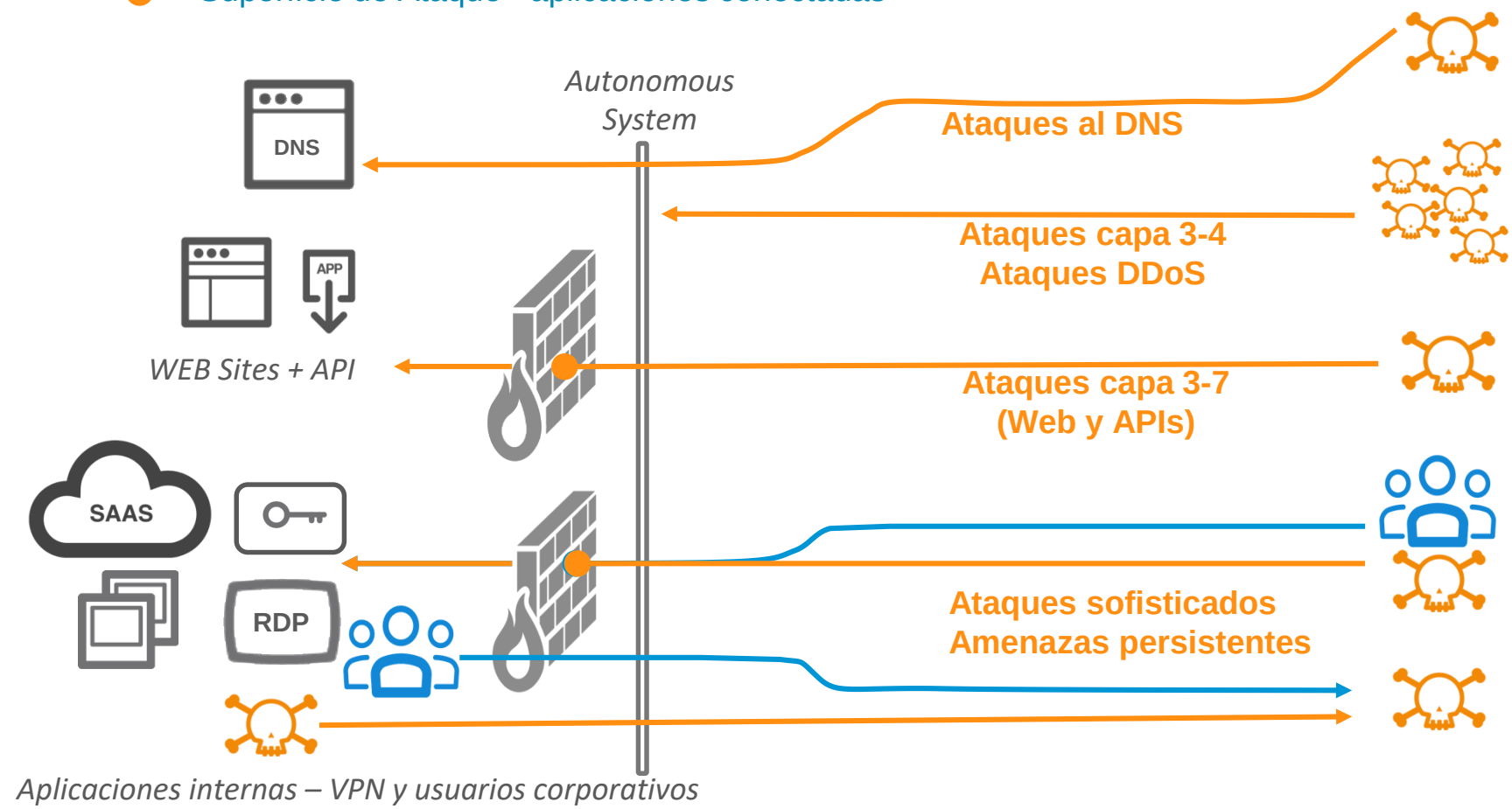
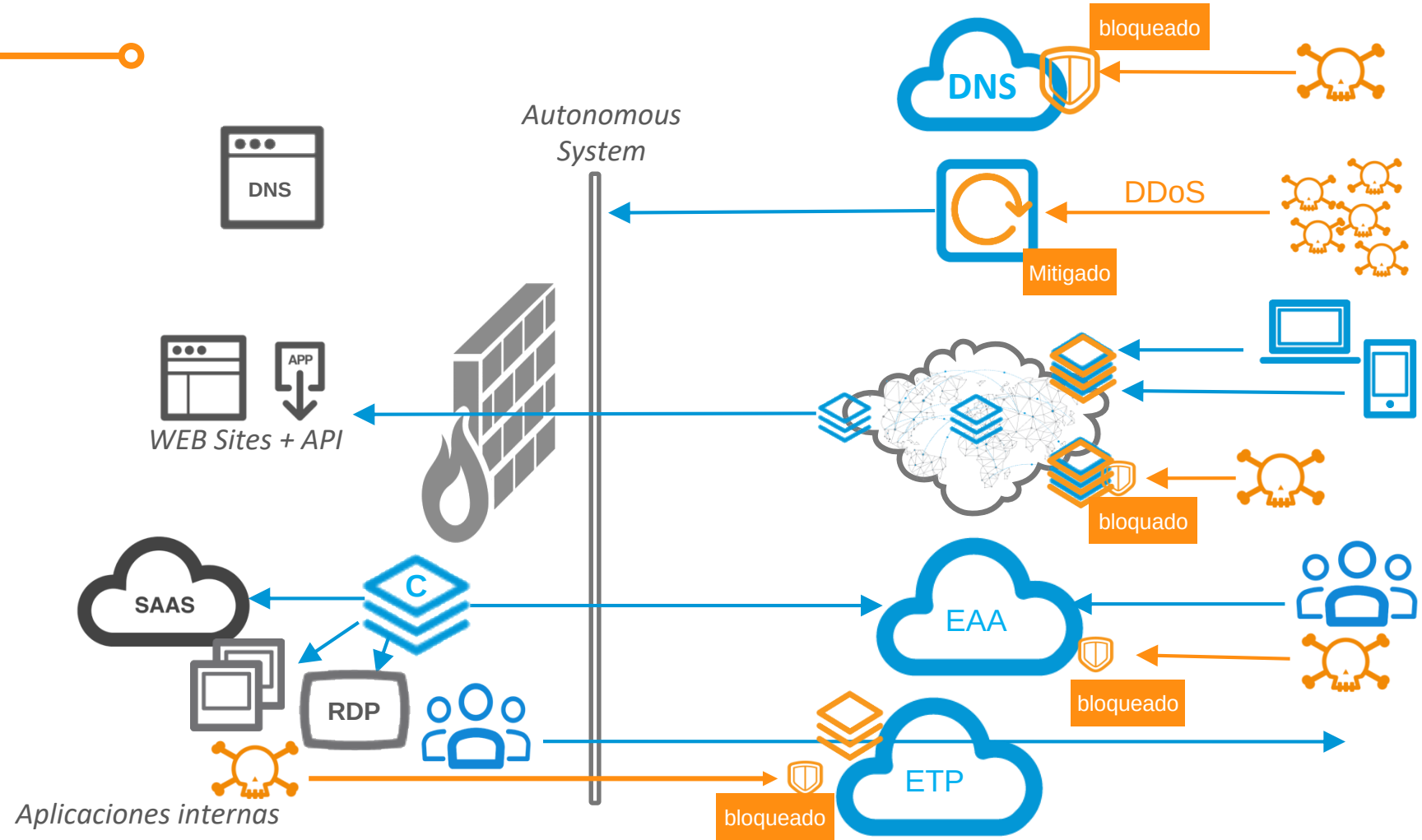
Superficie de Ataque de la Empresa actual

