Check Point
SOFTWARE TECHNOLOGIES LTD

IDENTIDADES

Protección y Aplicación

Eusebio Nieva

Director técnico para Iberia

Office of the CTO

Agenda

- Ataques
- Escenarios
  - Saas
  - Infraestructura en nube
  - Acceso basado en identidad

Ataques comunes

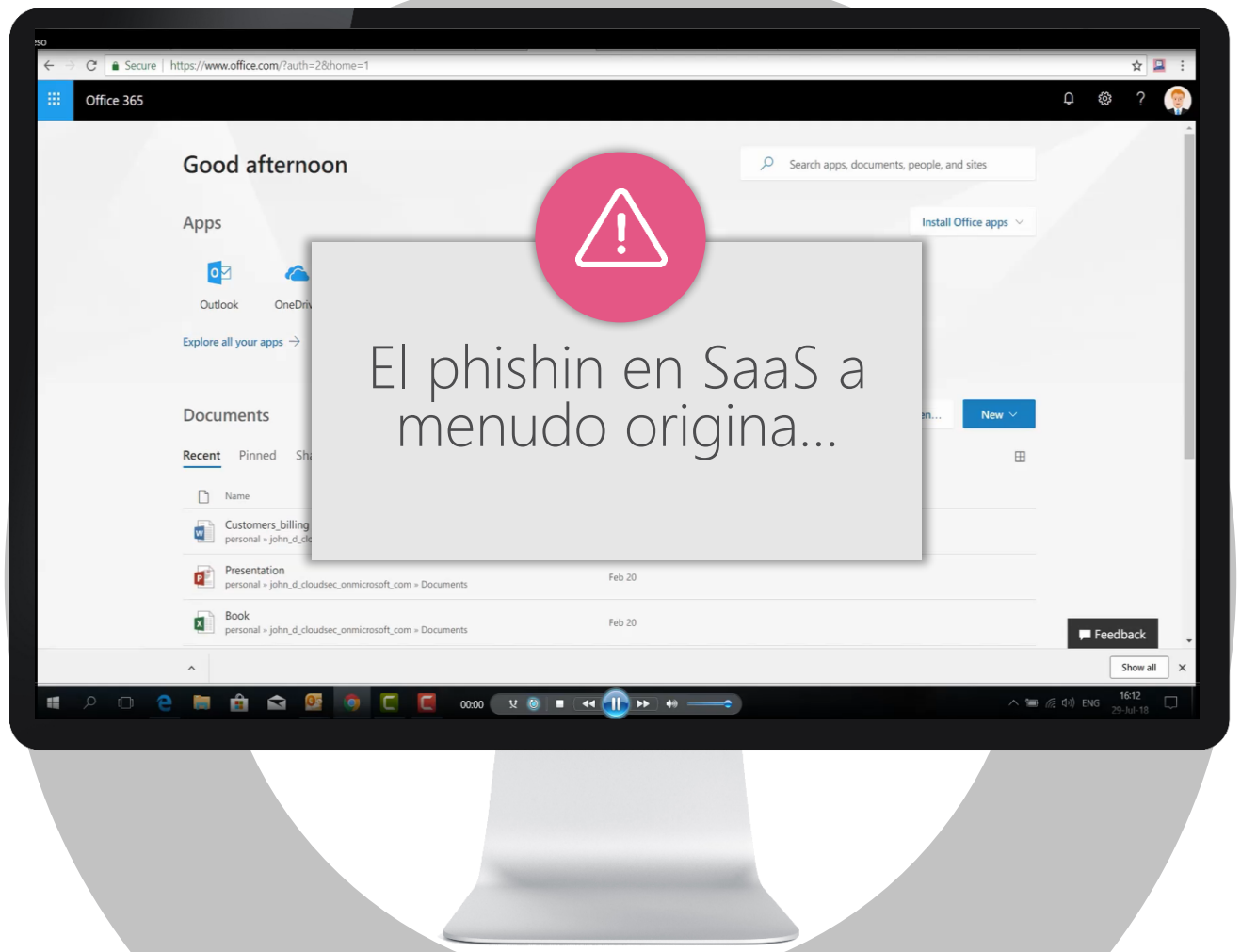
- Phishing
  - Spear phishing
  - Whaling attacks
- Reutilizar la contraseña
- Contraseñas débiles
- 2FA en dispositivos no protegidos

