제로 트러스트
실제 구현 사례를 통한
클라우드 보안 전략의 재 정의

Yongkhi Paek

Senior Enterprise Security Executive

Enterprise Security APJ

Akamai

Experience the Edge

PASCON 2019

2019 공공기관·기업 개인정보보호&정보보안 컨퍼런스

Public institution·Affiliated organization Information Security Conference 2019

Organizations Are Turning Inside Out

Applications can live anywhere,
users need access from everywhere

...but not everyone should have
access to everything

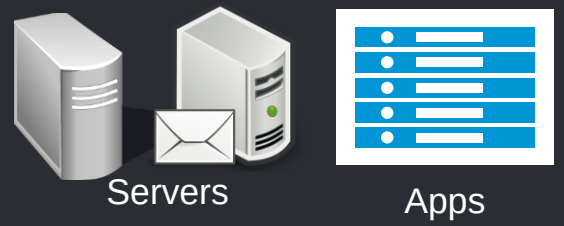
#ZERO TRUST – INDUSTRY TRENDS

- All industry sectors are increasingly vulnerable to cyberthreats
  - Attracting specific focus from phishing and malware authors
  - Real money to be made via Cybercrime
- Complex Supply & Delivery Chain increases risk
  - 56% of large breaches were the direct result of an initial breach into a third-party/supply-chain vendor
- Mitigate Business Risk
  - Protect development schedules to reduce delay in deliverables

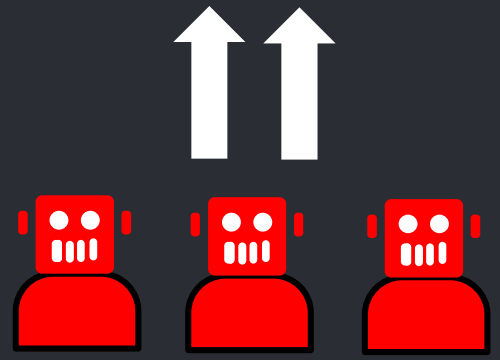
#ZERO TRUST – TYPICAL ECO SYSTEM

- Mobile & Highly Dispersed End Users
- Procurement
  - Internal
  - 3rd Party Services
- Acquisition
  - M&A
- Suppliers
- 3rd Party Developers
- 3rd Party Testers

Users & Apps Are Moving Outside



- Hybrid Cloud Infrastructure
- IaaS & PaaS
- SaaS



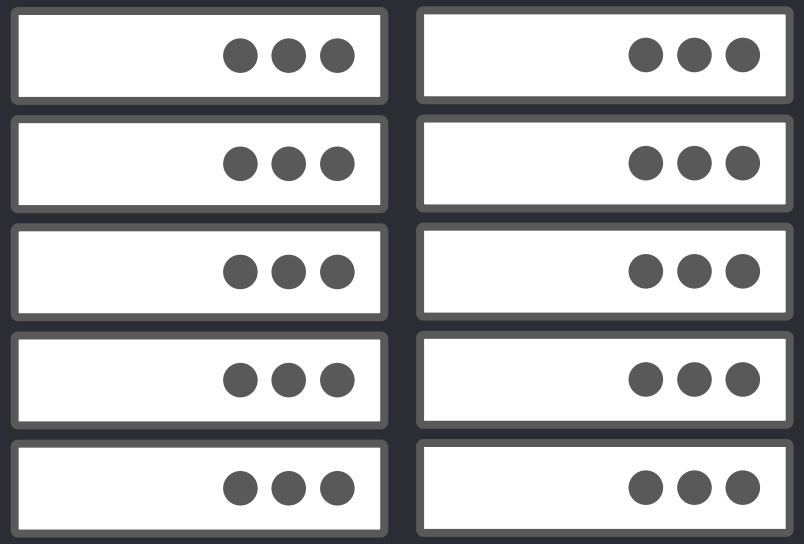
- Security architecture vulnerabilities
- Malware, phishing & data exfiltration
- Credential theft
- Single factor authentication
- Lateral network movement

There is no

INSIDE

Simplify With Edge Security

Virtual/hardware appliances



VS

Security as a service (SECaaS)

Zero Trust is the new approach

Key principles:

- The network is always assumed to be hostile.
- External and internal threats exist on the network at all times.
- Network locality is not sufficient for deciding trust in a network.
- Every device, user, and network flow is authenticated and authorized.
- Policies must be dynamic and calculated from as many sources of data as possible.

