Govern d'Andorra

ANDORRA DIGITAL

ANC AD

2ª Jornada CISO

ZERO TRUST

Juan Carlos Romero

1 de Març de 2024

Redefiniendo la seguridad: ¿Por qué Zero Trust es crucial en el entorno dinámico actual?

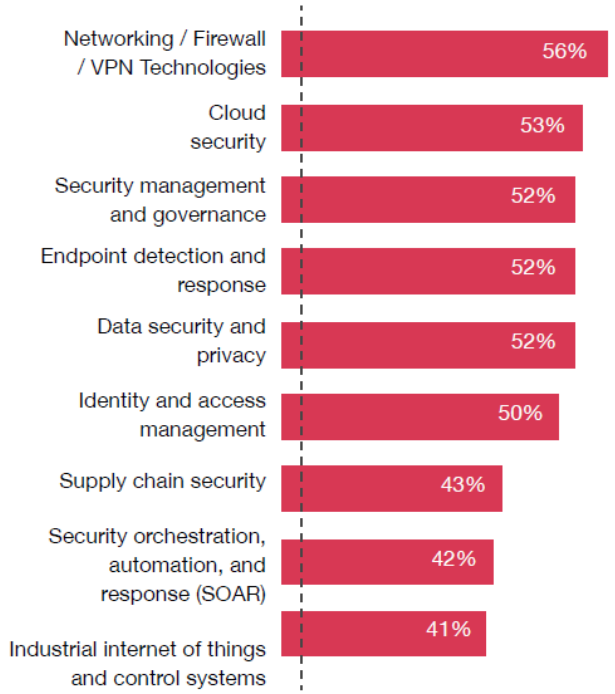
Everything is connected, including cyber attacks

Top cyber threats over the next 12 months

Q3. Over the next 12 months, which of the following cyber threats is your organisation most concerned about? (Ranked in top three).
Base: All respondents=3876
Source: PwC, 2024 Global Digital Trust Insights.

Only half are satisfied with their cyber-tech capabilities

Organisation's technology capabilities in key cybersecurity areas



Only 5% of security and IT respondents are very satisfied across all areas

Q23. How satisfied are you with your organisation's technology capabilities in the following areas? Base: Security and IT respondents= 1517
Source: PwC, 2024 Global Digital Trust Insights.

Desafíos de seguridad en redes – Perspectiva de las parte interesadas

CIO

- Seguridad de la red y acceso remoto
- Agilidad empresarial
- Eficiencia y reducción de costes
- Transformación digital en TI y seguridad

CISO

- Falta de cumplimiento y gobernanza de la seguridad de la información en general.
- Controles de acceso con privilegios mínimos limitados.
- Incapacidad para aplicar análisis y corrección de amenazas en tiempo real.
- Incapacidad para escalar rápidamente la arquitecturas de seguridad para satisfacer la satisfacer las necesidades.

Equipo de seguridad

- Incapacidad para aplicar controles de acceso granulares.
- Aplicación engorrosa de políticas
- Incapacidad para proporcionar seguridad PIM
- Esfuerzo manual para validar y revisar los controles.
- Incapacidad para definir políticas de acceso basadas en el contexto.

Requisitos

Identidad del usuario y dispositivo

- Proporcionar a los usuarios acceso seguro y autorizado desde cualquier lugar.
- Identificar el comportamiento de los usuarios/dispositivos en la red

Acceso condicional

- Conceder acceso basado en el principio del menor privilegio.
- Habilitar la monitorización en tiempo real y la automatización de la detección y respuesta a amenazas.

Segmentación de red

- Restringir la propagación de software malicioso entre los CPDs y entornos Cloud.
- Reducir el tiempo de respuesta ante ataques aprovechando las capacidades de microsegmentación

¿Por qué tenemos que cambiar el enfoque de la seguridad?

Una arquitectura basada en Zero Trust ayuda a prevenir los ataques relacionados con las nuevas amenazas.