Escenario

SAAS

PHISHING DE CREDENCIALES

Nunca ha sido más fácil

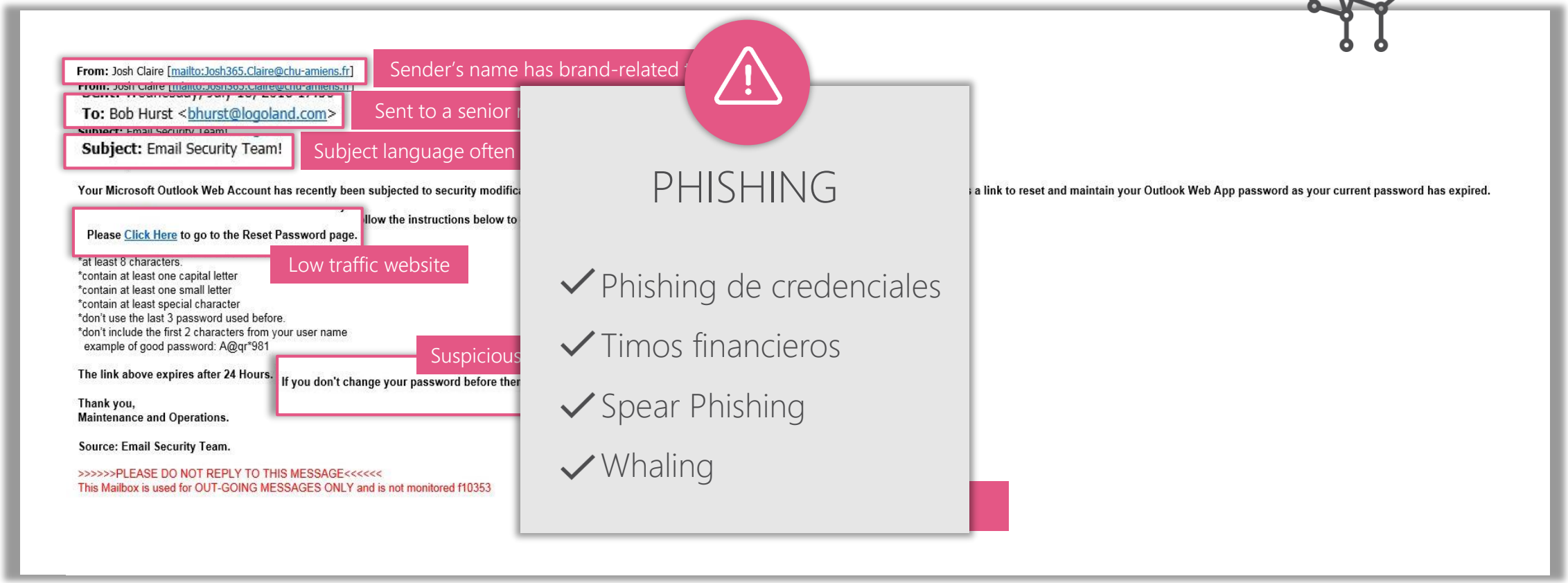


¿Cómo se ataca a las empresas?