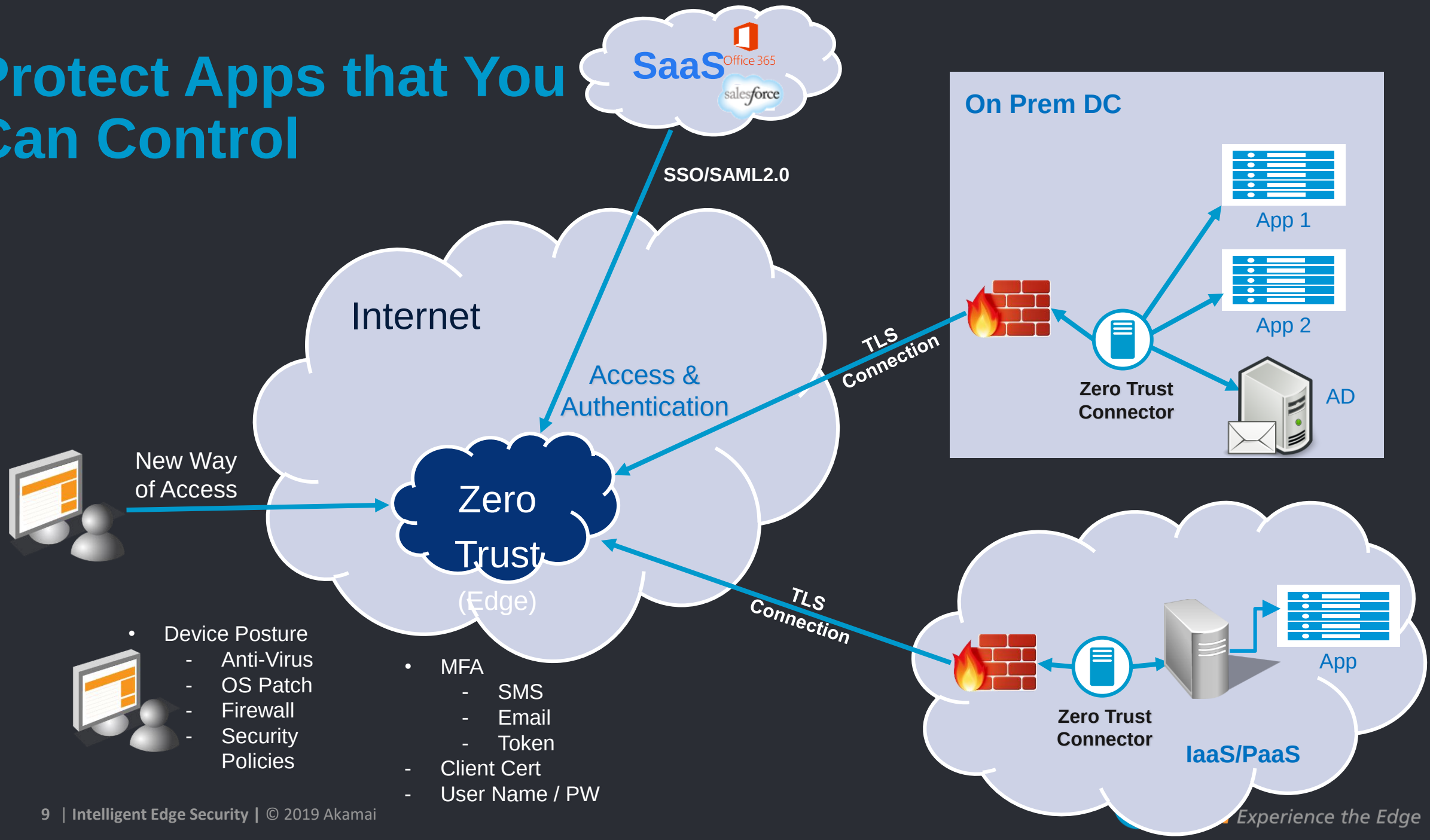
Zero Trust Security Model

Identity Centric Access Control

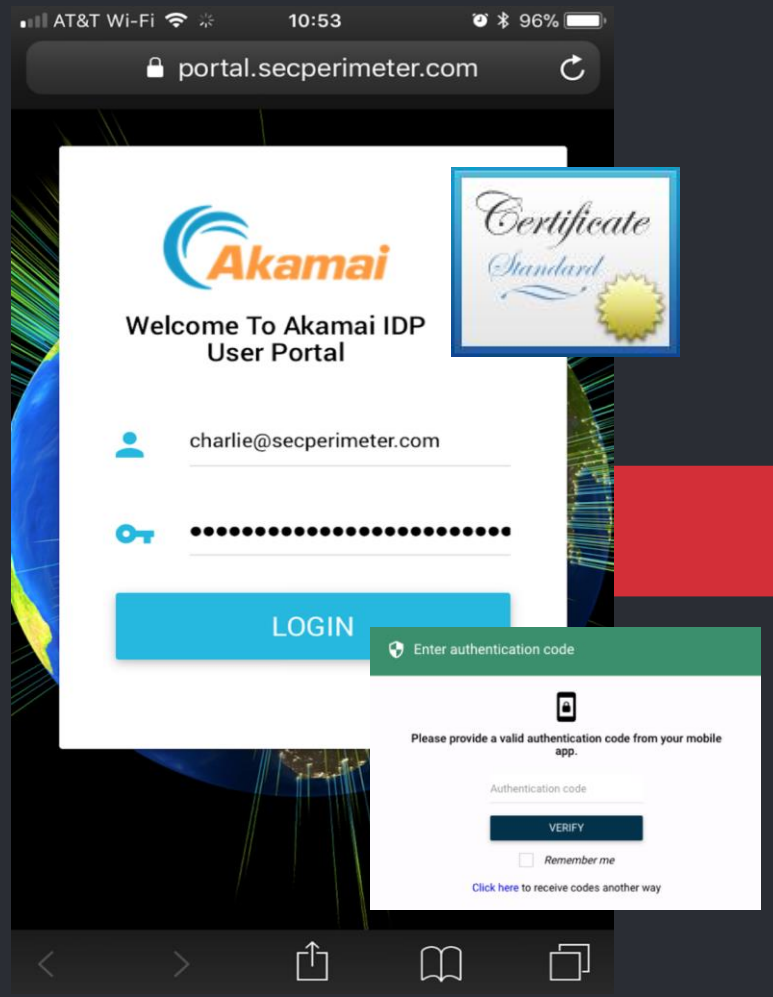
Zero Trust Security Model works on a few simple premise:

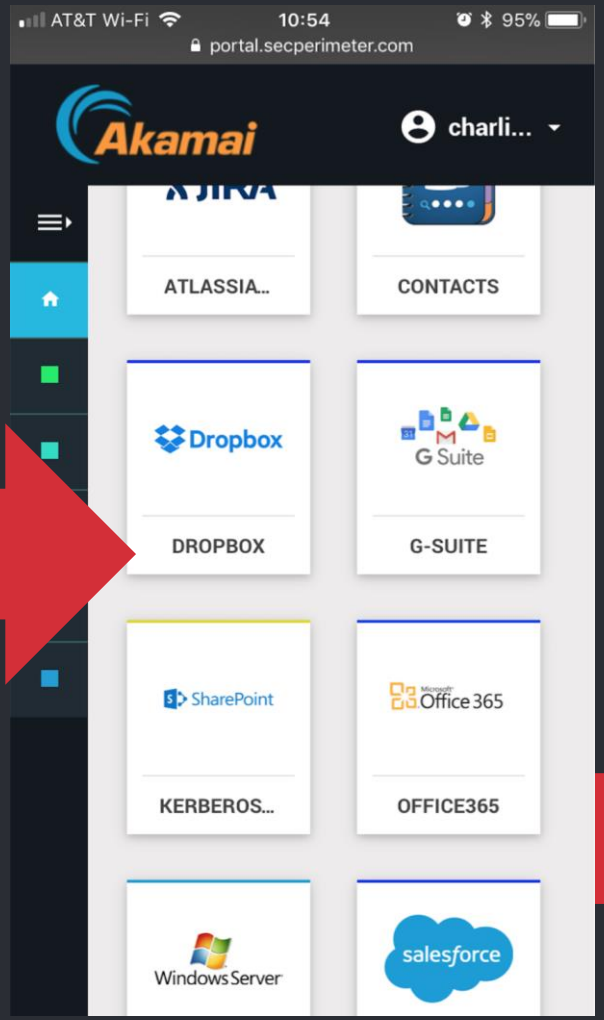
- Move to a least-privilege application access model
  - User identity is the key starting point
  - Authenticate....then authorize
  - Never Trust, ALWAYS Verify
- Protect against targeted threats when users are on or off network
- Improve your end-user experience AND reduce attack surface
  - Better application performance
  - Eliminate VPNs
  - Stop users having to enter passwords
  - 100% Availability SLA