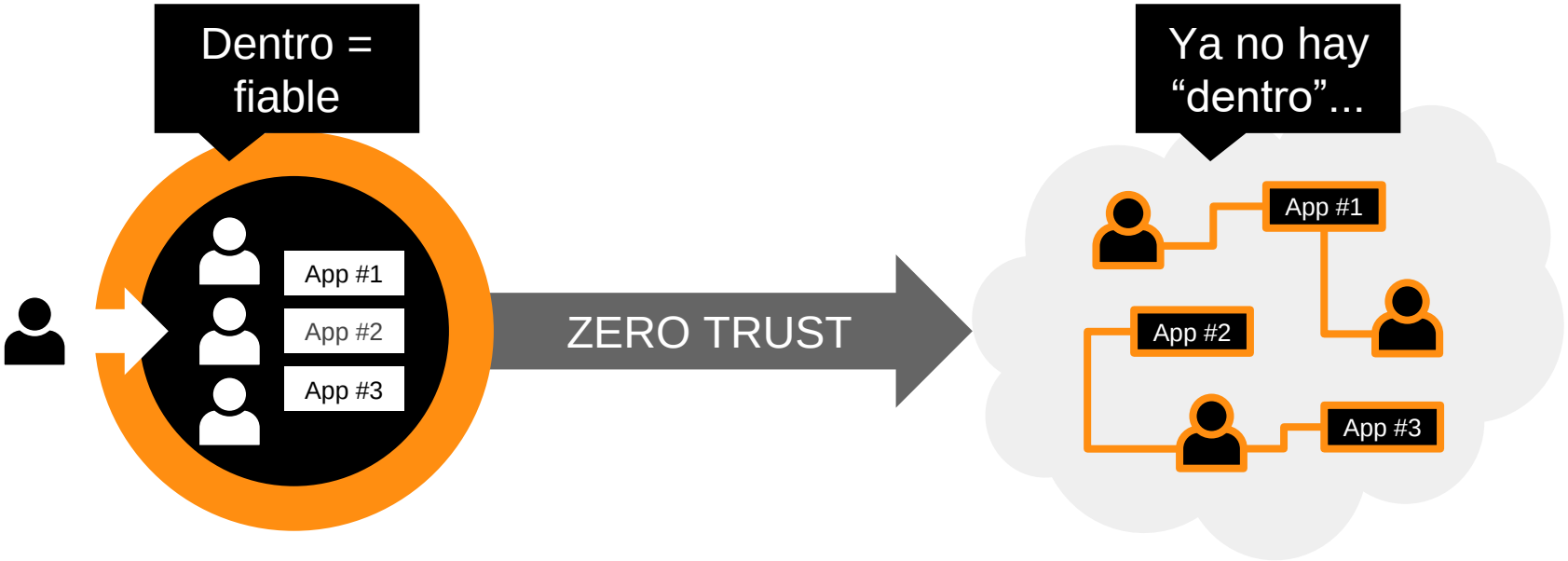
Luciano Lemberg – CTO
Enric Mañez, Enterprise Security Sales Manager Akamai Technologies
2019-11 – IT Digital

