



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

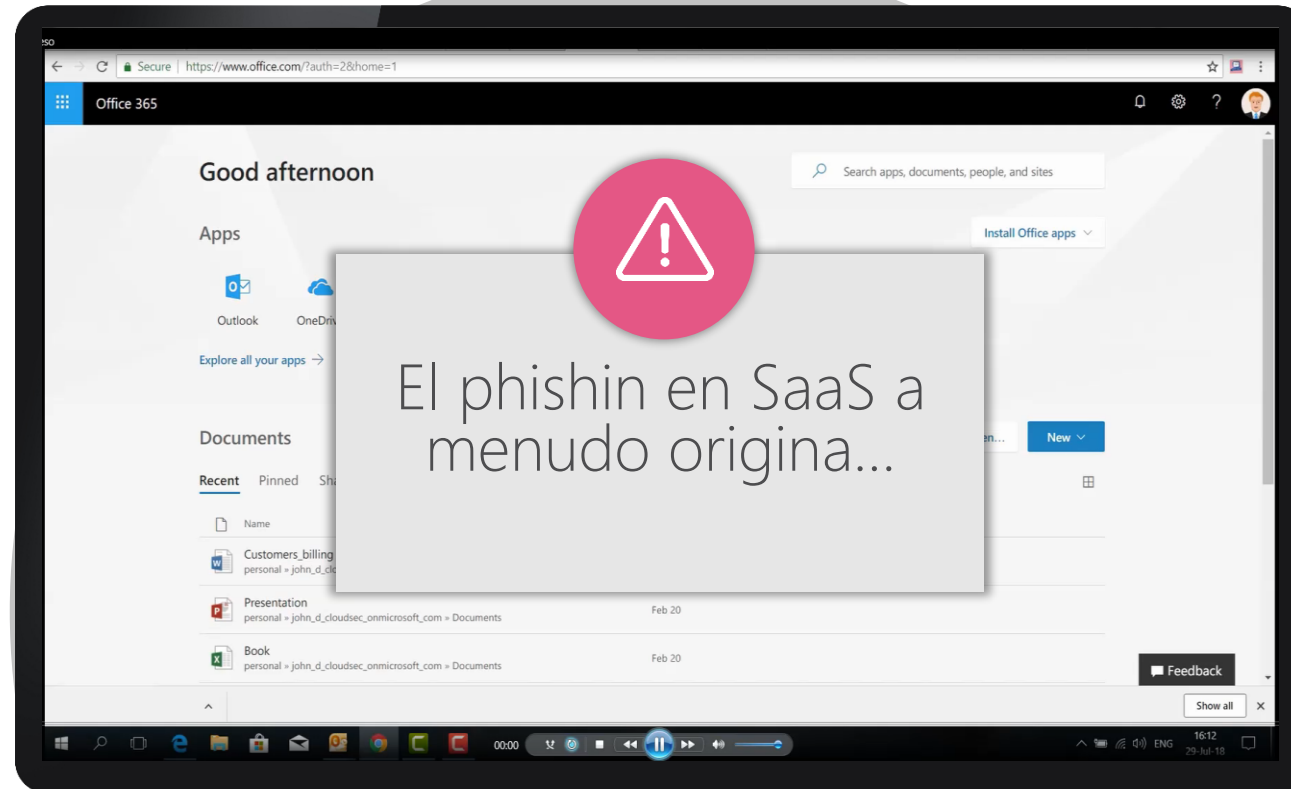
SAAS

15/12/11 SEARCH...A01



PHISHING DE CREDENCIALES

Nunca ha sido más fácil





¿Cómo se ataca a las empresas?



MALWARE



PHISHING



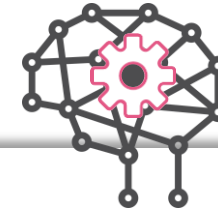
SECUESTRO DE CUENTAS

USER *****

PASS *****



CLOUDGUARD SAAS PHISHING PROTECTION



From: Josh Claire [mailto:Josh365.Claire@chu-amiens.fr]

Sender's name has brand-related



To: Bob Hurst <bhurst@logoland.com>

Sent to a senior

Subject: Email Security Team!