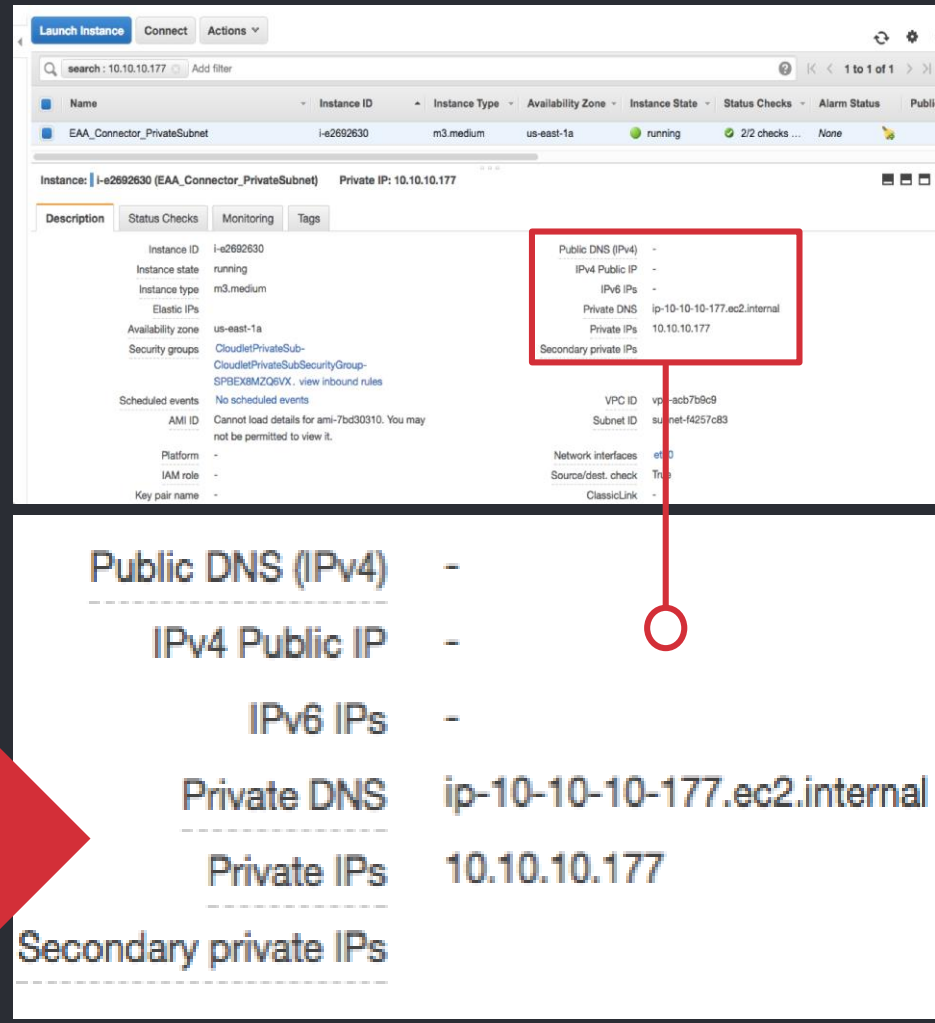
Protect Apps that You Can Control



Isolated From The Internet & Always Verified







Access Protection & Service Insertion

Web Application Firewall

DDoS Mitigation

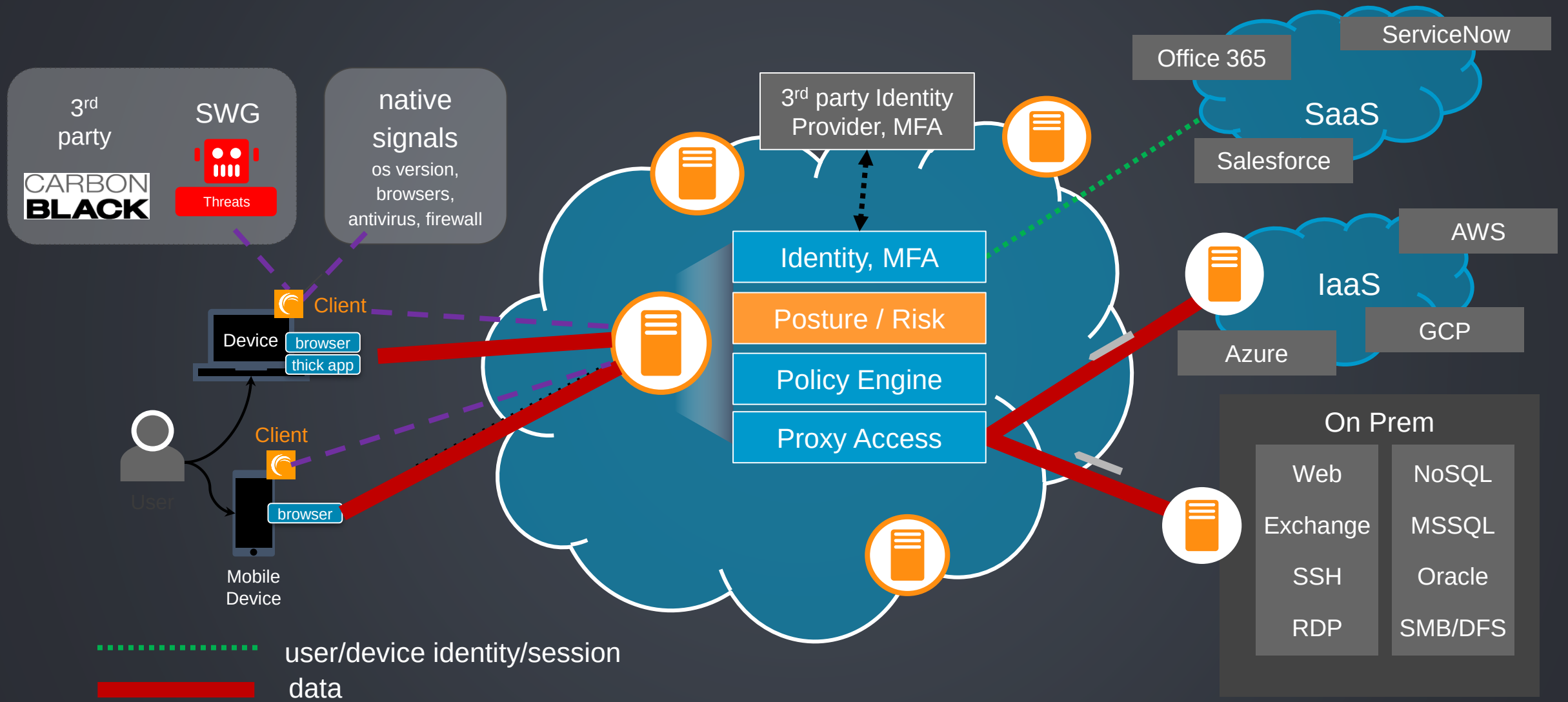
Protect apps & APIs from DDoS, exploits & misuse

Application Acceleration

Global Traffic Management

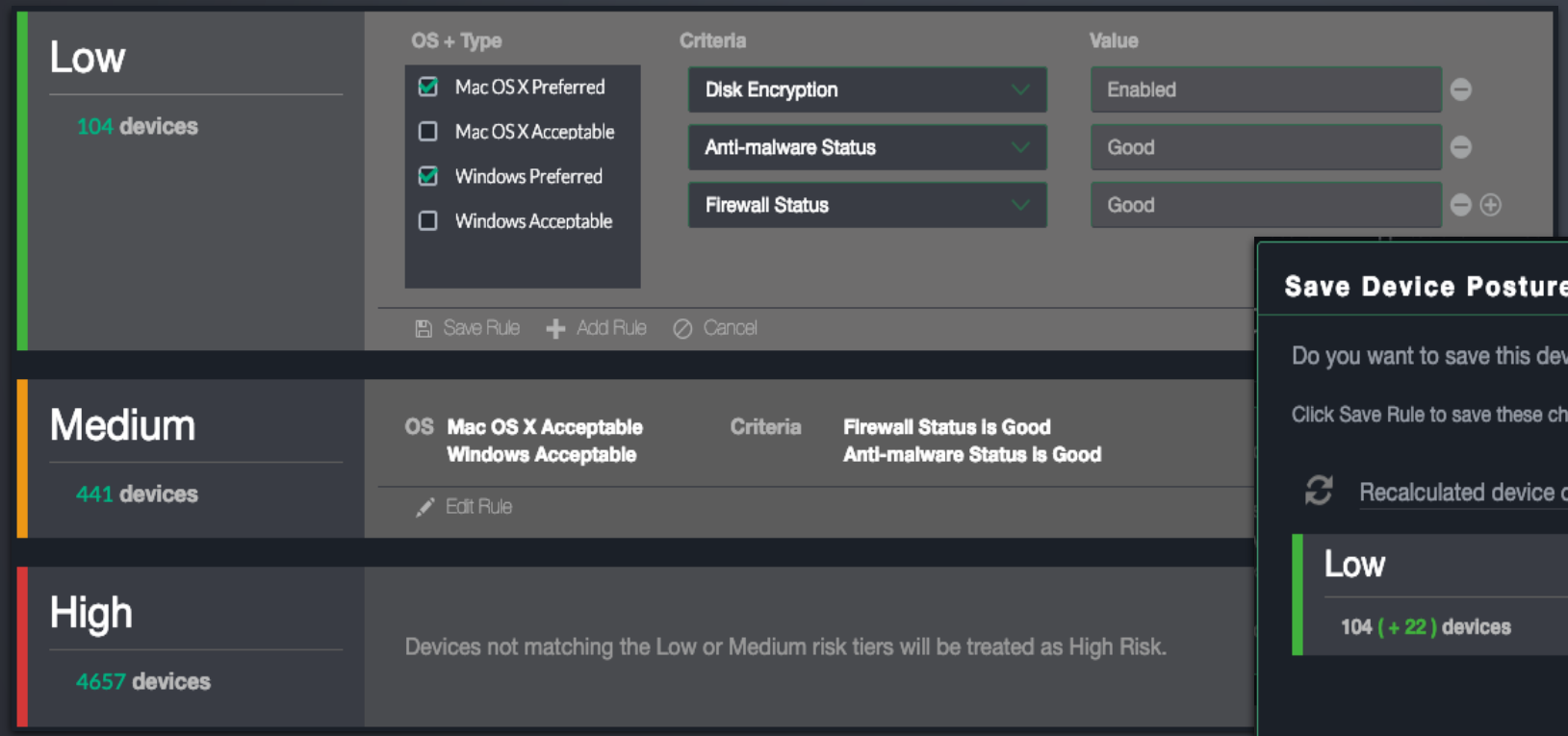
Provide fast & reliable corporate apps to end users

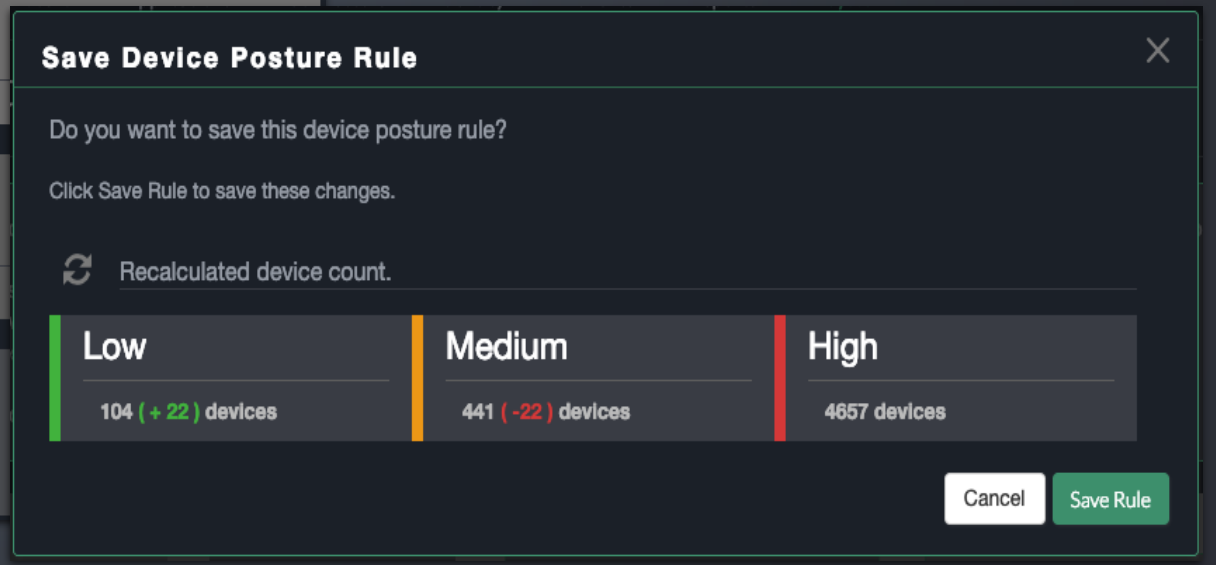
Posture in Enterprise Application Access