Superficie de Ataque - aplicaciones conectadas




DNS
bloqueado
Autonomous System
DNS
DDoS
Mitigado
APP
WEB Sites + API
bloquado
SAAS
C
EAA
bloqueado
RDP
ETP
bloqueado
Aplicaciones internas

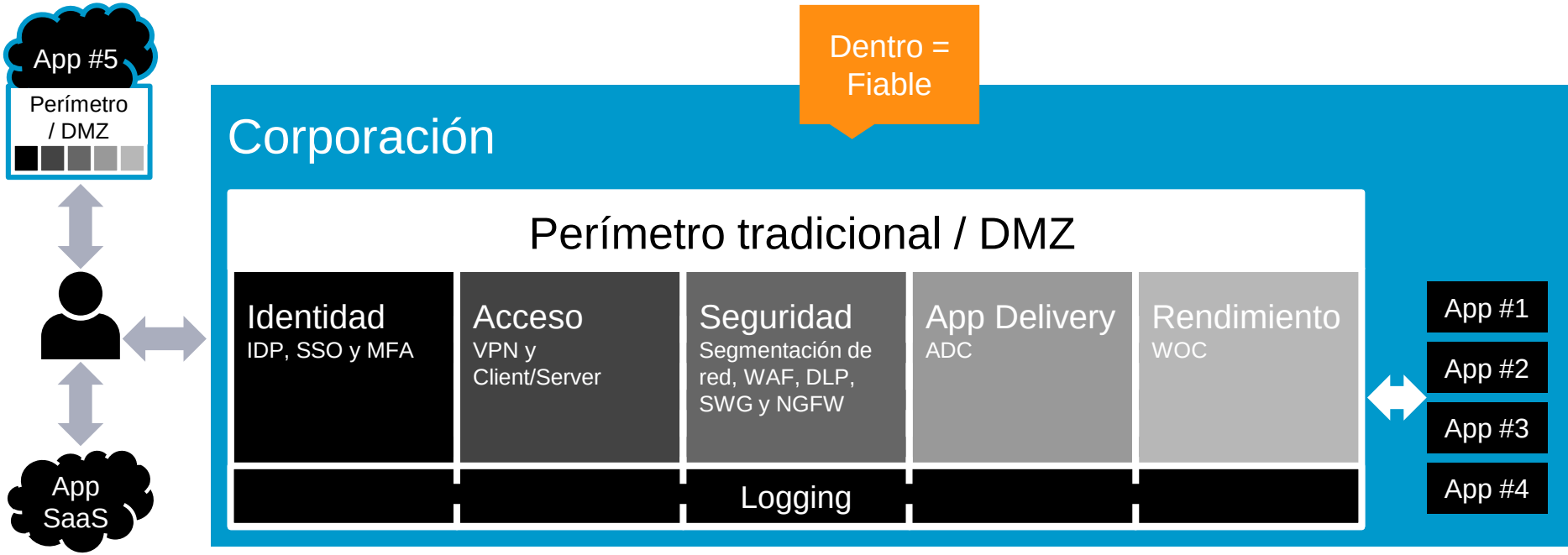
Movilidad y Cloud requieren una Evolución en Seguridad



