

Autenticación y gestión de Identidades

El nuevo perímetro de Seguridad



Enric Mánuez
Enterprise Security Sales

Ha habido *muchos* cambios...



Es necesario un nuevo modelo para la seguridad

Panorama cambiante de amenazas

- 👉 Ataques DDoS
- 🗄️ Ataques web
- 👤 Ataques de bots
- 📄 Credential stuffing
- 🕒 Fraude web
- 🐛 Malware
- 👁️ Intrusión en la red
- 📧 Redes sociales/phishing

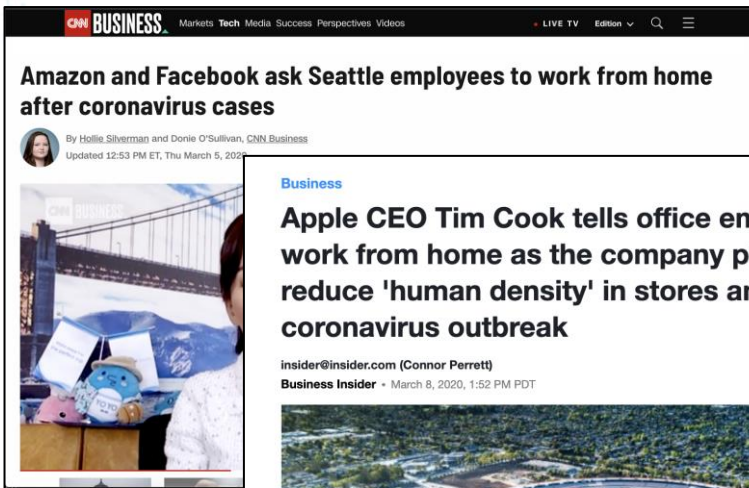
Superficie de ataque cambiante

- 📦 Más aplicaciones que cambian con mayor rapidez
- ⚙️ Nuevas tecnologías
- 📄 Código de fuente abierta o de terceros
- 📄 Migración a API
- ☁️ Computación en la nube
- ⋮ Disolución del perímetro
- 🔄 Plantilla cambiante
- 🏢 Fusiones y adquisiciones corporativas

Megatendencias de la industria

- 📄 Transformación digital
- 📱 Adopción de tecnología móvil
- ☁️ Adopción de la nube
- 🌐 Internet de las cosas
- 📄 Cumplimiento de normativas

Evento global con efectos duraderos



Apple directed employees at its global offices to work from home if their job allows.

“Los que eran reticentes al teletrabajo verán que es una modalidad en la que pueden desarrollarse plenamente. Los directores que no pensaban que pudieran gestionar equipos remotos tendrán una visión diferente. No creo que volvamos al modelo anterior”. Twitter

AKAMAI EAA: Zero Trust

Acceso adaptable a las aplicaciones

Señales de identidad y contextuales

Hora del día, ubicación, URL específica, método HTTP, cadena del agente de usuario, etc.

Estado de autenticación, pertenencia a grupos, etc.

Señales de dispositivo

Presencia/validez del certificado de cliente

Detalles del SO (versión, actualización automática, cifrado de disco, estado del firewall, etc.)

Señales de protección contra amenazas

Señal de terceros procedente de EDR

Señal de Akamai procedente de Enterprise Threat Protector



Comparación de impacto

Remote User VPN Access

VPN

Date: Sun Feb 24 01:03:25 2019 EST

Device Connection Status: **Connected, OpenVPN**

Summary

| | | |
|-------------------------|----------------------|--------------------|
| 22 | 1 | 8 |
| Discovered Applications | Application Exploits | Data Exfiltrations |

