

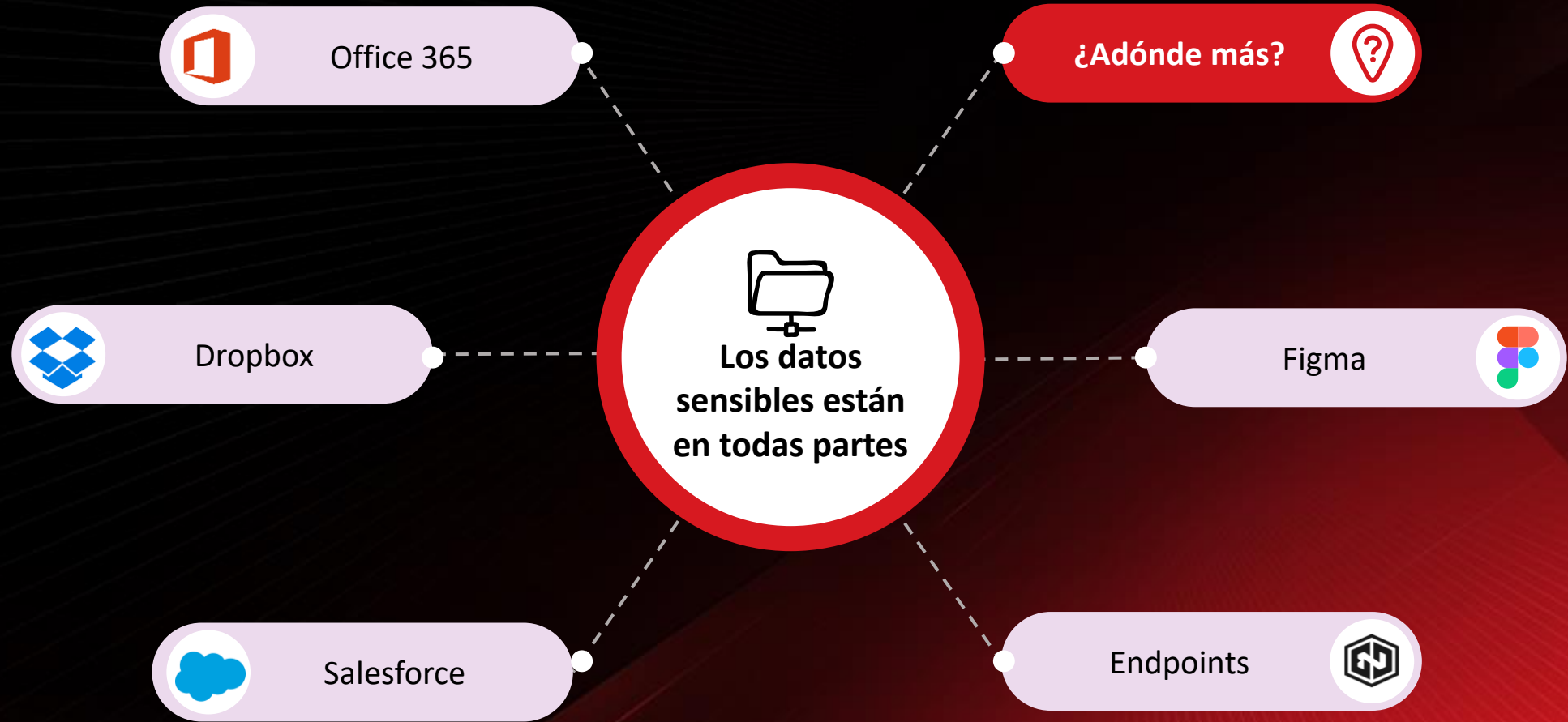
Zero Trust™



¿Por qué se ha convertido en una necesidad?



¿Por qué se ha convertido en una necesidad?



¿La solución? Zero Trust

¿Por qué se ha convertido en una necesidad?

El enfoque perimetral ya no es suficiente.



Falta visibilidad del comportamiento de los usuarios.

“¿Dónde están mis datos?”

“¿Están seguros mis datos?”