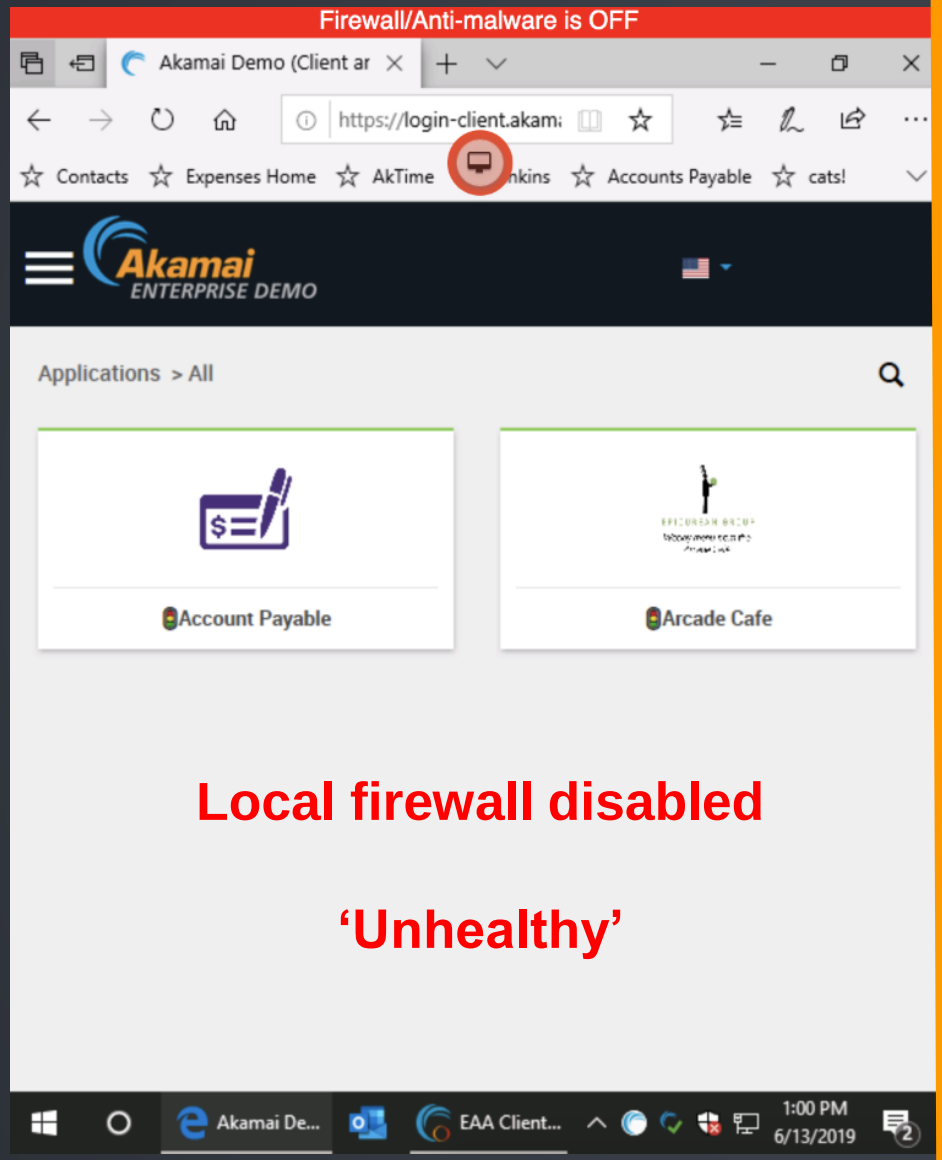
Risk Tiers

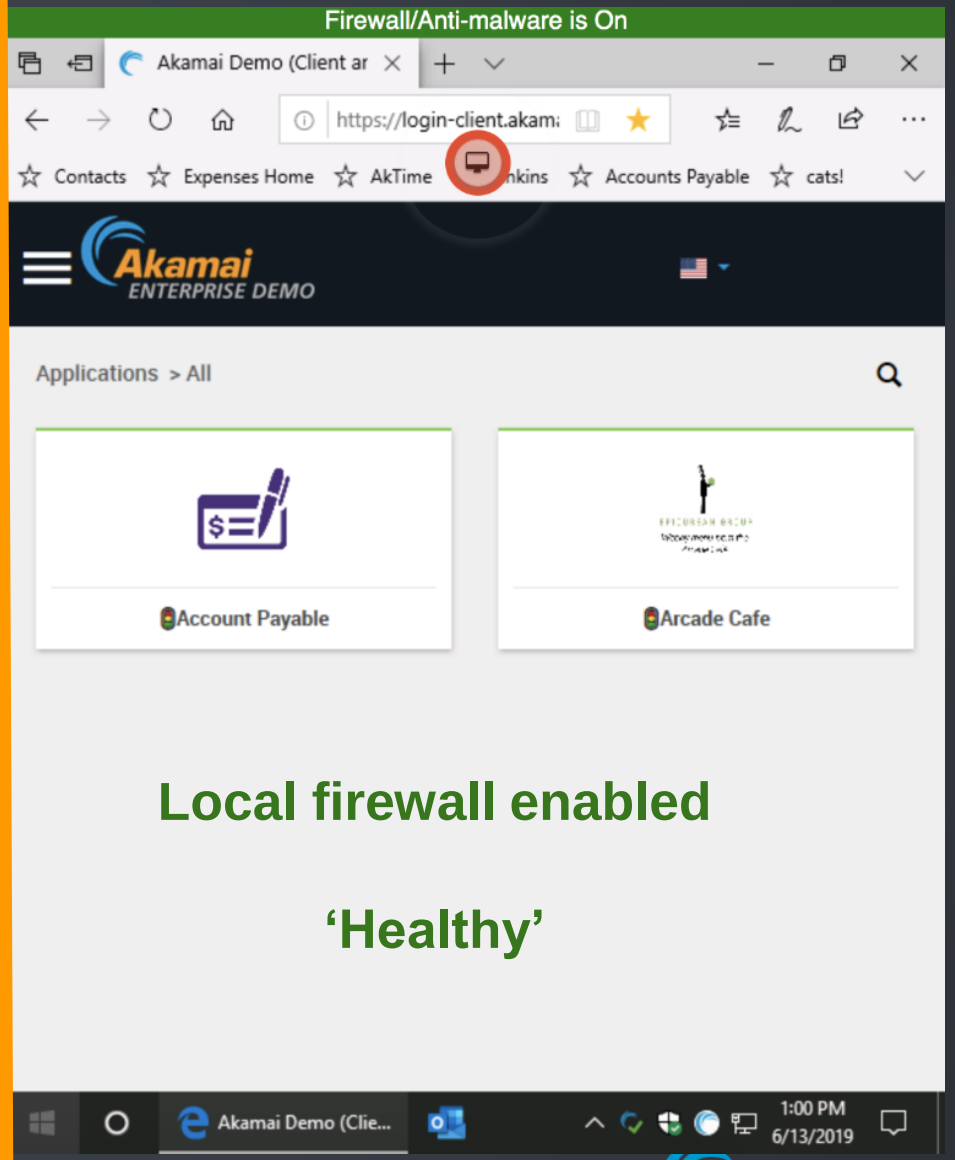
- Low, medium, high risk
  - Hierarchical (if not low, checks med, etc)
  - Select OS and signal criteria
  - Total device count per tier (clickable to display details)