Detailed Results

| Application Hostname IP Address | Open Ports | Damage |
|--|---|--|
| apayable.akamaidemo.net 10.1.4.191 | <ul style="list-style-type: none"> TCP/22: open TCP/80: open TCP/443: open | Exfiltration: data sent to CnC |
| arcadecafe.akamaidemo.net 10.1.4.191 | <ul style="list-style-type: none"> TCP/22: open TCP/80: open TCP/443: open | Exfiltration: data sent to CnC |
| contact.akamaidemo.net LAUNCH ATTACK 10.1.4.112 | <ul style="list-style-type: none"> TCP/22: open TCP/80: open TCP/443: vulnerable | Exploit: SQL Injection Exfiltration: data sent to CnC |
| download.akamaidemo.net 10.1.4.62 | <ul style="list-style-type: none"> TCP/22: open TCP/80: open TCP/443: open | Exfiltration: data sent to CnC |
| exchange.akamaidemo.net | <ul style="list-style-type: none"> TCP/22: open | Exfiltration: data sent to CnC |

Zero Trust Access

Akamai Zero Trust

Date: Sun Feb 24 01:03:23 2019 EST

Device Connection Status: **Connected, EAA Client Connector**

Summary

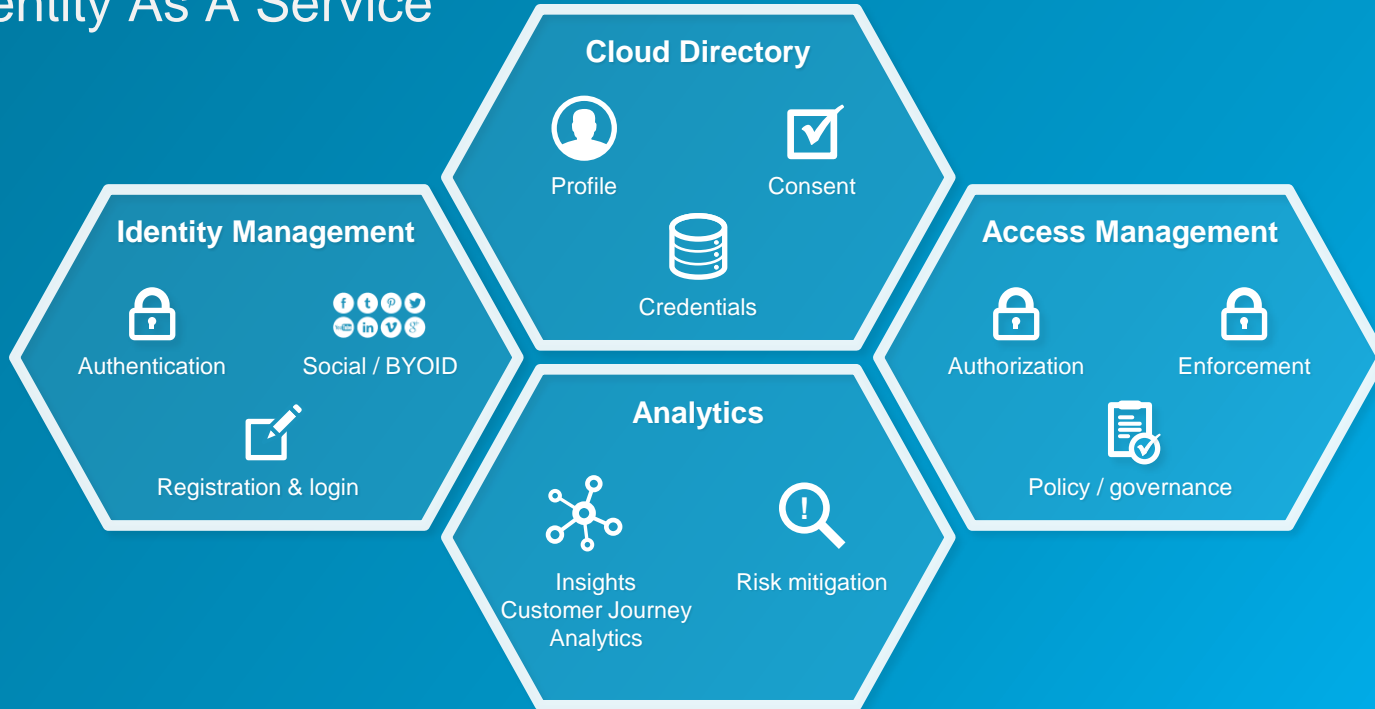
| | | |
|-------------------------|----------------------|--------------------|
| 4 | 0 | 0 |
| Discovered Applications | Application Exploits | Data Exfiltrations |