Usuarios y apps dentro
Confiar pero verificar
Acceso total a red

Usuarios y apps distribuidos
Verificar y nunca confiar
Acceso a la aplicación

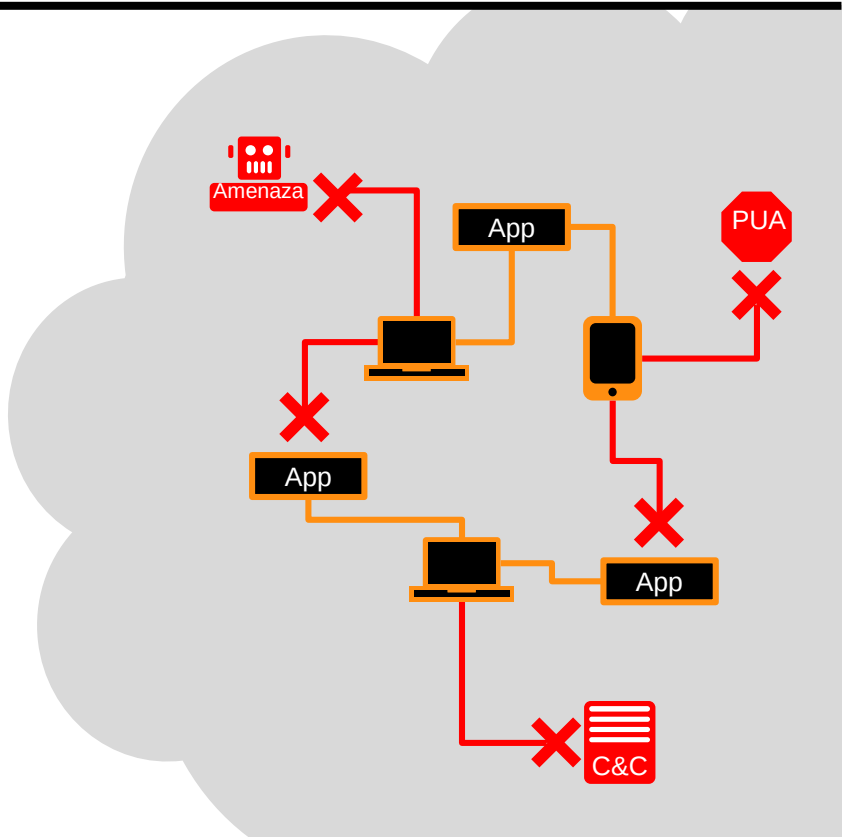
Los perímetros tradicionales son complejos y aumentan los riesgos



La seguridad Cloud es sencilla y reduce riesgos

Una única platforma Clooud para securizar todos los usuarios y aplicaciones de la empresa

- Identidad y acceso a app
- Single sign-on con autenticación multifactor
- Rendimiento y seguridad de apps
- Protección frente a amenazas avanzadas
- Inspección inline de datos



¿Qué aporta Akamai con Zero Trust?