1 **Compromiso de terceros**

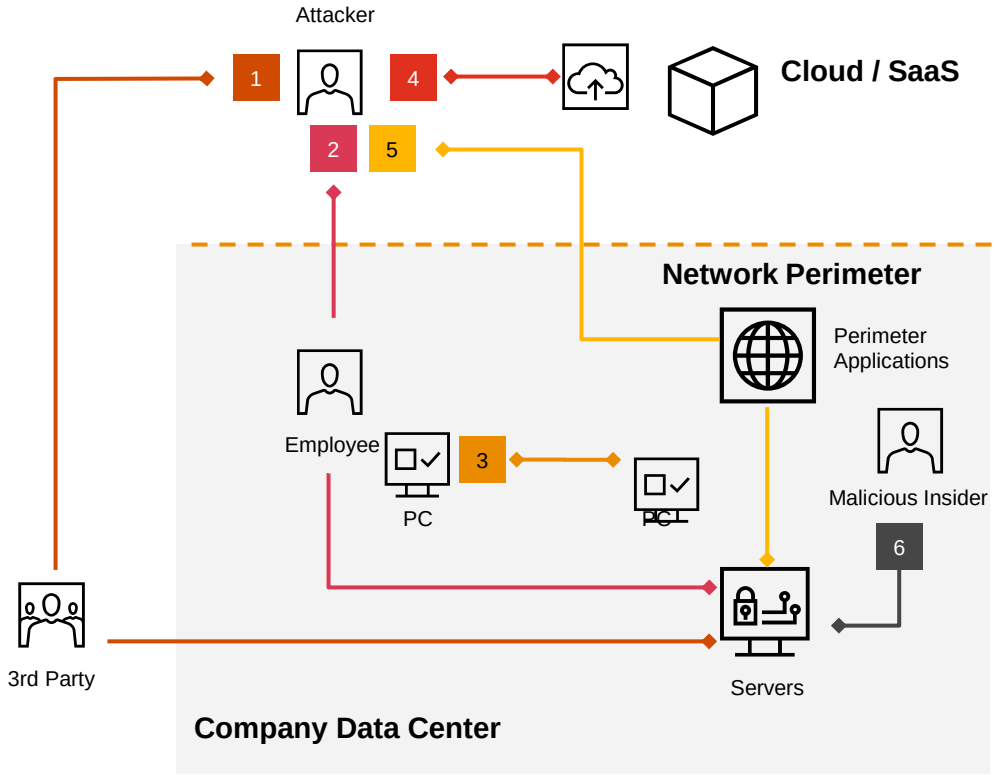
Los atacantes utilizan credenciales robadas de un tercero de **confianza**, saltándose los controles del perímetro.

2 **Ingeniería Social**

Los atacantes utilizan el *spear-phishing* y la ingeniería social para pasar atravesar el perímetro, ya que los empleados internos son de **confianza**.

3 **Ransomware**

El malware se propaga a través de la red debido a la falta de segmentación. Todos los equipos internos **confían** entre sí.



4 **Exposición de datos en la nube**

Los datos son robados debido a que el perímetro de la nube no está debidamente protegido. El servidor de BD alojado en la nube **confía** en las peticiones de otros servidores.