Subject language often

Your Microsoft Outlook Web Account has recently been subjected to security modifications.

Click here to go to a link to reset and maintain your Outlook Web App password as your current password has expired.

Please [Click Here](#) to go to the Reset Password page.

Follow the instructions below to

Low traffic website

- *at least 8 characters.
- *contain at least one capital letter
- *contain at least one small letter
- *contain at least special character
- *don't use the last 3 password used before.
- *don't include the first 2 characters from your user name
- example of good password: A@q*981

Suspicious

The link above expires after 24 Hours.

If you don't change your password before then

Thank you,
Maintenance and Operations.

Source: Email Security Team.

>>>>>PLEASE DO NOT REPLY TO THIS MESSAGE<<<<<<

This Mailbox is used for OUT-GOING MESSAGES ONLY and is not monitored f10353

PHISHING

- ✓ Phishing de credenciales
- ✓ Timos financieros
- ✓ Spear Phishing
- ✓ Whaling



IDENTITY PROTECTION



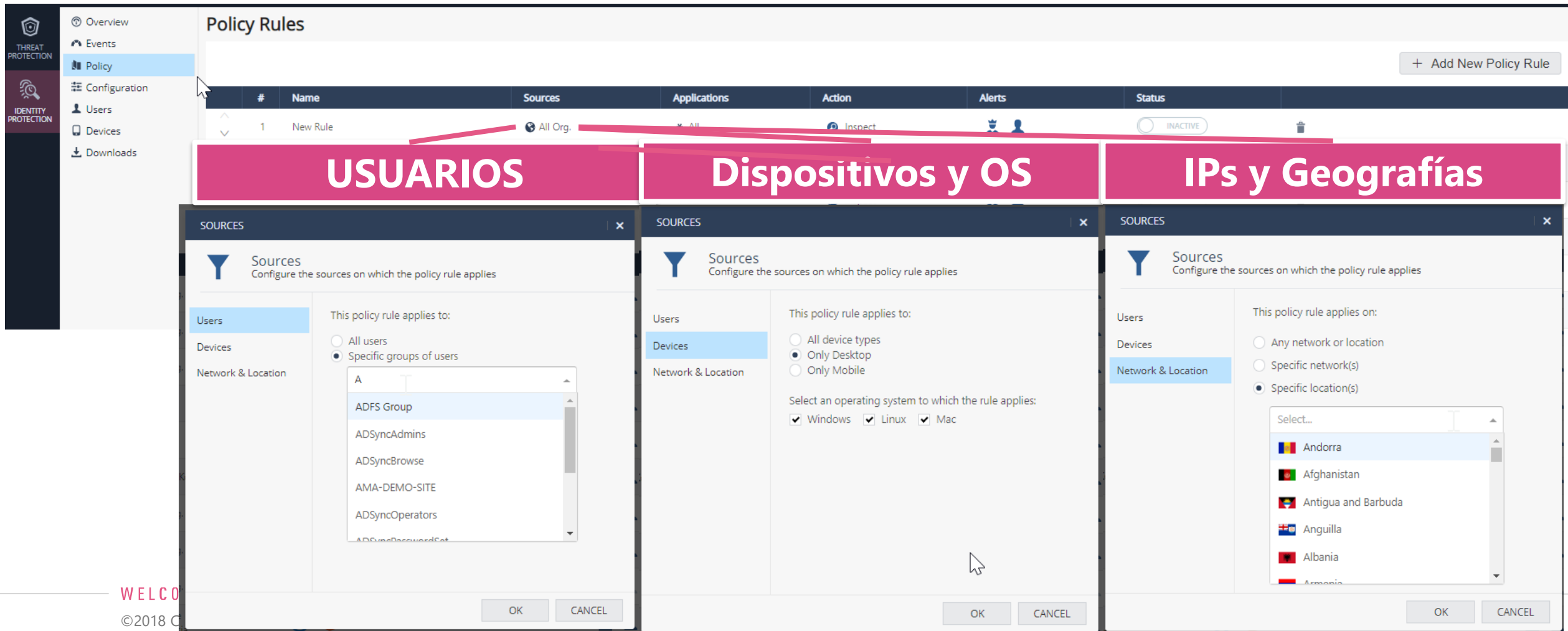
Eliminemos la amenaza principal en entornos SaaS con una autenticación fuerte