SEGURIDAD

Reduce las posibilidades de ataque por “movimiento lateral”

Bloquea y no hace uso del tráfico entrante en la red

SIMPLICIDAD

Elimina la complejidad de la publicación de aplicaciones

Facilita el despliegue y la escalabilidad de las aplicaciones en entornos híbridos

RENDIMIENTO

Añade todas las capacidades de aceleración inteligente de la plataforma

Mejora significativamente la experiencia del usuario

¿Dónde aplican nuestras soluciones?

Algunos ejemplos:

Acceso seguro de 3’s

Fusiones & Adquisiciones

Acceso seguro a Cloud (IaaS & SaaS)

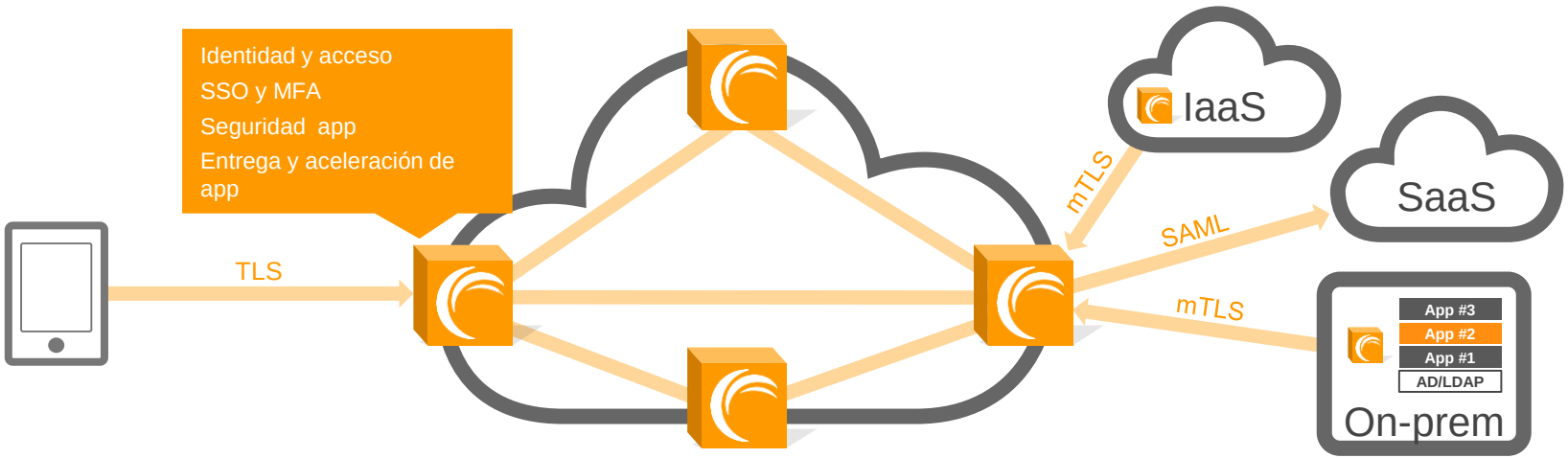
Eliminación de la VPN tradicional

Mejora de forma simple la “postura” de seguridad

Seguridad en el Edge para Acceso Directo a Internet (DIA)