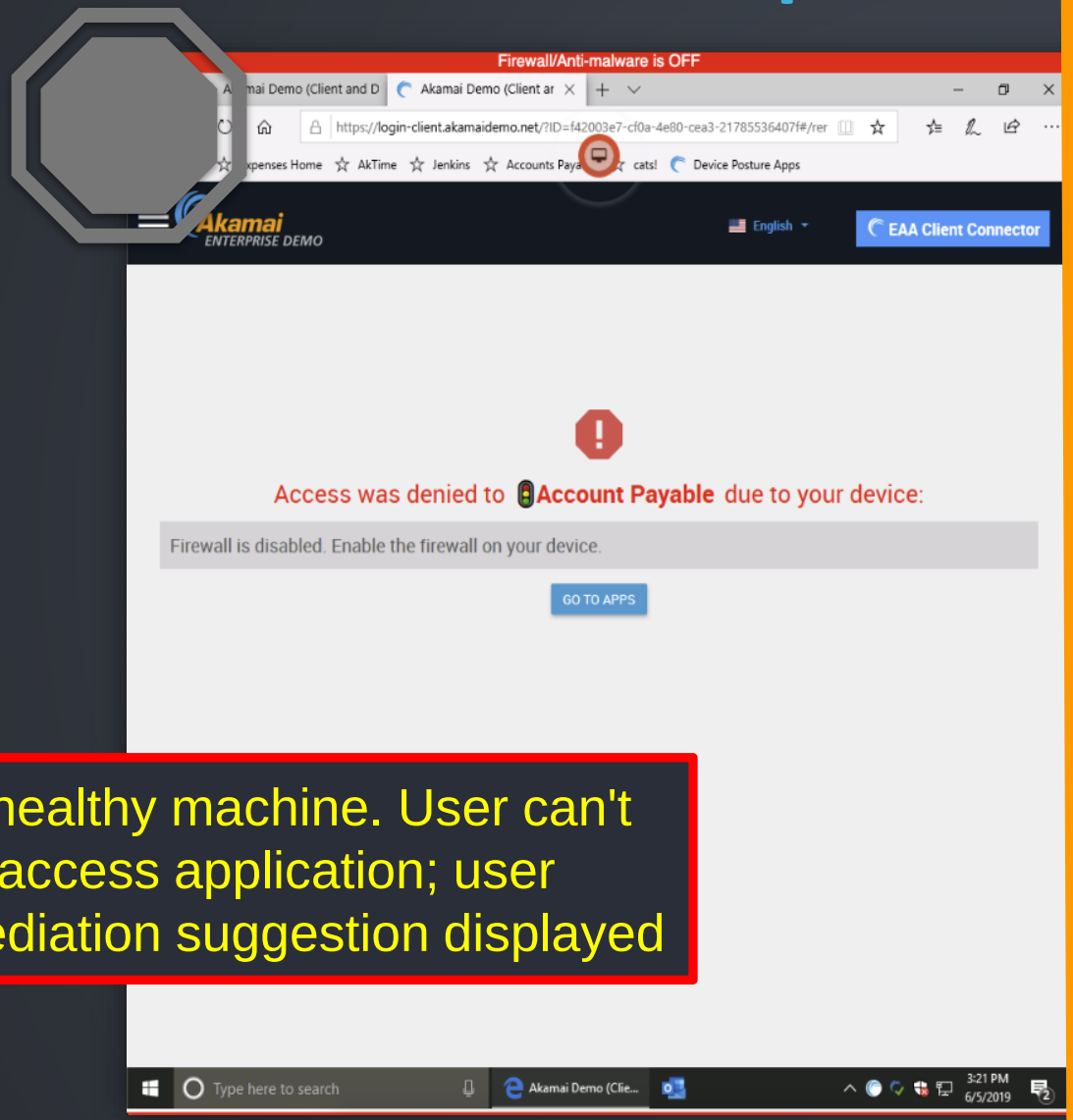


Device Posture - Example

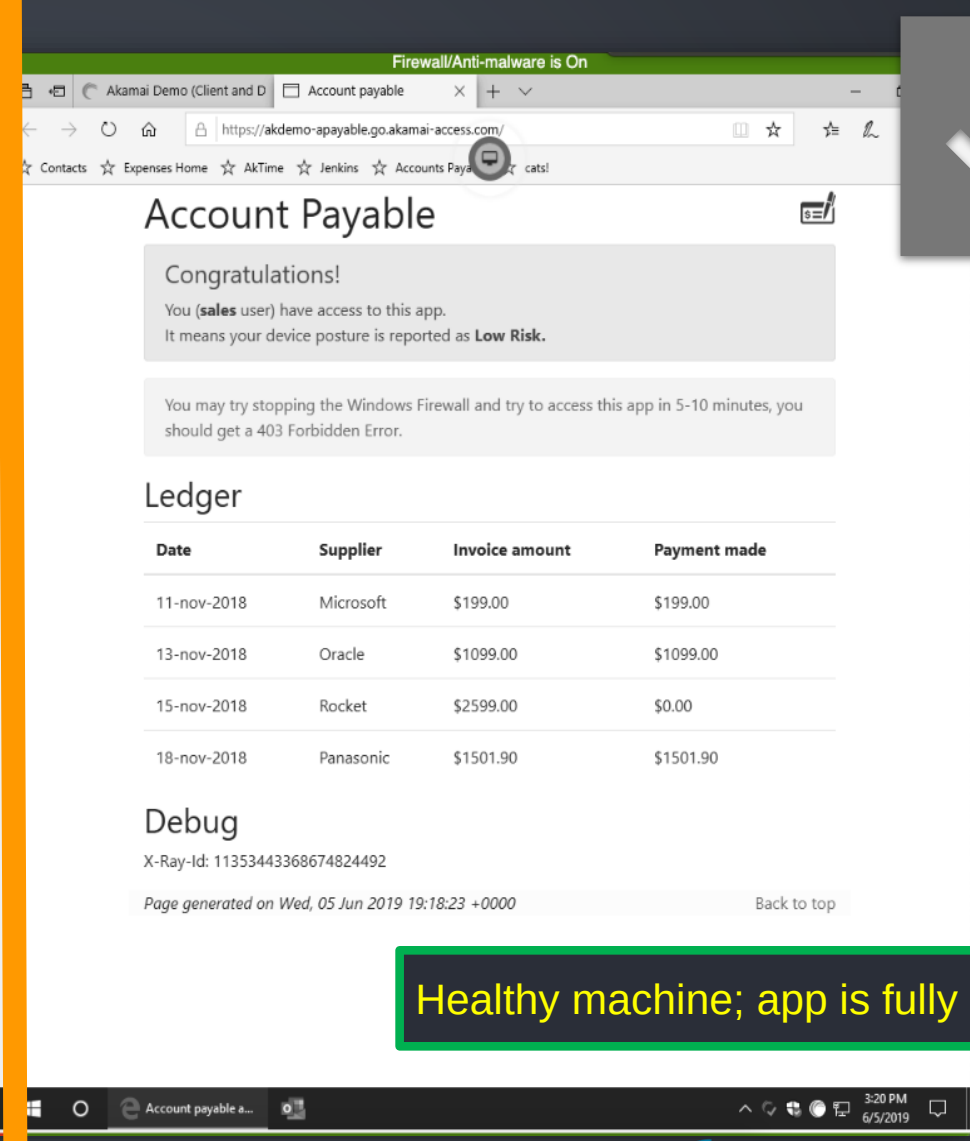




Device Posture - Example

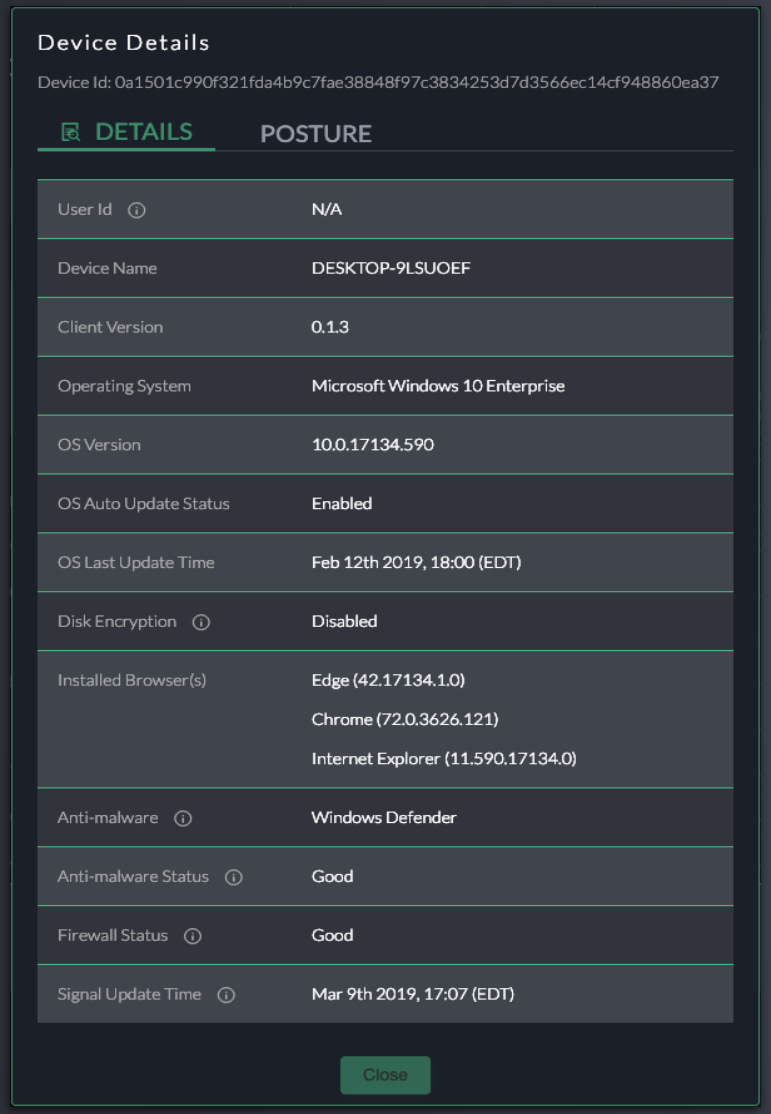


Unhealthy machine. User can't access application; user remediation suggestion displayed



Healthy machine; app is fully accessible

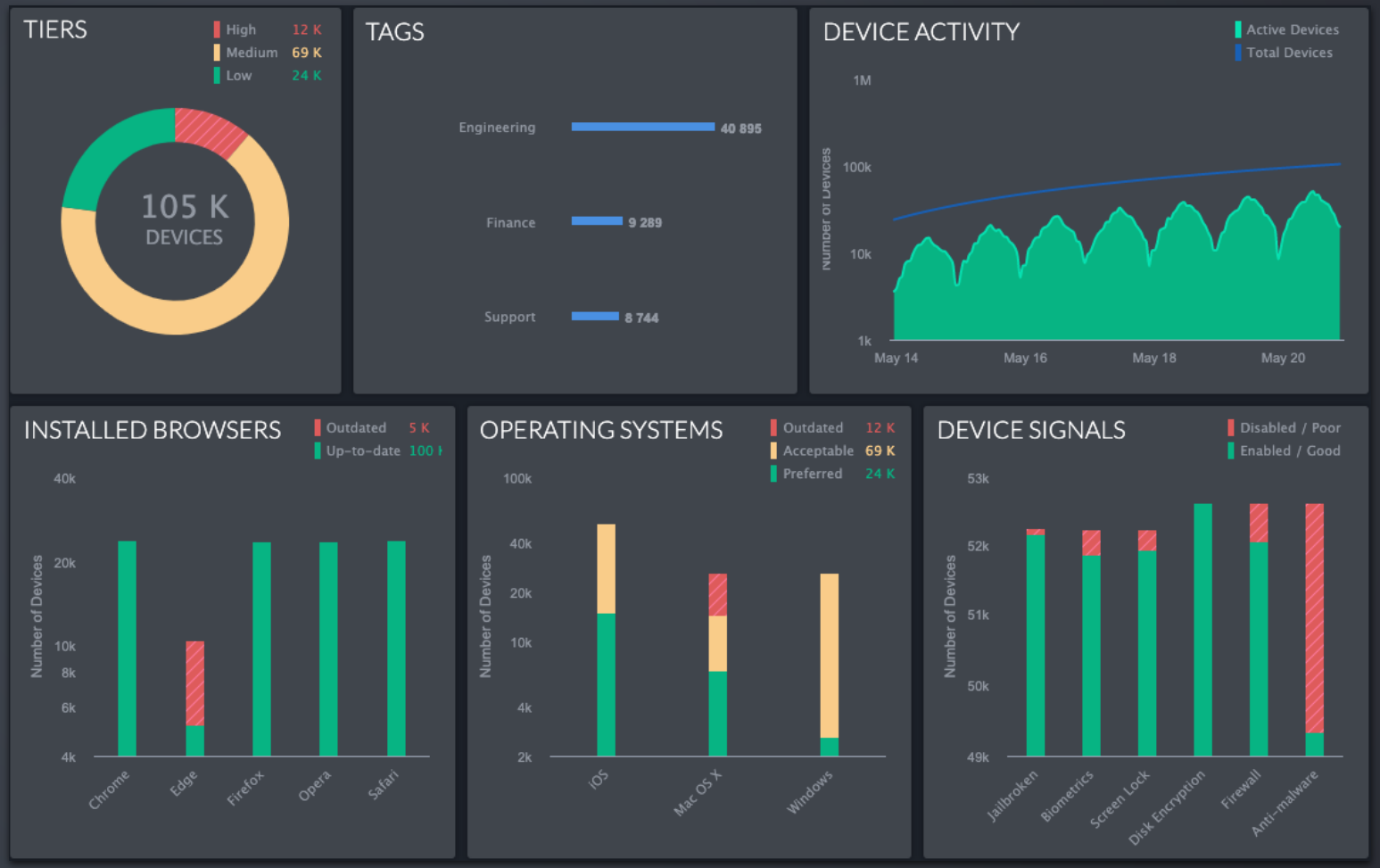
Device Signal Details



- Identifiers
  - Akamai unique device ID
  - Logged in user ID, machine name
- OS details
  - Platform and version info
  - OS auto update enablement status and last OS update time
- Disk encryption
  - Encryption status of the OS partition user is logged in to
- Installed web browser versions
  - Chrome, Firefox, Safari, Internet Explorer, Edge
- Firewall and anti-malware status
  - Status of OS built in firewall
  - Anti-malware as detected by Windows, or predefined software list on macOS
- Signal update time
  - Timestamp of last signal update from the device posture client
  - Expected 30 minute update interval for an online client
    - More often if signal changes are detected

Device Posture Dashboard

- Device risk & activity at a glance
  - Activity based on signal updates from device posture client
- Device signal breakdown
- Interactive graphs
  - Clickable to view device inventory details



Global Manufacturing Company Embraces Zero Trust

LIXIL

Lixil manufactures and sells water and housing products within its brands LIXIL, INAX, American Standard, and GROHE. The business has $12 billion in revenue and 70,000 employees in 150 countries.

Pain Points:

- Management and security of thousands of locations such as offices, showrooms, factory locations, and more.