Check Point
SOFTWARE TECHNOLOGIES LTD

- MALWARE
- PHISHING
- SECUESTRO DE CUENTAS

CLOUDGUARD SAAS
PHISHING PROTECTION



IDENTITY PROTECTION

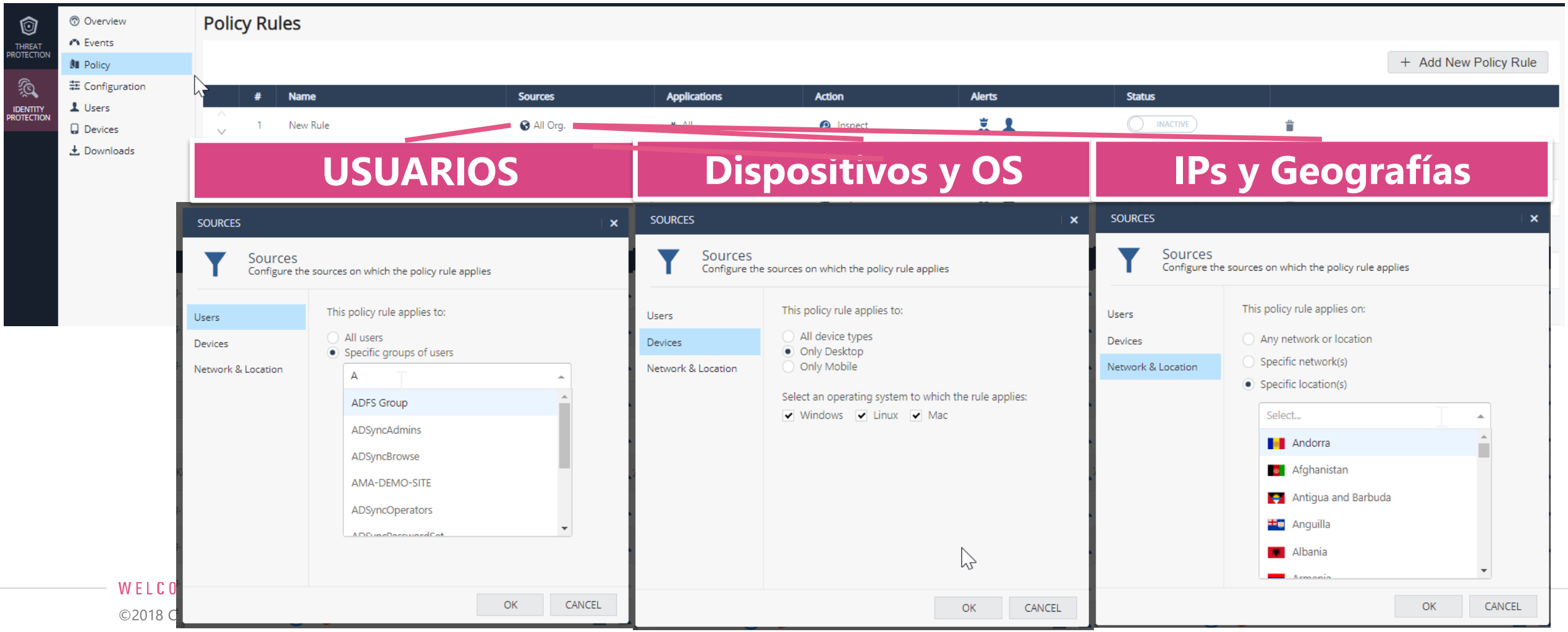
Eliminemos la amenaza principal en entornos SaaS con una autenticación fuerte

Prevenir secuestros de cuentas en cualqueir aplicación SaaS

- Despliegue con y sin agente
- Acceso condicional: por geografía, Ips, dispositivos, SO, etc..
- MFA centralizado
- Bloquear accesos desde dispositivos comprometidos.