Evolución de la confianza: nunca confíes, verifica siempre



Estado anterior

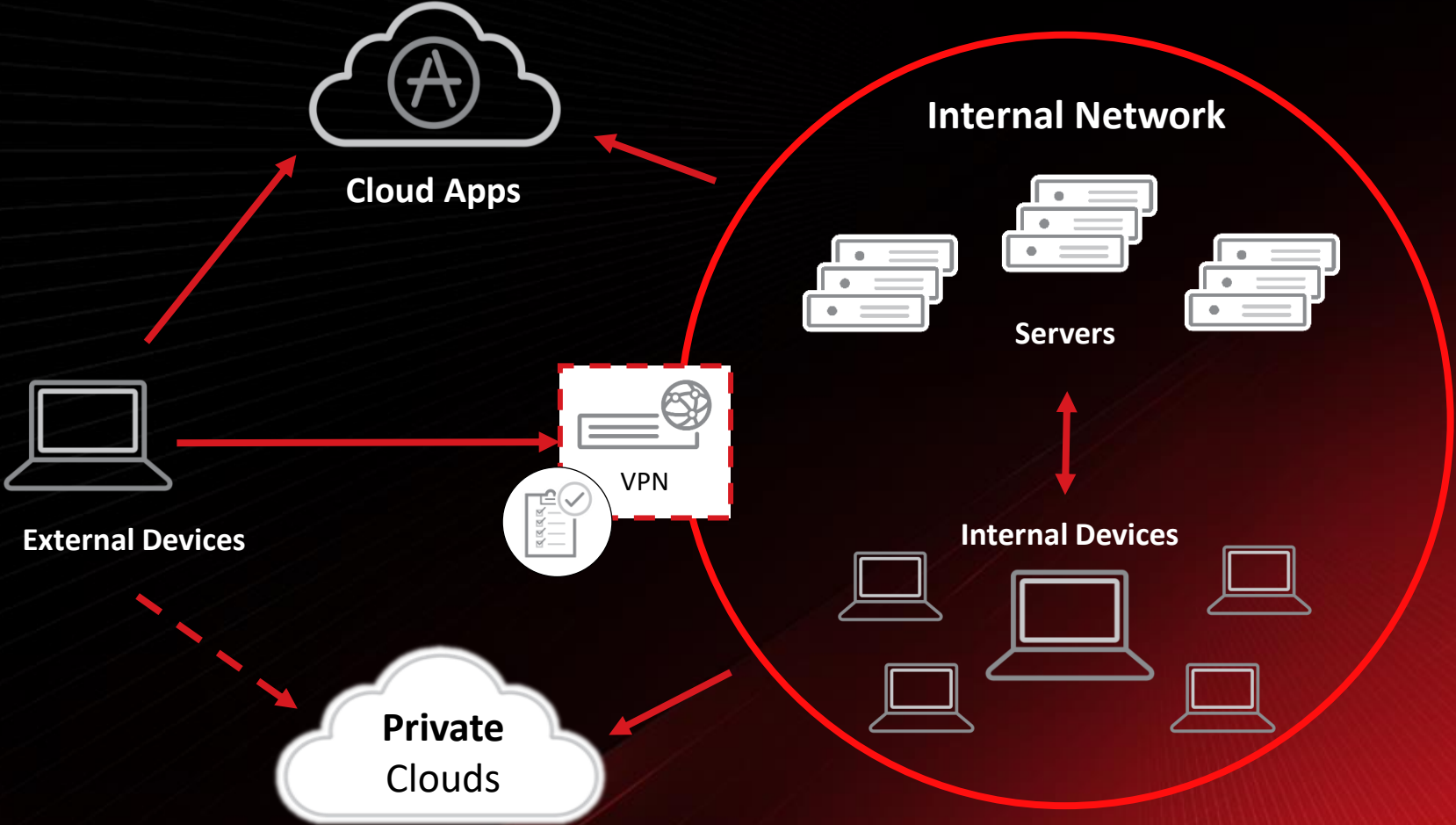
- A los usuarios y a los terminales se les permite automáticamente el acceso a la red y a Internet.



Zero Trust

- El acceso está restringido hasta que se verifican la identidad y el dispositivo.
- A continuación, utilice la evaluación continua durante la sesión para determinar si debe seguir concediéndose el acceso.

Antes de Zero Trust



Puesta en práctica de Zero Trust



Defina tu Superficie de Ataque



Evalúe su riesgo



Implementar la Autenticación Multifactor



Segmente su red



Monitore y detecte



Evaluar y ajustar continuamente



Acceso remoto seguro

Habilitar y proteger hybrid workforce

-  Complete Attack Surface Discovery
-  Continuous Risk Assessments
-  Least Privilege Access (Static Rules)
-  Conditional Access Based on Dynamic Rules