- Multiple business partners accessing internal applications.
- Malware lateral movement from ASEAN countries to Tokyo.
- Poor application performance, especially overseas users accessing Tokyo-based apps like SAP. Thus, current network-based.
- Approach had access to a large attack surface, high management overheads, spotty user experience, high rates of expense.
- Use Cases

Business Outcome

- Solution for cloud migration (modernized architecture)
- Replacing legacy systems, streamline the traditional IT system with strong requirement to increase security
- Modern auth-n/auth-z module

Indian Multinational – Agrochemicals

Client – Server Database access

Challenge

- Large database file transfer
- Access from remote location
  - slow performance

Solution

- Zero Trust + Acceleration

Test Case	Time taken (Approx.)	User Location
Test Case 1: Using VPN client (through open Internet)	~ 5 min.	Mumbai
Test Case 2: Through local LAN	< 2 min.	Mumbai
Test Case 3: Using Zero Trust Client (through open Internet)	~ 2.5 min.	Mumbai
Test Case 4: Using Zero Trust Client + Acceleration (through open Internet)	~ 1 min.	Mumbai
Test Case 5: Using VPN client (through open Internet)	Not useable / too long to measure	USA
Test Case 6: Using Zero Trust Client (through open Internet)	~ 13 minutes	USA
Test Case 7: Using Zero Trust Client + Acceleration (through open Internet)	~ 6 minutes	USA

Global Logistics Company

American Logistics company who is a leading global provider of specialized transportation and logistics services, and leading package delivery provider. They manage the flow of goods, funds, and information in more than 200 countries and territories worldwide.