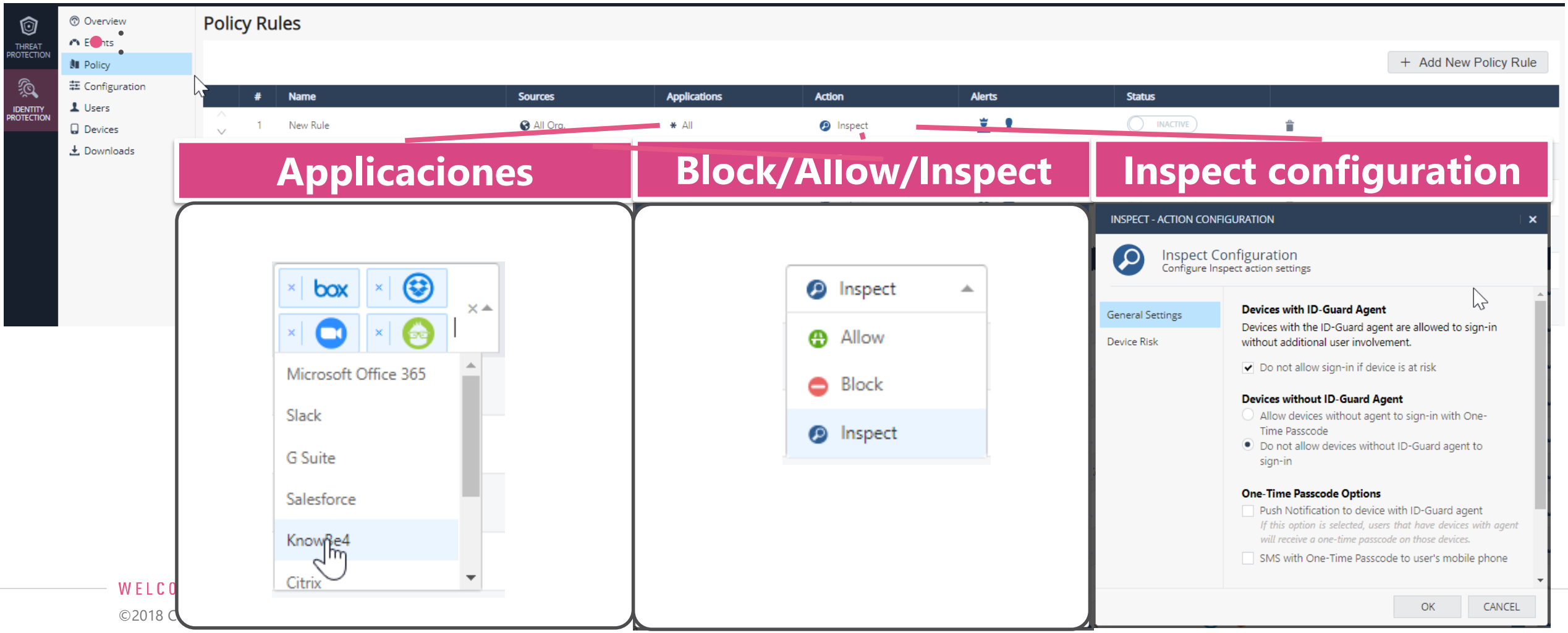
IDENTITY PROTECTION: Acceso condicional

- Limitar/Aprobar/Inspeccionar el acceso desde/a:



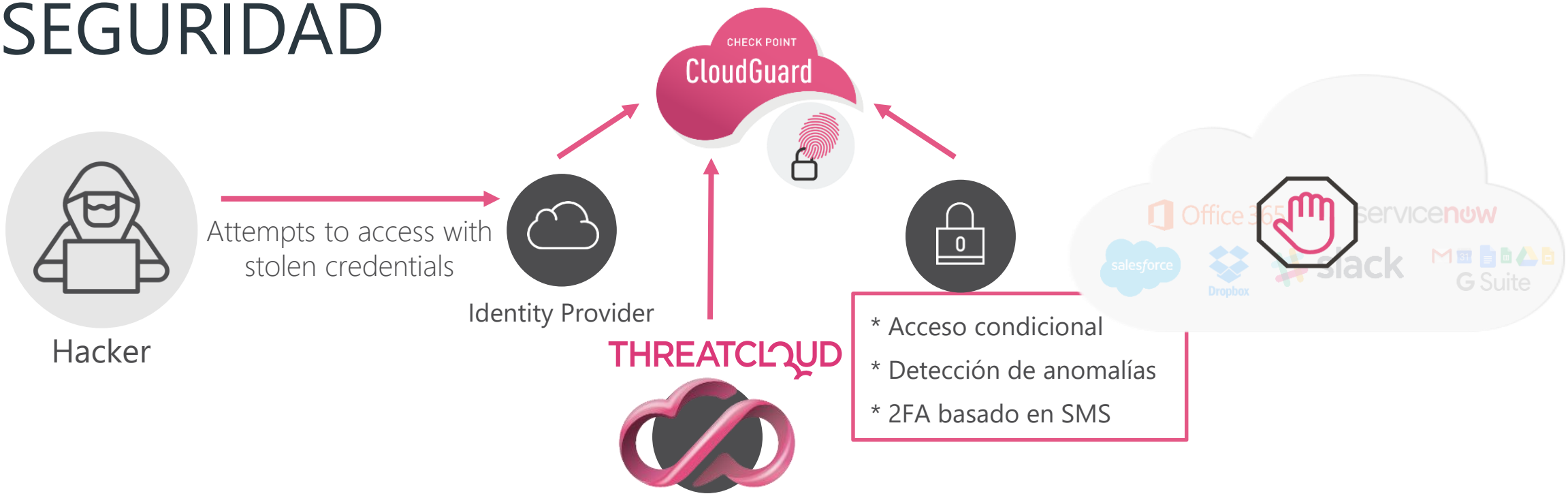
IDENTITY PROTECTION: ACCESO CONDICIONAL

- Limitar/Aprobar/Inspeccionar el acceso desde/a:



IDENTITY PROTECTION SIN AGENTE

DESPLIEGUE INSTANTÁNEO Y APROVECHANDO LA INTELIGENCIA DE SEGURIDAD



No es suficiente con 2FA

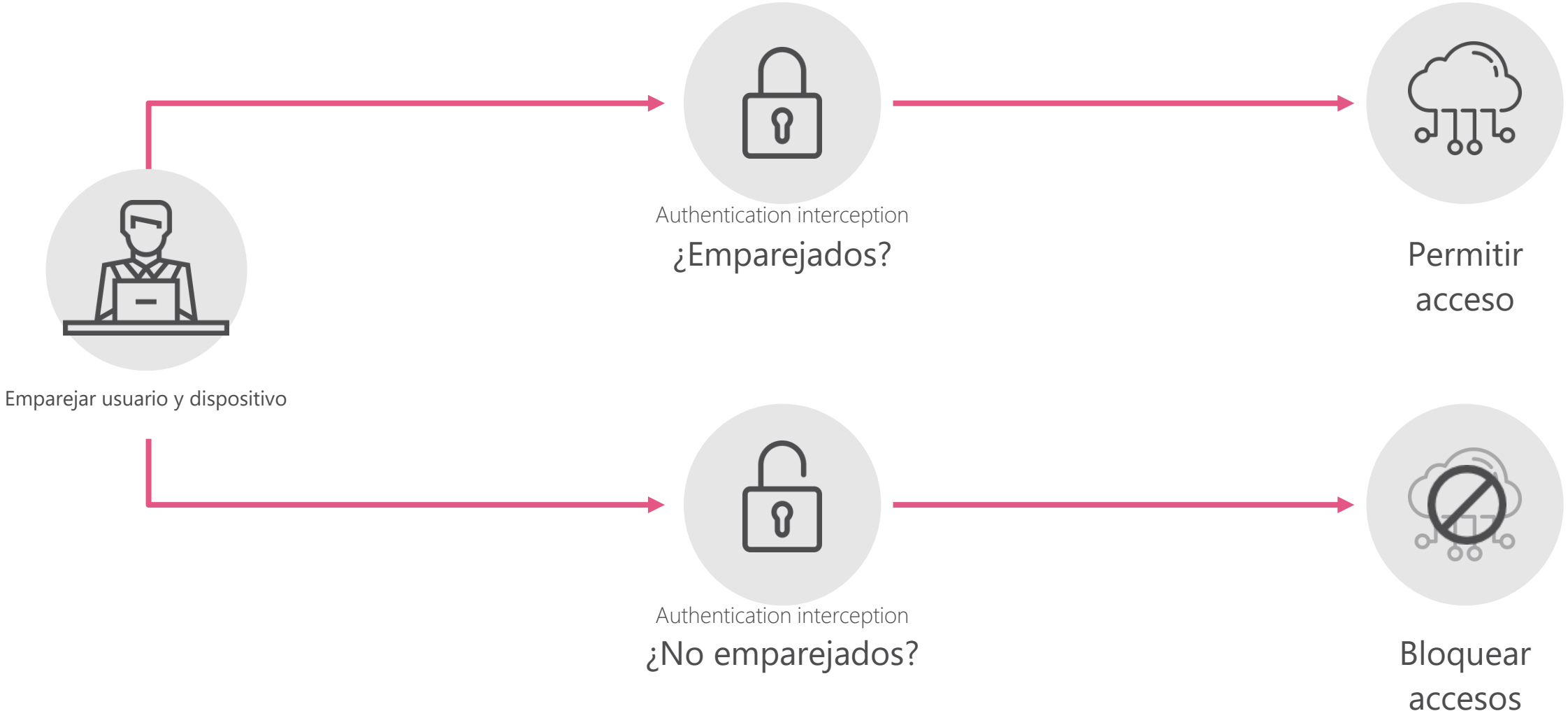
Lessons learned:

Se puede saltar el 2FA

Los dispositivos mobiles pueden tener amenazas y SMiShing

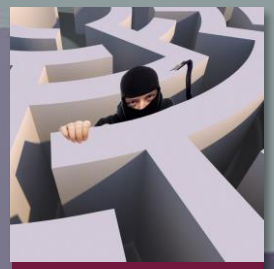
Se necesita: Visibilidad de la seguridad de los dispositivos

IDENTITY PROTECTION CON AGENTE



Escenario:

INFRAESTRUCTURA EN LA NUBE



Internal Risks

Check Point
SOFTWARE TECHNOLOGIES LTD.

Misconfigurations

Ejemplos:

- Configuracion de acceso a servicio demasiado permisivas
- Passwords débiles en usuarios administradores
- Desgobierno de servicios y uso de API

DARK Reading

Jun 1 2018 **10,000** businesses are affected by a widespread misconfiguration in Google Groups settings

Insider Threat

- Empeados maliciosos, descontentos.. Pueden aprovechar malas configuraciones para crear daños enormes.
- Un administrador con acceso a la cuenta root de un servicio cloud puede duplicar fácilmente la información en otros lugares.
- Las compañías guardan código Fuente en repositories externos como GitHub, con pocas o ninguna restricción de acceso.
- Un trabajador con acceso de alto nivel podría cargar software de minería de Bitcoin en la nube.

Dome9: control de la nube pública

- Visibilidad extensive en el entorno dinámico de la nube y los assets implicados. Gestión de los controles de seguridad nativos.
- Verificación de cumplimento, gobierno y regulaciones, solución (remediation) automática de fallos de configuración.
- Identity protection (IAM) : Previene acceso no autorizado y secuestro de cuentas.