Prevenir secuestros de cuentas en cualquier 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:



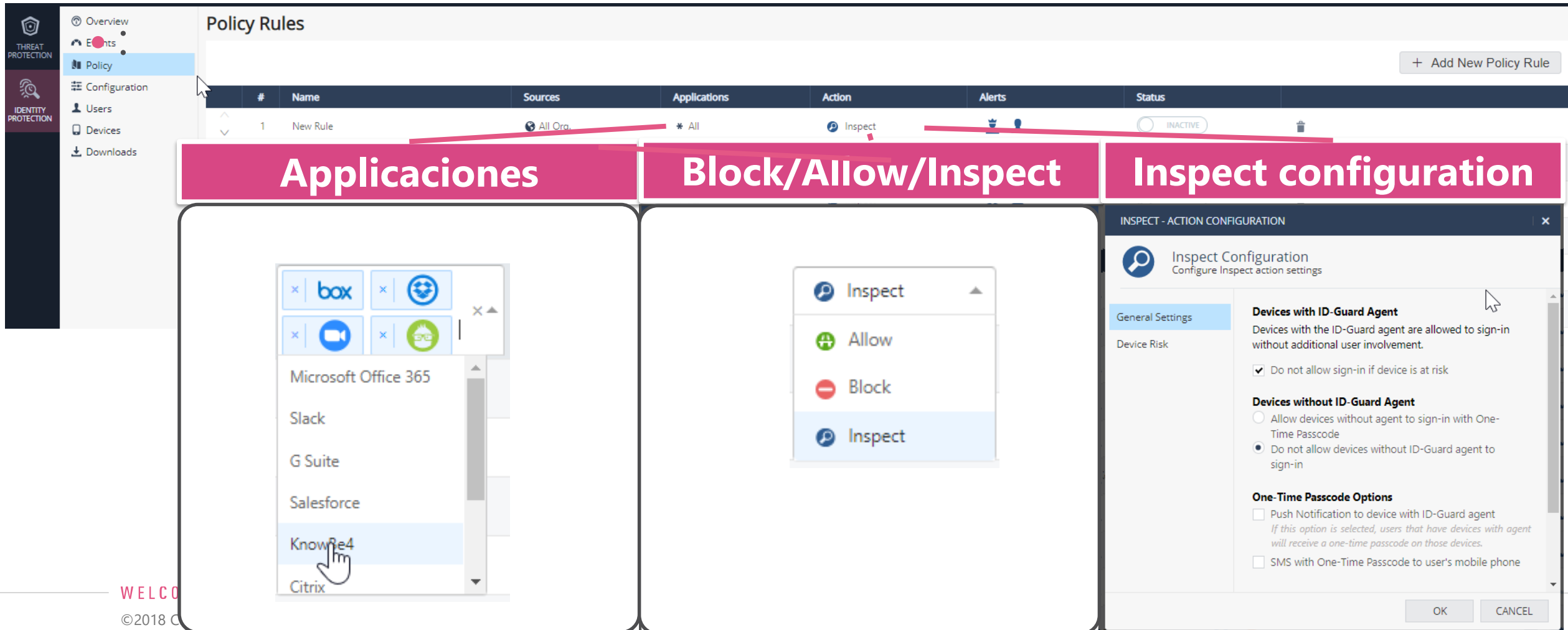
The screenshot displays the 'Policy Rules' configuration page in the Check Point Identity Protection console. The main table lists a 'New Rule' with columns for #, Name, Sources, Applications, Action, Alerts, and Status. Three modal windows are overlaid on the table, each with a pink header:

- USUARIOS**: This modal window is for configuring the 'Sources' column. It shows options for 'Users' (All users or Specific groups of users) and a list of groups including ADFS Group, ADSyncAdmins, ADSyncBrowse, AMA-DEMO-SITE, ADSyncOperators, and ADSyncPasswordSet.
- Dispositivos y OS**: This modal window is for configuring the 'Sources' column. It shows options for 'Devices' (All device types, Only Desktop, or Only Mobile) and checkboxes for operating systems: Windows, Linux, and Mac.
- IPs y Geografías**: This modal window is for configuring the 'Sources' column. It shows options for 'Network & Location' (Any network or location, Specific network(s), or Specific location(s)) and a list of countries including Andorra, Afghanistan, Antigua and Barbuda, Anguilla, Albania, and Armenia.

Each modal window has 'OK' and 'CANCEL' buttons at the bottom.

IDENTITY PROTECTION: ACCESO CONDICIONAL

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

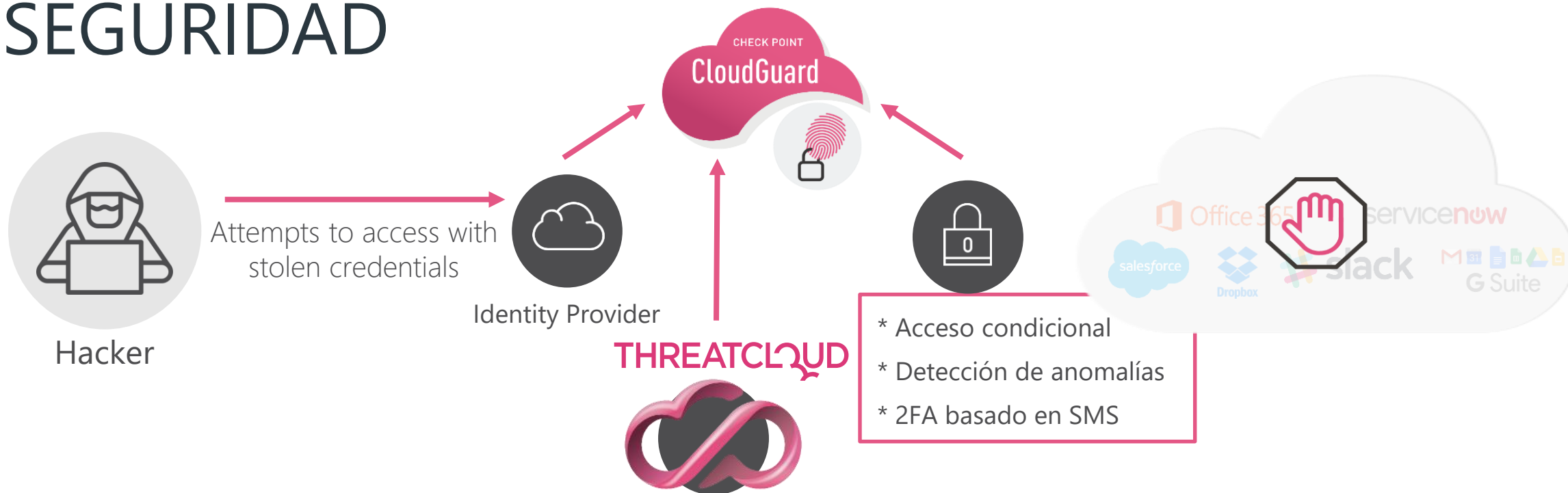


The screenshot displays the 'Policy Rules' configuration page in the Check Point Identity Protection console. The left sidebar shows navigation options: Overview, Events, Policy (selected), Configuration, Users, Devices, and Downloads. The main area shows a table with one rule named 'New Rule'. Below the table, three callout boxes highlight key configuration steps:

- Aplicaciones:** A list of applications is shown, with 'KnowRe4' selected. Other visible applications include box, Slack, G Suite, Salesforce, and Citrix.
- Block/Allow/Inspect:** A dropdown menu shows the action 'Inspect' selected.
- Inspect configuration:** The 'INSPECT - ACTION CONFIGURATION' dialog is open, showing settings for 'Devices with ID-Guard Agent' and 'Devices without ID-Guard Agent'. The 'Do not allow sign-in if device is at risk' option is checked under the 'Devices with ID-Guard Agent' section.



IDENTITY PROTECTION SIN AGENTE DESPLIEGUE INSTANTÁNEO Y APROVECHANDO LA INTELIGENCIA DE SEGURIDAD





No es suficiente con 2FA



Lessons learned:

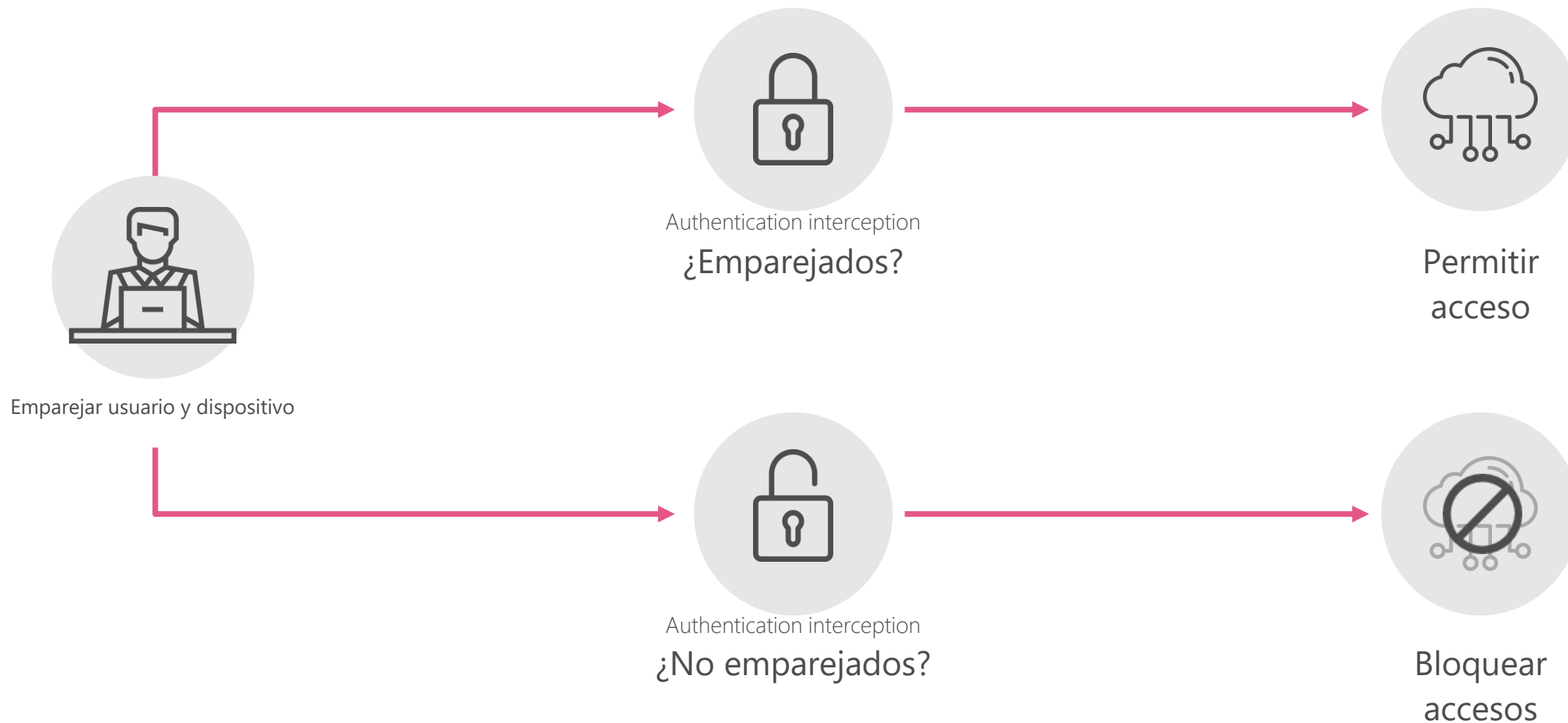
—
Se puede saltar el
2FA

—
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

15/11/2011 SEARCH...A01



Misconfigurations

Ejemplos:

- Configuración 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



Internal Risks



Internal Risks



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 extensiva en el entorno dinámico de la nube y los assets implicados. Gestión de los controles de seguridad nativos.
- ▶ Verificación de cumplimiento, 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