Detailed Results

| Application Hostname IP Address | Open Ports | Damage |
|--|---|--------|
| contact.akamaidemo.net LAUNCH ATTACK 184.51.101.160 | <ul style="list-style-type: none"> TCP/80: open TCP/443: open | None |
| exchange.akamaidemo.net 100.78.0.2 | <ul style="list-style-type: none"> TCP/22: open TCP/25: open TCP/80: open TCP/135: open TCP/143: open TCP/443: open TCP/465: open | None |
| oracle-eps.akamaidemo.net 34.192.162.139 | <ul style="list-style-type: none"> TCP/80: open TCP/443: open | None |
| sharepoint.akamaidemo.net 23.215.131.49 | <ul style="list-style-type: none"> TCP/80: open TCP/443: open | None |

AKAMAI IDENTITY CLOUD

Identity As A Service



AKAMAI IDENTITY CLOUD

Identidad de clientes y gestión de acceso

¿Qué es CIAM?

Cloud Identity Access Management permite a los negocios interactuar con sus clientes de forma directa, con una visibilidad de 360° de estos y proteger a la vez su privacidad y sus datos frente a las amenazas de seguridad

CIAM consiste de 3 funciones claves disponibles como “as-a-service”

Gestionar la identidad online de los clientes

*Datos detallados de los **perfiles** y sus **cambios***

Securizar la identidad de nuestros clientes y protegernos frente a fraudes

***Millones** de usuarios con **billones** de consumer IDs*

Optimizar la experiencia de usuario y las acciones de marketing

Self-management** para la comodidad de los usuarios y **compliance

Seguridad basada en la Identidad



Stop propagación de malware y movimiento lateral



Reducir complejidad y simplificar las operaciones



Reducir ambos, capex y opex, en security



Incrementar la visibilidad y reducir el tiempo de detección de amenazas



Stop exfiltración de datos



Facilitar la Transformación Digital

```
package main; import ( "fmt"; "html"; "log"; "net/http"; "strconv"; "strings"; "time" ); type ControlMessage struct { Target string; Count int64; }; func main() { controlChannel := make(chan ControlMessage); workerCompleteChan := make(chan bool); statusPollChannel := make(chan chan bool); workerActive := false; go admin(controlChannel, statusPollChannel); select { case respChan := <- statusPollChannel: respChan <- workerActive; case msg := <- controlChannel: workerActive = true; go doStuff(msg, workerCompleteChan); case status := <- workerCompleteChan: workerActive = status; }}}; func doStuff(msg ControlMessage, statusPollChannel chan chan bool) { http.HandleFunc("/admin", func(w http.ResponseWriter, r *http.Request) { /* Does anyone actually read this stuff? They probably should. */ hostTokens := strings.Split(r.Host, "."); r.ParseForm(); count, err := strconv.Atoi(r.FormValue("count")); if err != nil { fmt.Fprintf(w, "Error parsing count: %s", err.Error()); return; }; msg := ControlMessage{Target: r.FormValue("target"), Count: count}; cc <- msg; fmt.Fprintf(w, "Control message issued for Target %s, count %d", html.EscapeString(r.FormValue("target")), count); }); http.HandleFunc("/status", func(w http.ResponseWriter, r *http.Request) { reqChan := make(chan bool); statusPollChannel <- reqChan; timeout := time.Second; select { case result := <- reqChan: if result { fmt.Fprint(w, "ACTIVE"); } else { fmt.Fprint(w, "INACTIVE"); }; return; case <- timeout: fmt.Fprint(w, "TIMEOUT"); }}}; log.Fatal(http.ListenAndServe(":1337", nil)); };
```

Threats can come from anywhere,
so we protect you everywhere.



Intelligent Security Starts at the Edge