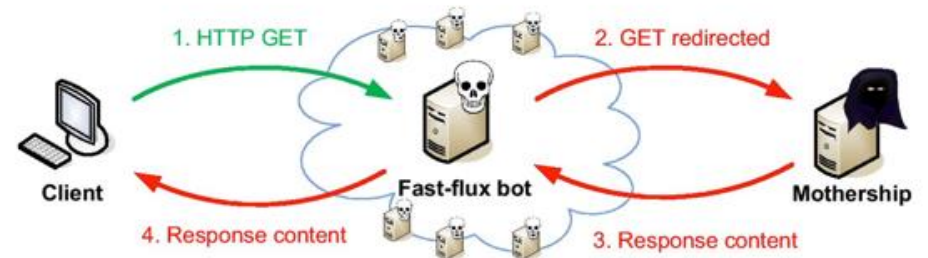
Recursive DNS

DOMAIN	TOTAL
All Filtered Domains	
p7Z2hxpq2UndT23gwa7H5b0eqbaeq.a.e.e5.sk	5
feqfwebcorgu7p6fq33xvinyb0eqbaeq.a.e.e5.sk	5
mkekshov5urasmrmpmxomb0eqbaeq.a.e.e5.sk	5
ThQ2qfweyuhU23f3oeuh0eqbaeq.a.e.e5.sk	5
c3h2qhpocpuguz7jaryx4b0eqbaeq.a.e.e5.sk	5
uap7pahp2vau7fpekyf4b0eqbaeq.a.e.e5.sk	5
7eryverfside3pnykmmmb0eqbaeq.a.e.e5.sk	5
Q2eh9iugpubqee4odt3pmb0eqbaeq.a.e.e5.sk	5
.rhooaacakaaaaah7777b0aqaaw263qafp3z4egyahdof53aaabup.fg5aaataaiaa447mwd54evbzryeha2qa3byfddqymkgbq3	3
piduacaaakaaaaah7777b0aqaaw263qafp3z4enbahdpof53aaaboe.ne4aaataaiaa447mwd54evbzryeha2qa3byfddqymkgbq3	3
cufuacaaakaaaaah7777b0aqaaw263qafp3z44elyah777723aaabof.wfdaaaataaiaa447mwd54evbzryeha2qa3byfddqymkgbq3	3
juruaacaaakaaaaah7777b0aqaaw263qafp3z4egyahdof53aaabof.wfdaaaataaiaa447mwd54evbzryeha2qa3byfddqymkgbq3	3
impuacaaakaaaaah7777b0aqaaw263qafp3z44elyah77773aaabp.7aypcaaaafqbyymbzafq6b77yyskdu44pnt05427y.a.j.e5.sk	3
fdouacaaakaaaaah7777b0aqaaw263qafp3z4enbahdpof53aaabof.wfdaaaataaiaa447mwd54evbzryeha2qa3byfddqymkgbq3	3
dnduacaaakaaaaah7777b0aqaaw263qafp3z44elyah77773aaabf5.hwqcaaaafq4mcv773pwn7jv77h0pva9qijc7y.a.j.e5.sk	3
d7puaacaaakaaaaah7777b0aqaaw263qafp3z4egyahdof53aaabof.wfdaaaataaiaa447mwd54evbzryeha2qa3byfddqymkgbq3	3
7puaacaaakaaaaah7777b0aqaaw263qafp3z44elyah77773aaabf5.6ppcaaaafqbw7776mmes2vlnhgz76d5bkyummm7y.a.j.e5.sk	3
77puaacaaakaaaaah7777b0aqaaw263qafp3z44elyah77773aaabf5.hdfdaaaataaiaa447mwd54evbzryeha2qa3byfddqymkgbq3	3
4cuaacaaakaaaaah7777b0aqaaw263qafp3z44elyah77773aaabf5.svqcaaaafqavesthup3mqftr7mmn2aa2m8qbn7y.a.j.e5.sk	3
4puaacaaakaaaaah7777b0aqaaw263qafp3z44elyah77773aaabf5.7mwcacaaafq428dofm6ruftelgnrshnagaw7y.a.j.e5.sk	3
4hucacaaakaaaaah7777b0aqaaw263qafp3z44elyah77773aaabf5.uz2oc3acaaafq42ocq3ahcwrqj0uep6kdeh7y.a.j.e5.sk	3
3ghuacaaakaaaaah7777b0aqaaw263qafp3z4enbahdpof53aaabup.fg5aaataaiaa447mwd54evbzryeha2qa3byfddqymkgbq3	3
26uacaaakaaaaah7777b0aqaaw263qafp3z44elyah77773aaabue.k2h7acaaafq428dofm6ruftelgnrshnagaw7y.a.j.e5.sk	3
yyuacaaakaaaaah7777b0aqaaw263qafp3z44elyah77773aaabof.wfdaaaataaiaa447mwd54evbzryeha2qa3byfddqymkgbq3	3