Challenges

- Frequent acquisitions and has typically spun up VPN tunnels for newly acquired groups to access apps.
- Time-consuming (6-9 months) and creates a bad user experience
- Needed a convenient way to expose customer facing apps to clients
- Required a secure DevOps environment for remote contractors to build and test applications

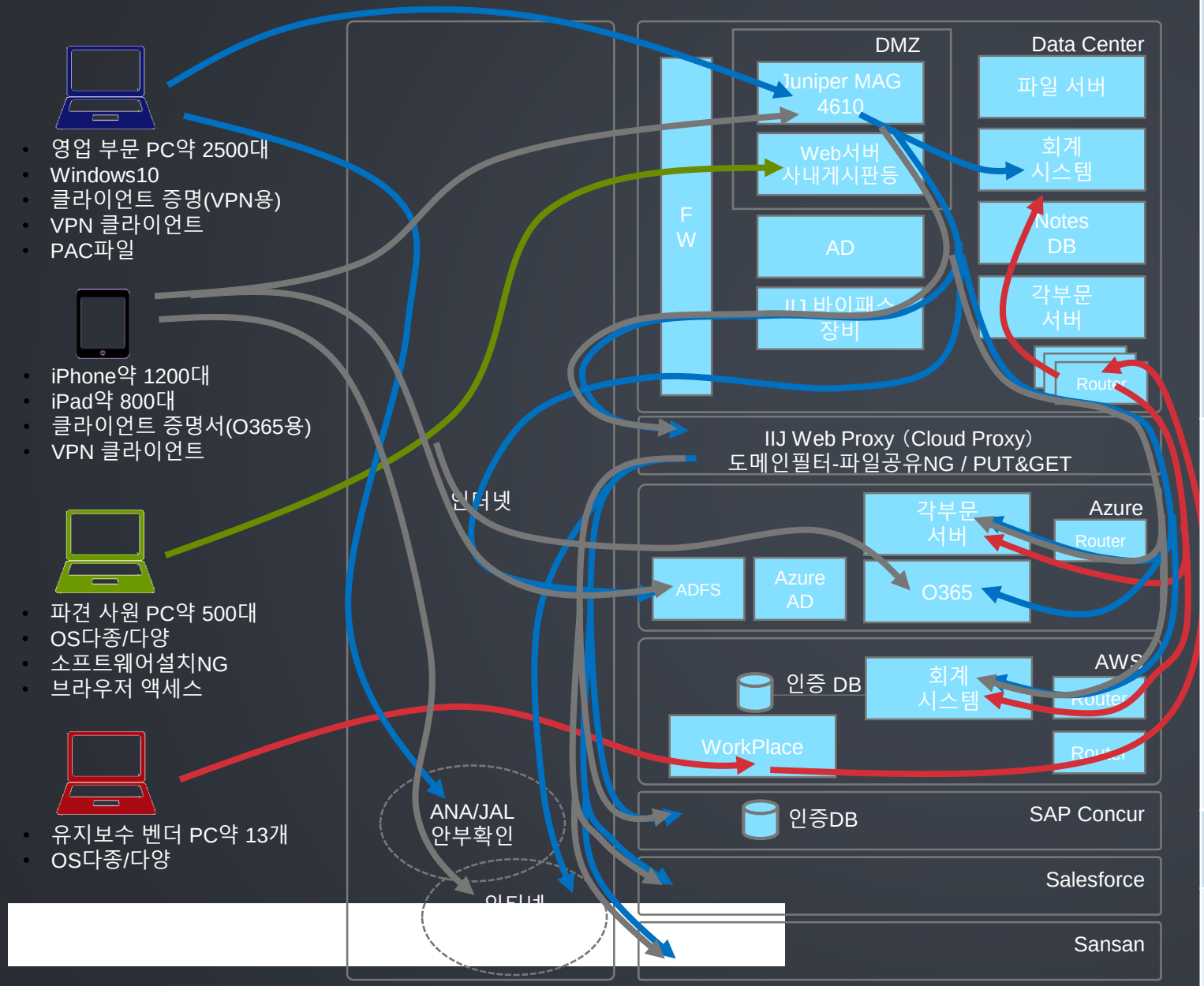
How Zero Trust Solved the Issues

- Zero Trust grants access to new users with a simple AD sync, cutting months off of the integration time
- Able to spin-up access on the fly to new clients with a simple URL and credentials
- Provide app-level access to developers and meet security requirements

Where can this take us?

- Internet is the corporate network
- Every office is a hotspot
- All apps feel like SaaS apps
- No Passwords, No VPN

AS-IS



출발지	목적지	방식
영업 부문 PC	사내시스템 DC Azure AWS	• Juniper MAG에서 Client증명서, AD인증 • 각 서버에는 kerberos 인증 • 수신처가 Azure/AWS의 경우는 개별회선경유 • AWS에 대해서는 AD인증이 아닌 개별인증
	SaaS 애플리케이션 Salesforce SAP Concur SanSan	• Juniper MAG에서 Client증명서, AD인증 • IIJ바이패스기를 통과후, IIJ Web Proxy(Cloud)를 경유하여 액세스 • IIJ Web Proxy 에서는 도메인 필터를 실시 • 몇몇 SaaS에는 IIJ Web Proxy를 경유할 때의 글로벌 IP를 송신원IP로서 필터를 정의
	SaaS 애플리케이션 O365	• Juniper MAG에서 Client증명서, AD인증 • IIJ 바이패스, IIJ Web Proxy는 경유하지 않는다 • ADFS 경유로 AD연계 하고 있는 Azure AD로 인증 • 인증후 접속은 개별회선경유
	인터넷 접속	• Juniper MAG에서 Client증명서, AD인증 • IIJ바이패스기를 통과후, IIJ Web Proxy(Cloud)를 경유하여 액세스 • IIJ Web Proxy 에서는 도메인 필터를 실시
	인터넷 액세스(예외)	• ANA/JAL, 안부 확인 등의 예외사이트에는 PC에서 직접 접속
iPhone /iPad	사내시스템 Azure AWS	• Juniper MAG에서 Client증명서, AD인증 • 개별 회선 경유 • AWS에 대해서는 AD인증이 아닌 개별인증
	SaaS 애플리케이션 Salesforce SAP Concur SanSan	• Juniper MAG에서 Client증명서, AD인증 • IIJ바이패스기를 통과후, IIJ Web Proxy(Cloud)를 경유하여 액세스 • IIJ Web Proxy 에서는 도메인 필터를 실시 • 몇몇 SaaS에는 IIJ Web Proxy를 경유할 때의 글로벌 IP를 송신원IP로서 필터를 정의
	SaaS 애플리케이션 O365	• 디바이스로부터 직접 인터넷을 경유해 액세스 • Client 증명서와 ADFS 경유로 AD연계 하고 있는 Azure AD로 인증
	인터넷 접속	• 디바이스로부터 직접 인터넷을 경유해 액세스
	인터넷 액세스(예외)	• ANA/JAL, 안부확인 등의 예외사이트에는 PC로부터 직접 접속
파견 사원 PC	게시판/인사정보	• DMZ상의 Web서버에 다이렉트 액세스 • 인증은 휴대폰 인증 • 파견지의 글로벌 IP를 송신원IP로서 필터를 정의
유지보수 벤더PC	사내시스템 DC Azure AWS	• Amazon WorkSpaces로 인증 • 개별회선으로 DC를 경유해 거기서부터 각 사내 인프라에 SSH/RDP로 접속