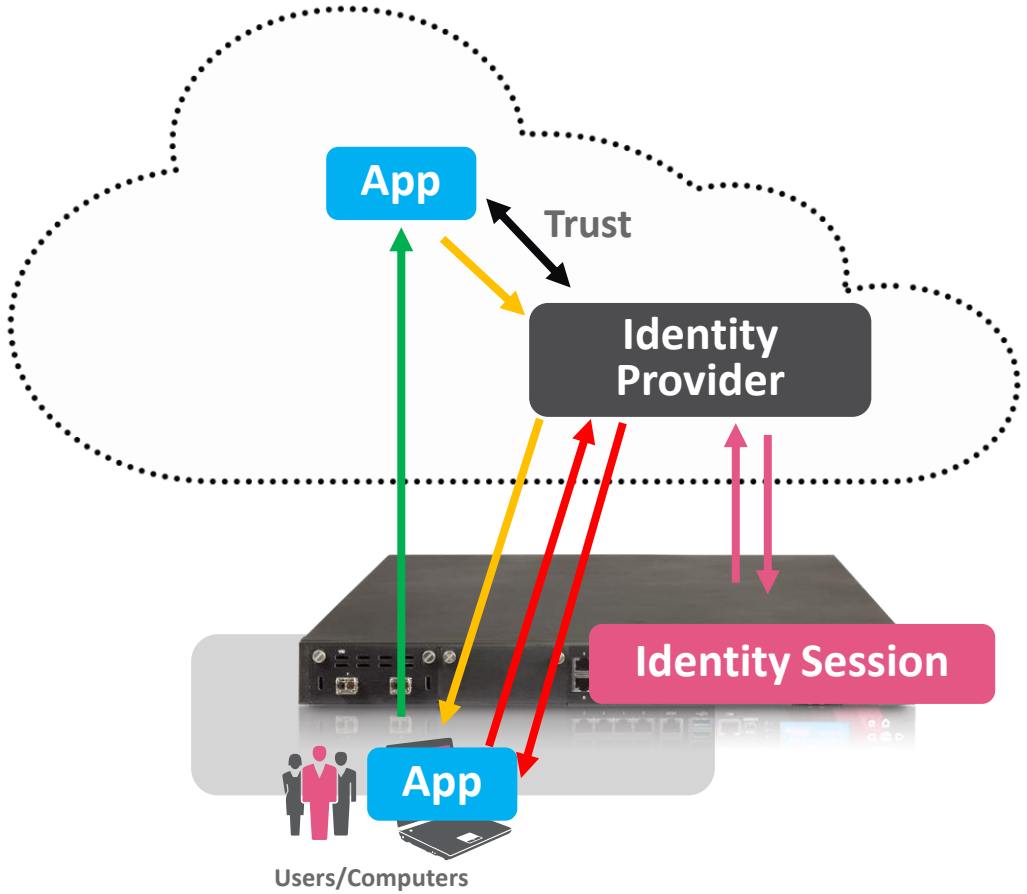
Escenario

ACCESO BASADO EN IDENTIDAD

Acceso basado en identidad – Zero Trust

- Consumo de aplicaciones basadas en la nube
- Consumo de aplicaciones internas con identity provider externos
- Adquisición de identidades (directorios locales o externos)
  - Con agente o no
  - Identidad de máquina
  - Cliente VPN
- y aplicación en la política de seguridad
  - Identidad
  - Aplicación
  - Contenido