EAA: Enterprise Application Access

Acceso seguro a aplicaciones On-Prem, IaaS y SaaS



Centralice el control de seguridad y acceso

A aplicaciones específicas sobre I/SaaS y on-prem

Mantenga a los usuarios fuera de la red corporativa

Haga su infrastructura invisible en Internet

Single sign-on para todas sus aplicaciones

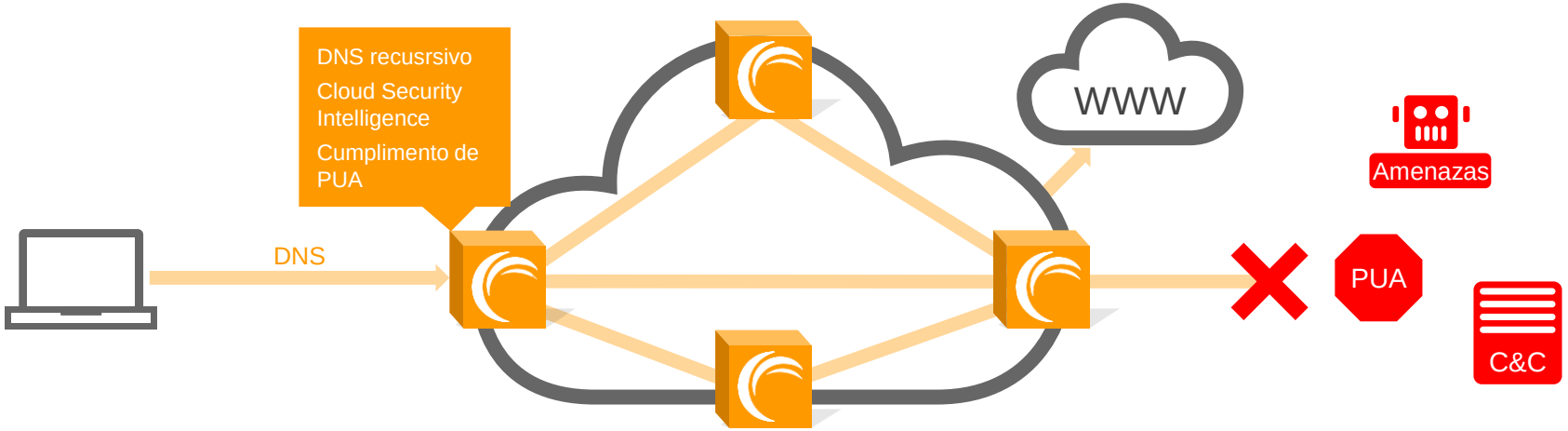
I/SaaS y on-prem

Autenticación multifactor para todas las aplicaciones

Soporta email, SMS, TOTP o Duo

ETP: Enterprise Threat Protector

Protección proactiva frente a malware usando DNS



Identifique y bloquee acceso a dominios nocivos – en cualquier localización

Rechaza peticiones o comunicaciones a dominios nocivos de los que se sabe que sirven malware o phishing

Bloquee las comunicaciones desde dispositvos comprometidos o infectados

Corta las conexiones existentes entre dispostivos infectados y la infraestructura de command & control de los atacantes

Prevenga el acceso a contenido inapropiado

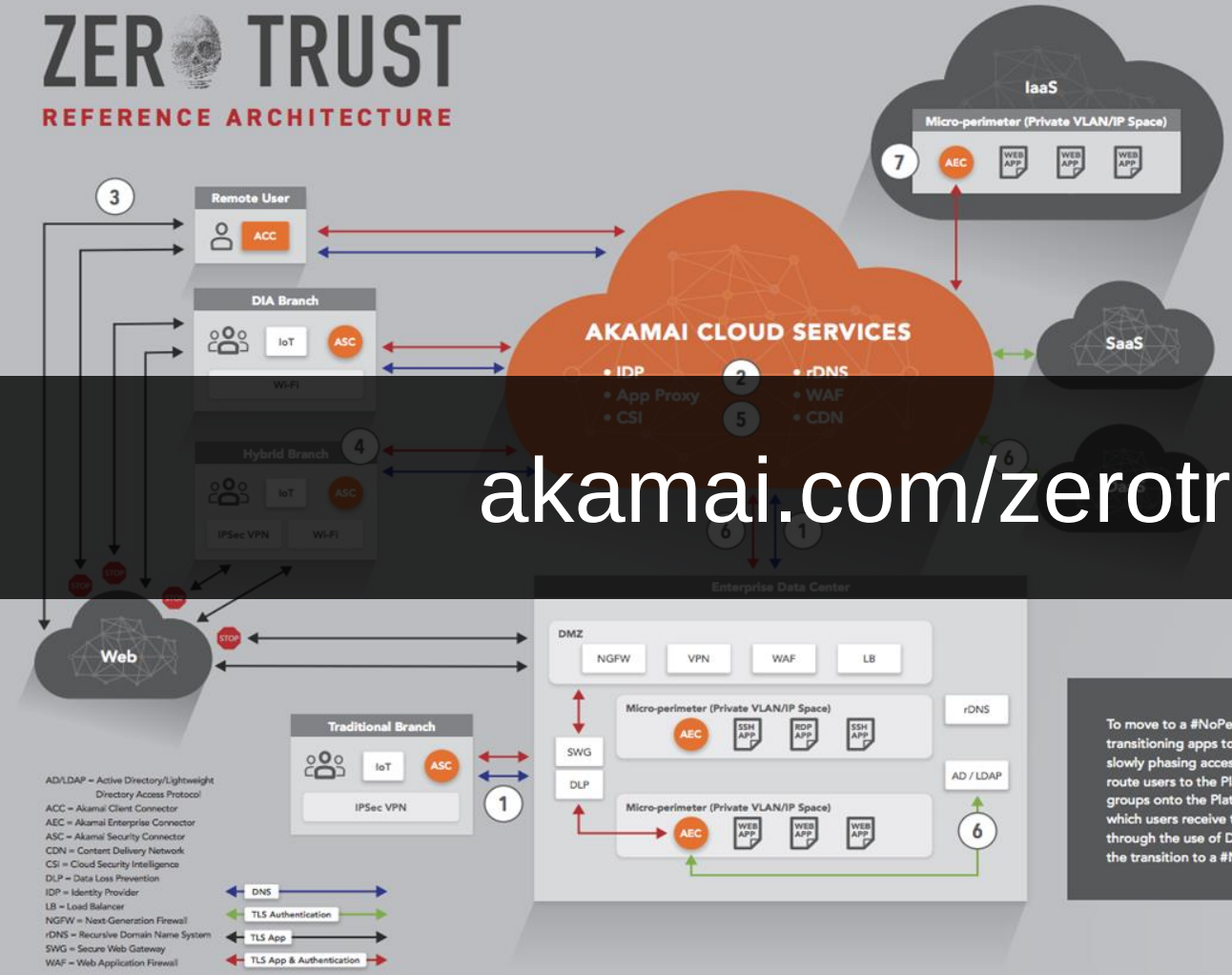
Hace cumplir de forma fácil las políticas de uso aceptable de internet de la empresa, de forma eficaz y consistente