Fast Flux Network

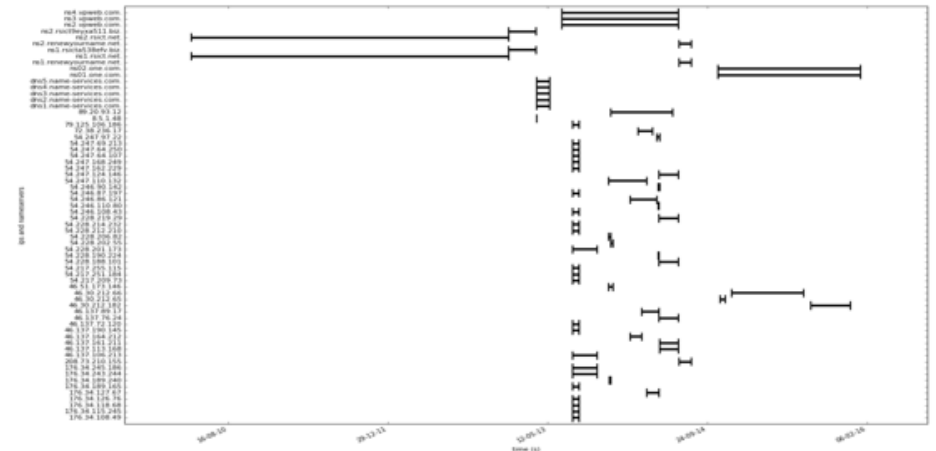
공격자가 Malware C&C 서버 IP를 숨기기 위해 프록시 네트워크를 사용

- IP 기반 방화벽을 회피하기 위해 사용 합니다.
- 탐지를 회피 하기 위해 Proxy IP 가 계속 변경 되며 이를 반영 하기 위해 짧은 TTL 값을 가지게 됩니다.
- 짧은 TTL 값을 가지는 도메인을 무조건 차단하면 CDN, IaaS 및 DNS 서비스에 문제가 발생 할 수 있습니다.