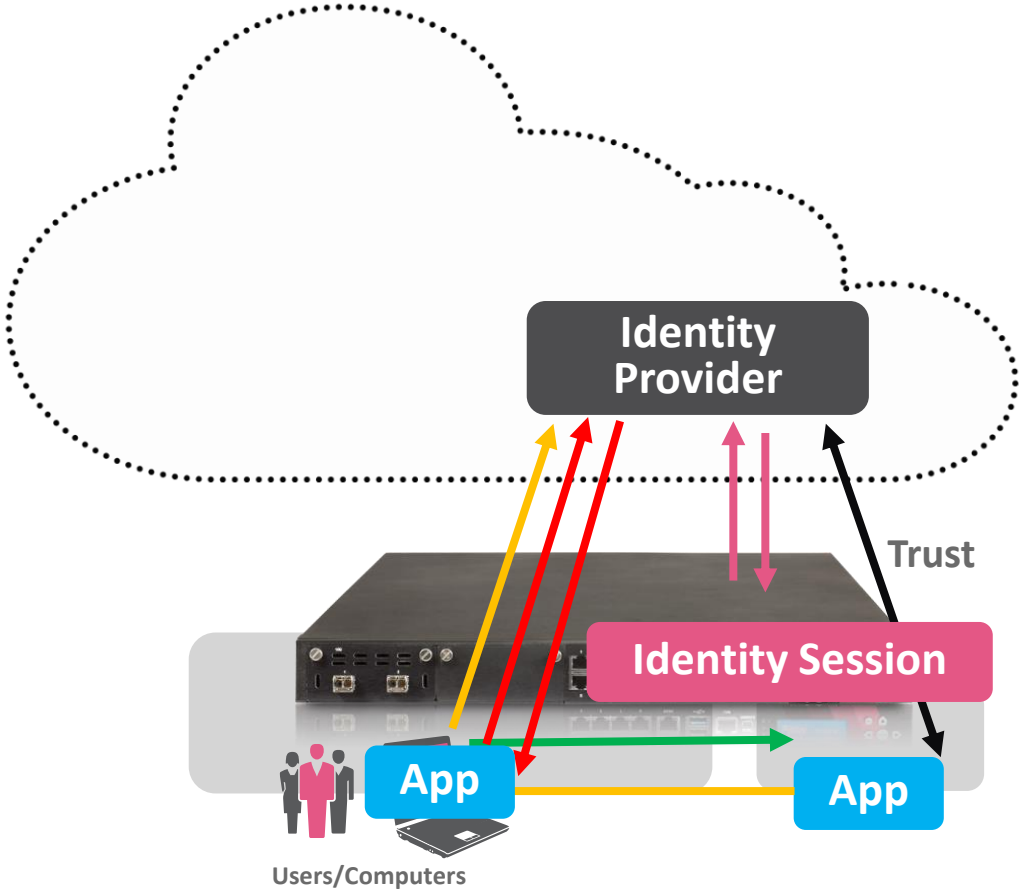
Consumo de aplicaciones basadas en la nube
Proveedor de identidad externo (trusted by app) (SAML)



https://app.domain.com

- La app confía en Identity Provider
- Accedemos al servicio cloud
- Redirigimos al servicio de autenticación
- Autenticación contra Identity Provider
  - Gateway participa en el proceso
    - En términos SAML terms: el **gateway es un Service Provider**
  - Identity Provider proporciona un 'token'
- Se genera una Identity Session
- Se permite acceso a la aplicación (según los términos de la política de seguridad del gateway)
- La aplicación verifica el 'token' y permite el servicio

Consumo de aplicaciones internas
Identity provider en la nube…



Política de seguridad integral

Protocolo y Aplicación

Contenido

Origen:

- **Red**
- **Usuarios**
- **Máquinas**
- **Clientes vpn**

DMZ (6-10)								
	Access to company's web server	ExternalZone	Web Server	Any	https	Any	Customer Service Ser	N/A
	Allow corporate LANs to DMZ	auth_users	DMZZone	Any	Adobe Flash-stream... SharePoint SharePoint-blog-po... SharePoint-calendar SharePoint-docume...	Any Direction Spreadshe... Markup File Document...	Accept	Log Accounting
	Public FTP Access	Any	Public FTP Server	Any	Any	Any	Public FTP Layer	N/A
	Proxy Web access	Proxy Server	Any	Any	Web	Any	Accept	Log
	External mail traffic	Mail Relay	Any	Any	smtp SMTPS	Any	Accept	Log
Data Center Access (11-12)								
11	RDP Exceptions	Any	Any	Any	Remote_Desktop_Pr... Remote_Desktop_Pr...	Any	RDP Exceptions Laye	N/A
12	Policy for access to Data Center servers	Any	Data Center LAN	Any	Any	Any	Data Center Layer	N/A

Resumen

- Identidad como factor fundamental de la seguridad
- 2FA no es suficiente
- Gestión integral de la política y la identidad

GRACIAS