15/11/2011 SEARCH...A01

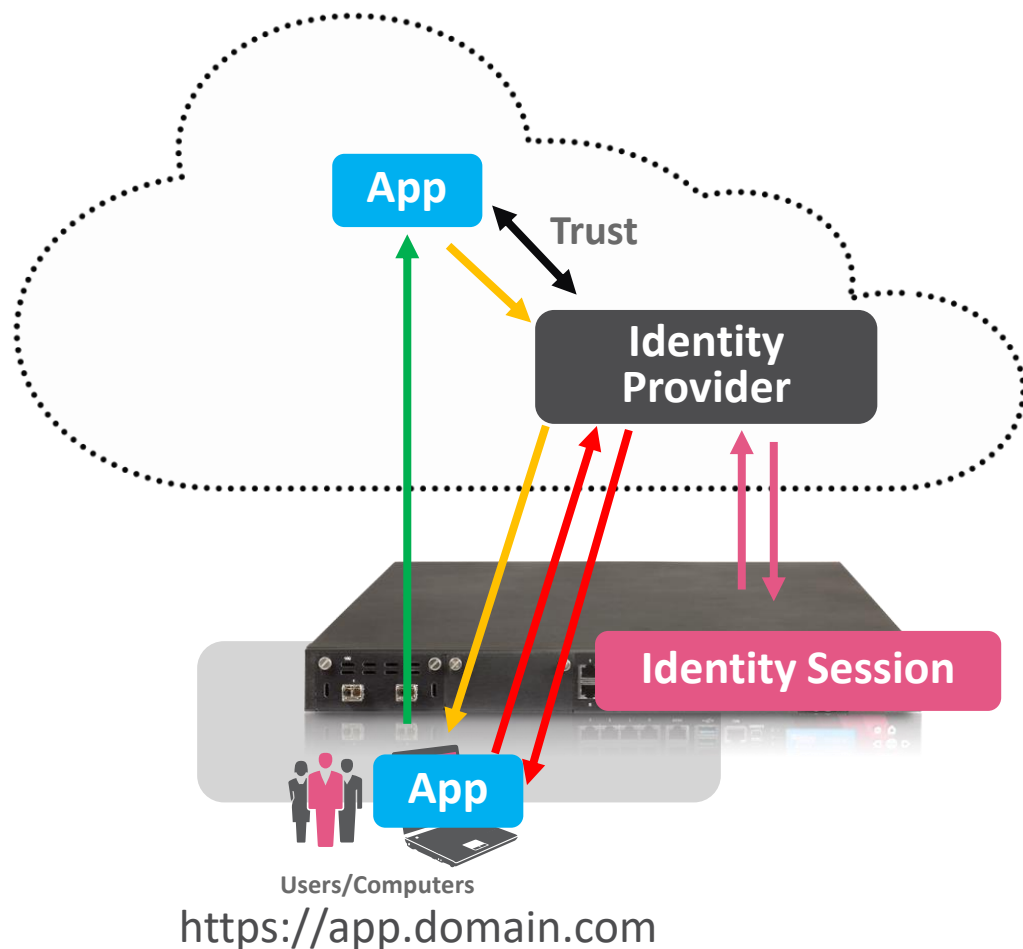
Acceso basado en identidad – Zero Trust

- 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

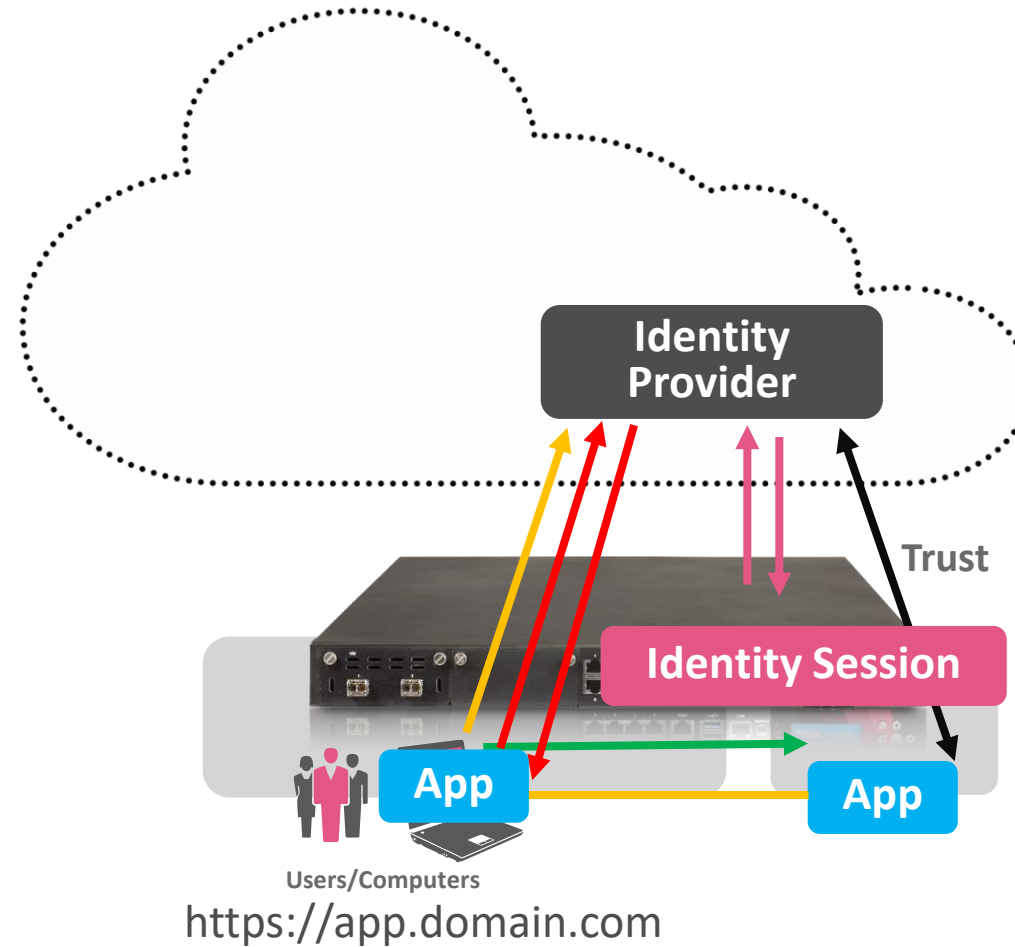
Proveedor de identidad externo (trusted by app) (SAML)



- 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	<ul style="list-style-type: none"> Adobe Flash-stream... SharePoint SharePoint-blog-po... SharePoint-calendar SharePoint-docume... 	<ul style="list-style-type: none"> 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	* Any	Accept	Log		
				SMTPS					
Data Center Access (11-12)									
11	RDP Exceptions	* Any	* Any	* Any	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



Check Point[®]
SOFTWARE TECHNOLOGIES LTD

GRACIAS