문제점 및 해결 방안

항목	단적으로 말하면	내용
편리성	번거로움	• 메일이나 캘린더를 참조할 때마다 VPN 클라이언트를 기동할 필요가 있다.
	번거로움	• 인터넷을 참조할 때도 VPN 클라이언트를 기동할 필요가 있다. • 모바일 디바이스로 참조할 수 있으므로 그 쪽을 이용하고 있을 가능성도 있다.
	번거로움	• Sansan, Salesforce를 참조할 때도 VPN 클라이언트를 기동할 필요가 있다.
	번거로움	• 접속처에 따라 인증방법이 다르다. 기억해둘 수 없다.
	속도	• VPN접속에 시간이 걸린다.1-2분 걸리기도 하고 원인은 특정할 수 있지 않지만 Juniper MAG의 퍼포먼스의 가능성 있어.
	속도	• VPN 접속 후에도 퍼포먼스가 나쁘다.
보안	정보 유출	• 접속지/접속자에 따라 인증 방법이 다르다. • 간단한 패스워드 설정이나 PC에 메모장 보존하고 있을 가능성이 나온다.
	Gray Zone의 여부	• iPhone/iPad는 인터넷에 다이렉트 액세스 되어 있어 필터링 등은 실시되어 있지 않다.
	정보유출	• 파견직원이 이용하는 PC는 OS나 소프트웨어를 관리하지 않으며, PC가 바이러스에 감염되면 DMZ내 접속 서버가 공격을 받을 수 있다.
	정보유출	• 기본적으로 네트워크 레벨의 VPN 접속으로 하고 있기 때문에, 원격 디바이스가 DMZ상에 있는 상태가 되고 있다. 이 때문에, 만일 원격 디바이스가 말웨어에 감염되었을 경우 사내의 모든 접속자에 피해가 초래될 가능성이 있다.
운용	일관성의 결여	• 인터넷에 직접 접속할 수 있는 경우, VPN을 경유하는 경우, 그렇지 않은 경우, 개별 회선을 지나는 PaaS와 그렇지 않은 PaaS도 있는 인증 방식도 통일되어 있지 않다. • 문제가 생기면 그 원인을 규명하는 데 시간이 더 필요할 수도 있다
	번거로움	• PaaS와의 통신에 개별회선을 이용하는 경우와 이용하지 않는 경우가 존재하여 PAC로 관리하는 것도 매우 번거롭다. • 특히 O365는 PAC의 운용이 번거롭다
장래성		• 사내 업무 어플리케이션은 DC에서 클라우드로 이행하게 되면 데이터센터 중심으로 생각할 필요가 없어지지만 네트워크나 보안이 따라오지 못하고 있다.

- Zero Trust Architecture
- 탈 데이터센터 중심
- 탈 개별 회선
- 접근의 유연성
- 운용성의 향상
- 편리성의 향상
- 아키텍쳐의 평준화

Akamai Experience the Edge

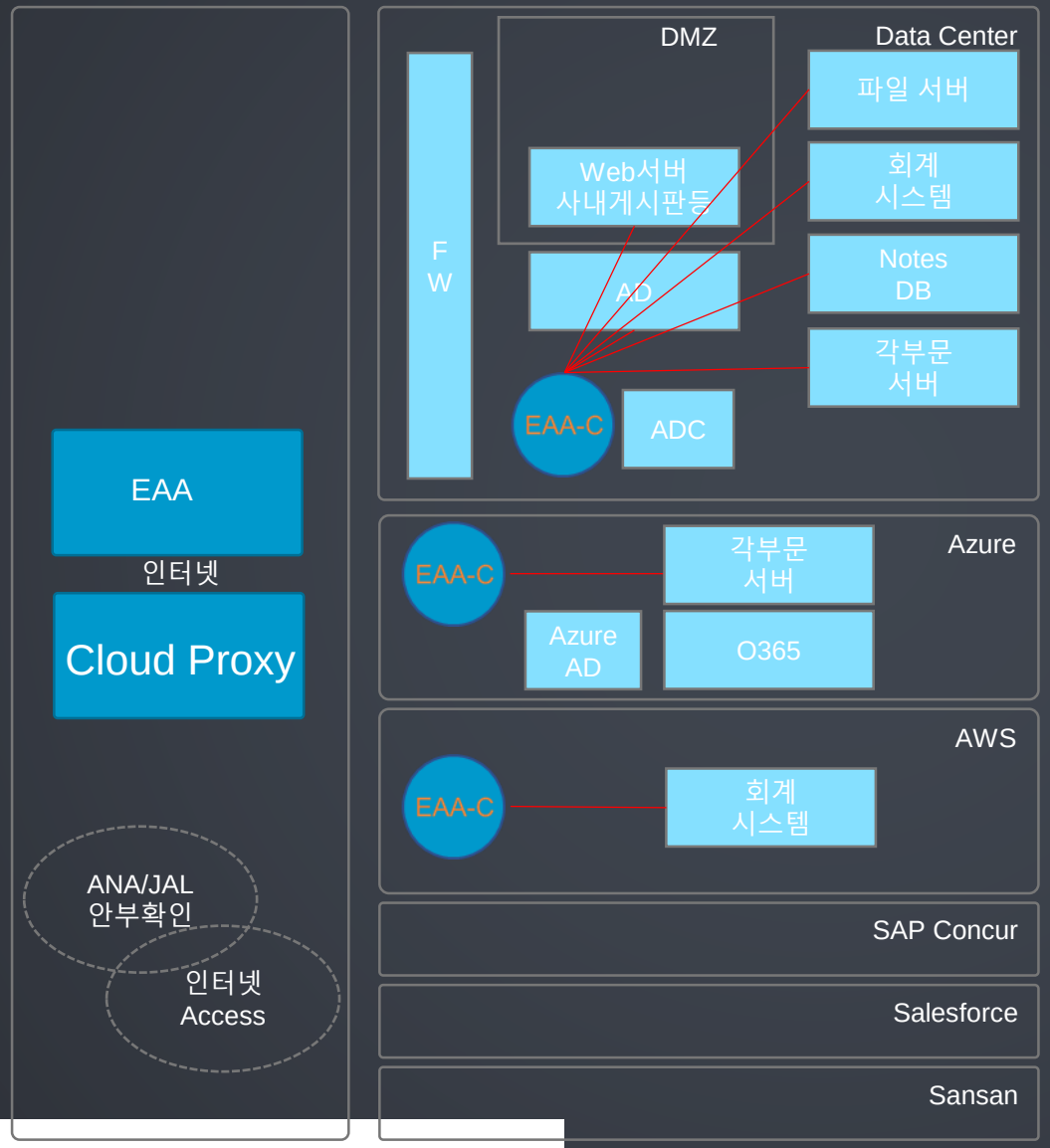
TO-BE

- 영업 부문 PC약 2500대
- Windows10
- 클라이언트 증명(VPN용)
- VPN 클라이언트
- PAC파일

- iPhone약 1200대
- iPad약 800대
- 클라이언트 증명서(O365용)
- VPN 클라이언트

- 파견 사원 PC약 500대
- OS다종/다양
- 소프트웨어설치NG
- 브라우저 액세스

- 유지보수 벤더 PC약 13개
- OS다종/다양



출발지	목적지	방식
영업 부문 PC	사내시스템 DC Azure AWS	• EAA 경유로 액세스, AD인증 • 각 서버에는 kerberos 인증 • 수신처가 Azure/AWS의 경우여도 EAA 경유, 개별회선철폐 • 각부문 서버의 개별 Directory도 AD에 통합
	SaaS 애플리케이션 Salesforce SAP Concur SanSan	• EAA 경유로 액세스, AD인증 • EAA를 IDP로서 SAML 제휴 • 인증 후에는 직접통신 • 웹프록시는 철폐
	SaaS 애플리케이션 O365	• EAA 경유로 액세스, AD인증 • EAA를 IDP로서 SAML 제휴 • 인증 후에는 직접통신
	인터넷 접속	• 단말기에서 ETP경유로 통신 • Cloud Proxy에 의해 위협 분석을 실시
	인터넷 액세스(예외)	• ANA/JAL, 안부 확인 등의 예외 사이트에도 단말기로부터 ETP 경유로 통신 • Cloud Proxy에 의해 위협 분석을 실시
iPhone /iPad	사내시스템 Azure AWS	• EAA 경유로 액세스, AD인증 • 각 서버에는 kerberos 인증 • 각부문 서버의 개별 Directory도 AD에 통합
	SaaS 애플리케이션 Salesforce SAP Concur SanSan	• EAA 경유로 액세스, AD인증 • EAA를 IDP로서 SAML 제휴 • 인증 후에는 직접통신 • 웹프록시는 철폐
	SaaS 애플리케이션 O365	• EAA 경유로 액세스, AD인증 • EAA를 IDP로서 SAML 제휴 • 인증 후에는 직접통신
	인터넷 접속	• 단말기에서 ETP경유로 통신 • Cloud Proxy에 의해 위협 분석을 실시
	인터넷 액세스(예외)	• ANA/JAL, 안부 확인 등의 예외 사이트에도 단말기로부터 ETP 경유로 통신 • Cloud Proxy에 의해 위협 분석을 실시
파견 사원 PC	게시판/인사정보	• EAA 경유로 액세스, AD인증
유지보수 벤더PC	사내시스템 DC Azure AWS	• EAA 경유로 액세스, AD인증

Moving Beyond Perimeter Security

A comprehensive & achievable roadmap to less risk

akamai.com/zerotrust

THANK YOU

www.akamai.com/zerotrust

ypaek@akamai.com

Akamai

Experience the Edge