Prevenga la exfiltración de datos basada en DNS

Impide a los actores maliciosos usar el protocolo DNS para extraer datos corporativos

ZERO TRUST

REFERENCE ARCHITECTURE



1. The user makes a DNS request for an enterprise app or domain on the web. The local enterprise rDNS infrastructure, or the Akamai Client Connector (ACC) if off-network, forwards the request to the Akamai rDNS Platform.
2. Akamai evaluates the domain against Akamai's Cloud Security Intelligence (CSI) to determine whether it is known or suspected to be malicious.
3. If the domain is not malicious, Akamai's infrastructure will hand back the appropriate IP to the destination on the web or the Akamai Platform for enterprise app access authentication and authorization.
4. If the domain is malicious, or inappropriate based on configured policy, the Akamai Platform will either block access or hand back the internal IP of the Akamai Security Connector (ASC). The ASC will capture the internal IP of the endpoint making the malicious request and send that over TLS to Akamai CSI for correlation to facilitate endpoint identification.
5. If the domain was for an enterprise app on the Akamai Platform, it will use the CNAME process to hand out the appropriate IP to the WAF, CDN, IDP, and App Proxy functionality on the Akamai Platform.
6. The Akamai Platform will serve a login page, optionally using a client certificate for initial authentication, and use the Akamai Enterprise Connector (AEC) to validate that the user and password exists in the appropriate identity store (IDaaS, Akamai IDP, and AD/LDAP on-prem) to authenticate the user, (optionally triggering Multi-Factor Authentication) and authorize specific app access.
7. The AEC will leverage a mutually authenticated TLS connection (outbound only) with the Akamai Platform, and the TLS connection from the user's browser, to create a proxied path across the Akamai Platform from the end user to the application. For configured SaaS apps, Akamai will handle authentication and authorization only, but for other apps, will log access details.

To move to a #NoPerimeter security model that embraces zero trust and BeyondCorp™ ideologies, begin transitioning apps to the Akamai Platform in small batches. Part of the application transition will involve slowly phasing access to select user groups. Application hostnames are CNAME'd to Akamai in order to route users to the Platform. Take advantage of this architecture as a way to phase the different user groups onto the Platform for each application by controlling which groups follow the CNAME chain and which users receive the internal A-record using the outdated perimeter method. This can be achieved through the use of DNS Views, also known as split-horizon DNS, to define the set of users and facilitate the transition to a #NoPerimeter security model. To learn more, visit akamai.com/zerotrust.

Akamai

¿Por qué pasar a Seguridad Cloud con Akamai?

Cloud Nativo

Menor OpEx

Menos Riesgos

Mejor Rendimiento

Faster Forward

@Akamai