아카마이 ETP 대응

- 공격에 사용된 이력이 있는 IP와 도메인을 추적 관리
- 예전에 공격이 발생한 이력이 있는 IP를 도메인에 할당한 내역을 추적 관리



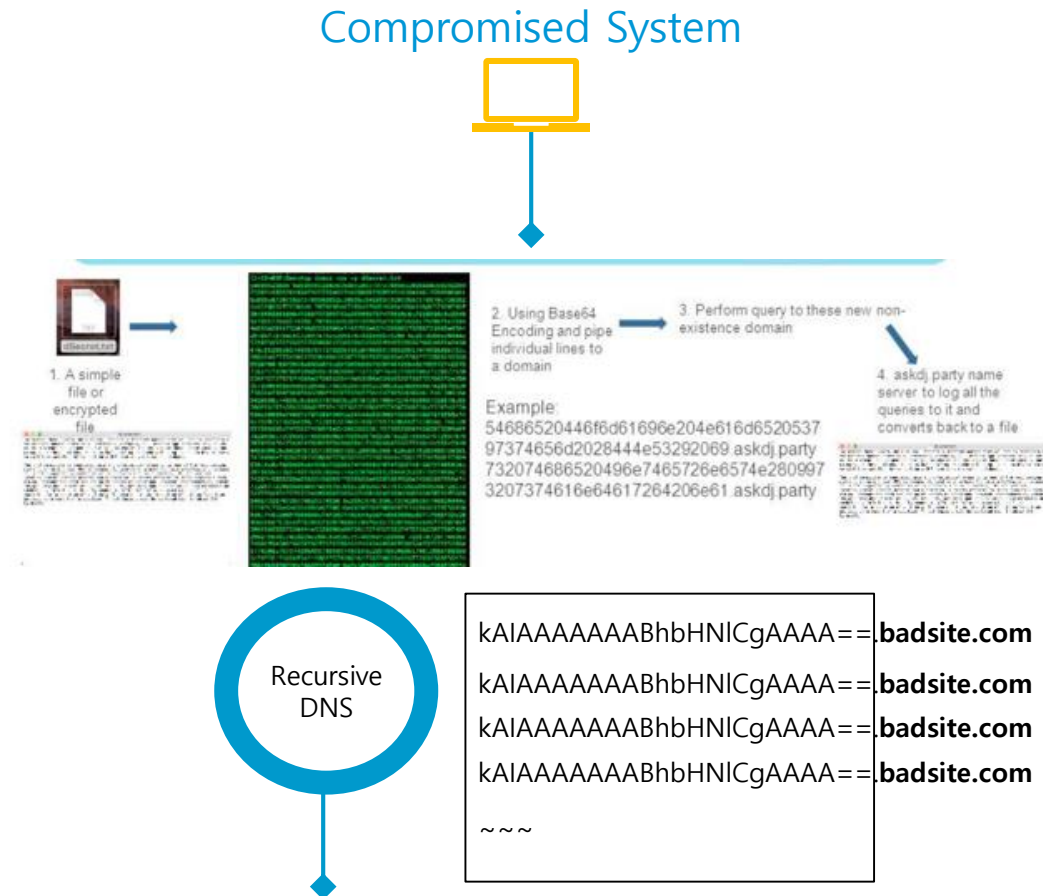
DNS Query를 이용한 데이터 유출

공격자가 감염된 PC의 데이터를 유출하기 위해 DNS Query를 이용하는 기법

- DNS Query 에 암호화 된 데이터를 Hostname 처럼 사용 하는 방식
- Query 내용이 C&C 서버로 전달 되면 도메인 부분을 잘라 내고 복호화

아카마이 ETP 대응

- 대상 도메인에 비정상적인 DNS Query 트래픽 탐지
- 하나의 도메인에 다량의 비정상적 서브 도메인 탐지
- DGA 탐지 기법으로 확인 및 차단 가능



Monitoring & Management



ETP 고객 사례 – 교육 사례

1. 고객 이슈

- 캠퍼스 3곳에서 수천 명의 학생과 직원들에게 인터넷 접속을 제공하며 주간, 야간, 온라인 강의
- 교내 네트워크 DNS 인프라에 대한 보안 시스템이 배치되어 있지 않아 여러 위협에 노출
- 대학은 연중무휴 운영되는 고등 교육기관이기 때문에 유지보수 또는 업데이트를 위해 시스템 중단 불가
- 캠퍼스 인터넷에 접속하는 학생, 교수, 직원, 게스트 사용자 수로 인해 고가의 복잡한 물리적 연결이나 기타 클라우드 기반이 아닌 솔루션을 사용하는 것도 불가능

2. 요구 사항

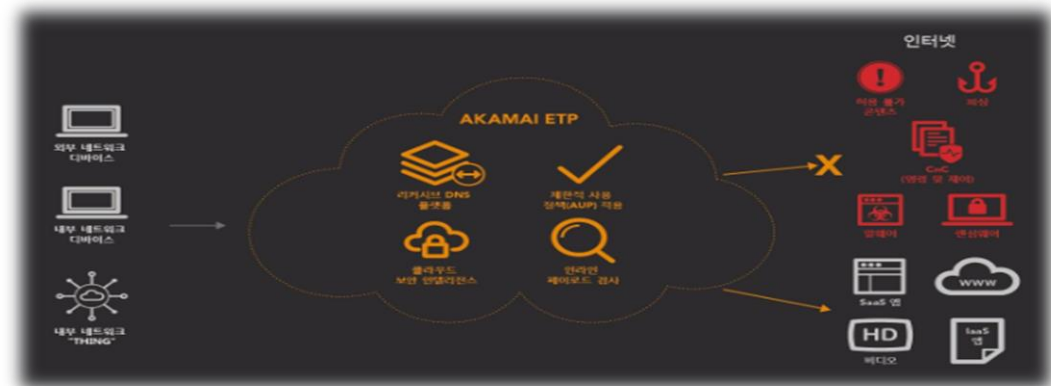
- 대학의 네트워크에 도달하는 멀웨어 및 랜섬웨어 수 감소와 보안 체계 강화
- 관리 시간 최소화
- 복잡성 또는 하드웨어 추가 없이 모든 사용자 보호

3. 솔루션 도입 과정

- 2주간의 POC 기간 동안 PandaBot 멀웨어와 Locky 랜섬웨어를 확인했고 네트워크 상태 보고서 확인
- ETP는 다수의 명령 및 제어와 피싱 시도를 탐지하고 차단했습니다.
- 네트워크 트래픽에 대한 가시성에 만족했고 ETP를 즉각 대학의 보안 스택에 추가하기로 결정

4. 결과

- 대학 전체 네트워크를 멀웨어로부터 방어 및 네트워크 중단 최소화
- 피싱 시도와 명령 및 제어(CnC) 콜아웃 차단



영업 상담 문의

- 담당자 : 신동준 매니저
- Email : sdj@mz.co.kr
- Tel : 010-2551-8418





THANK YOU