SERVIDORES (FÍSICOS O VIRTUALES) O APLICACIONES NATIVAS EN LA NUBE



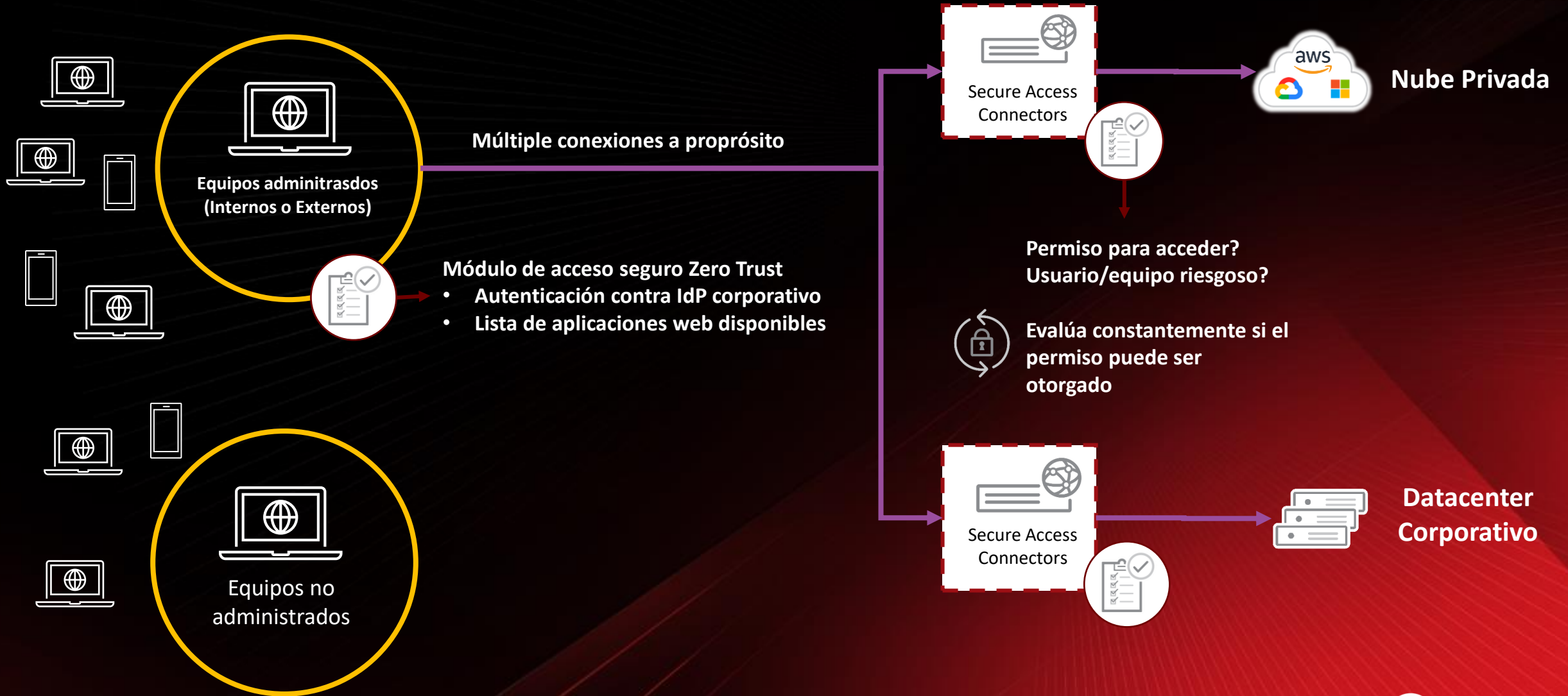
INTERNET ACCESS



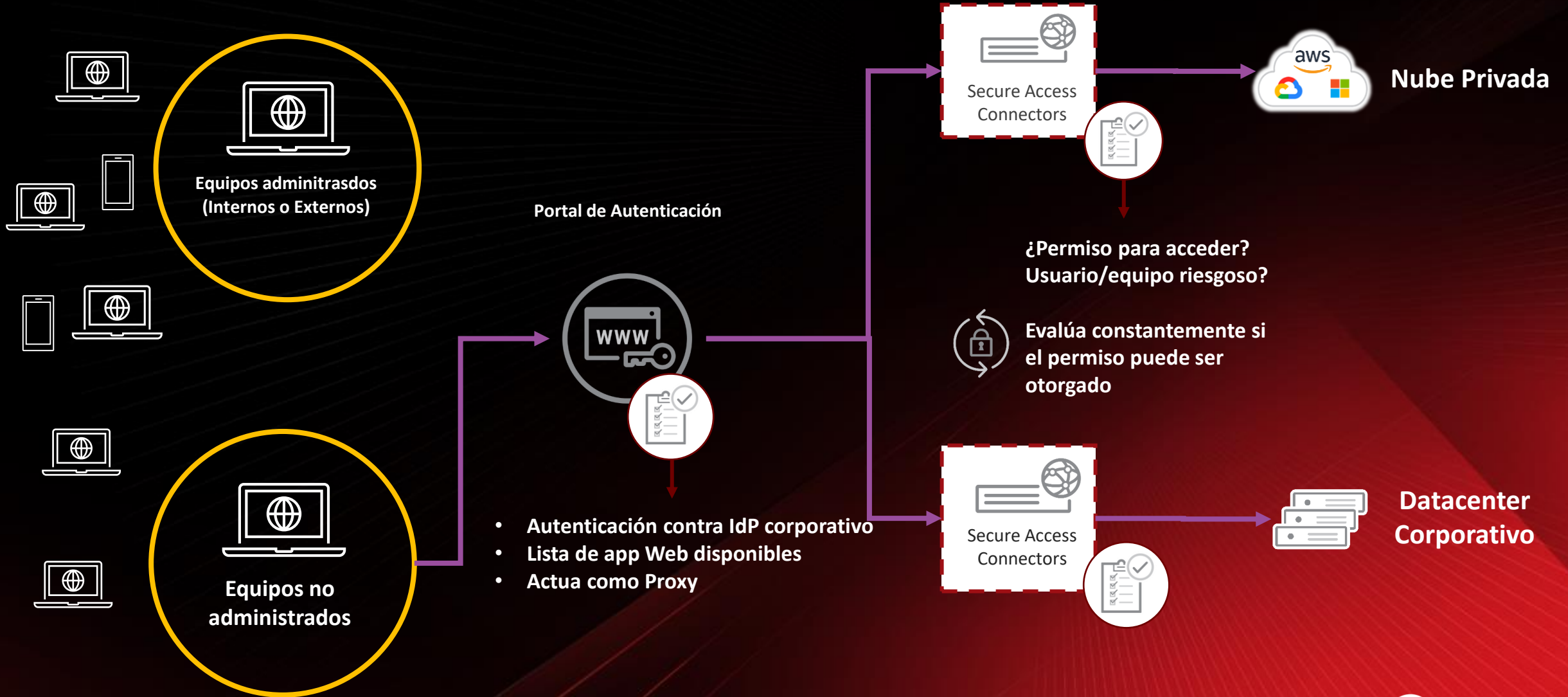
INTERNOS O DISPOSITIVOS EXTERNOS

 Zero Trust Secure Access

Private Access: Transform your remote access solution



Private Access: Transform your remote access solution



Internet Access: Deliver fast and secure access to cloud apps

Managed Devices



Secure Web Gateway



Web Sites & SaaS Apps



Unmanaged Devices



Using a Proxy Auto Config (PAC) file

Corporate Network

Mix of Managed and Unmanaged Devices



Optional On-Premises Web Gateway



Permission to access?
Is user/device risky?




Constantly assess if access
should be granted.

Modernizing with ZTNA

Zero Trust Network Access	Traditional VPN
Dynamic access control, continuous monitoring	Has no monitoring after login
One-to-many tunnel	One-to-one tunnel
Secure Access Connectors are invisible from the Internet	VPN concentrator is publicly accessible
Access restricted to pre-defined applications	Open to the whole network
Easy deployment with a virtual appliance	Hardware needed, sometimes with complex ACL/firewall settings
Easily scalable with connector grouping	Hard to increase capacity
Only domain name for pre-defined apps can be resolved	All DNS records are exposed
The internal IP addresses of applications are disguised with CGNAT IP addresses	Real internal IP addresses are visible to the end user

Built to enable Zero Trust



-  Complete Attack Surface Discovery
-  Continuous Risk Assessments
-  Least Privilege Access (Static Rules)
-  Conditional Access Based on Dynamic Rules

Managed Services

Attack Surface Risk Management
Discover Attack Surface • Assess Risk • Mitigate Risk

Zero Trust Architecture

Extended Detection and Response (XDR)

- User and Identity
- Endpoints and Servers
- Email
- Cloud Infra
- Applications
- Code Repo
- Data
- Network
- 5G
- ICS/OT

Email Security

Endpoint Security

Cloud Security

Network Security

OT Security

Orchestration and Automation

Global Threat Intelligence

Attack Surface Intelligence | Zero Day Initiative | Threat Research | AI/ML | Big Data Analytics

Platform Foundations

Multi-Tenancy | Role-Based Access Control | Single Sign-On | Policy Decision Point

Ecosystem Integration





¡Muchas gracias!