5 **Movimiento Lateral**

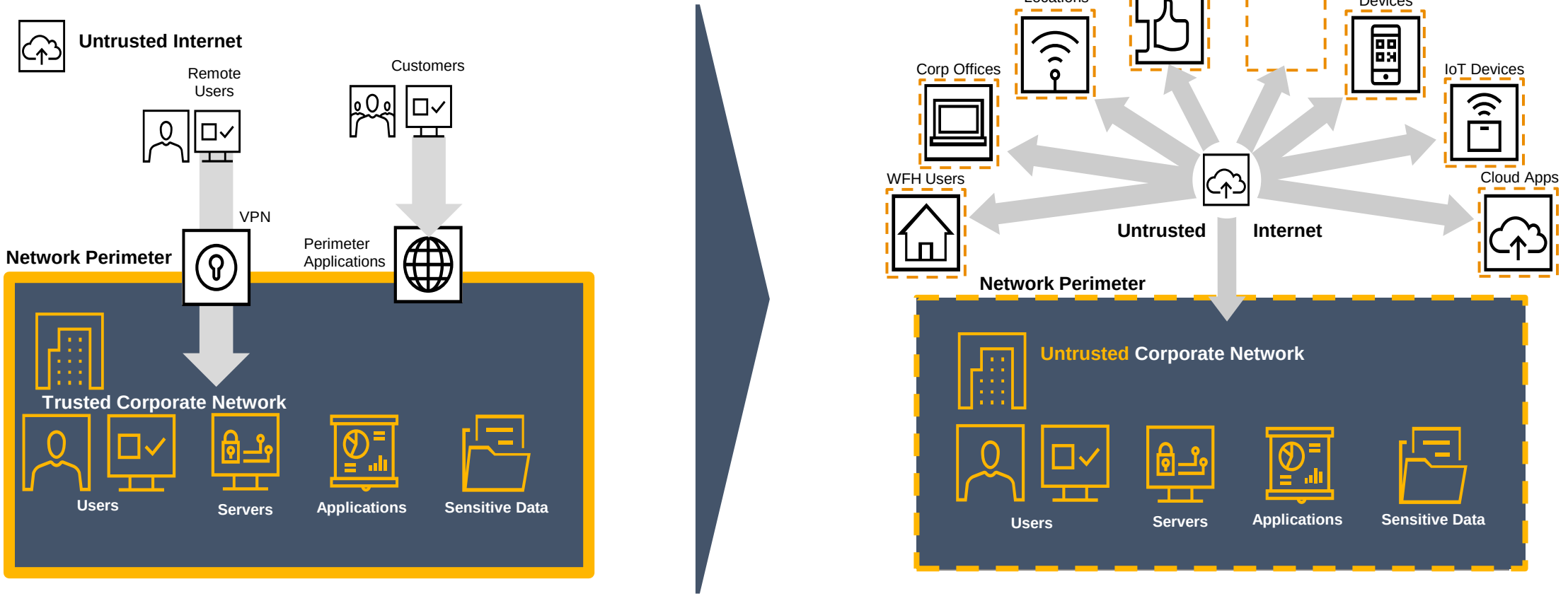
Los atacantes comprometen un servidor web vulnerable de cara al exterior y luego se mueven lateralmente dentro del centro de datos porque el servidor web es de **confianza**.

6 **Amenazas internas**

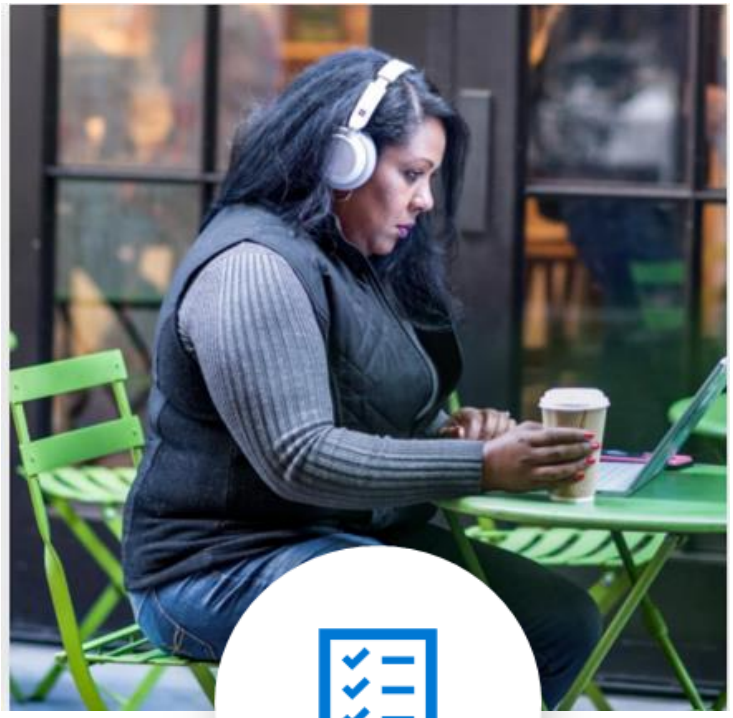
Los informantes maliciosos se aprovechan de su derecho a la **confianza** y del acceso privilegiado para hacer cosas que no deberían hacer.

¿Por qué tenemos que cambiar el enfoque de la seguridad?

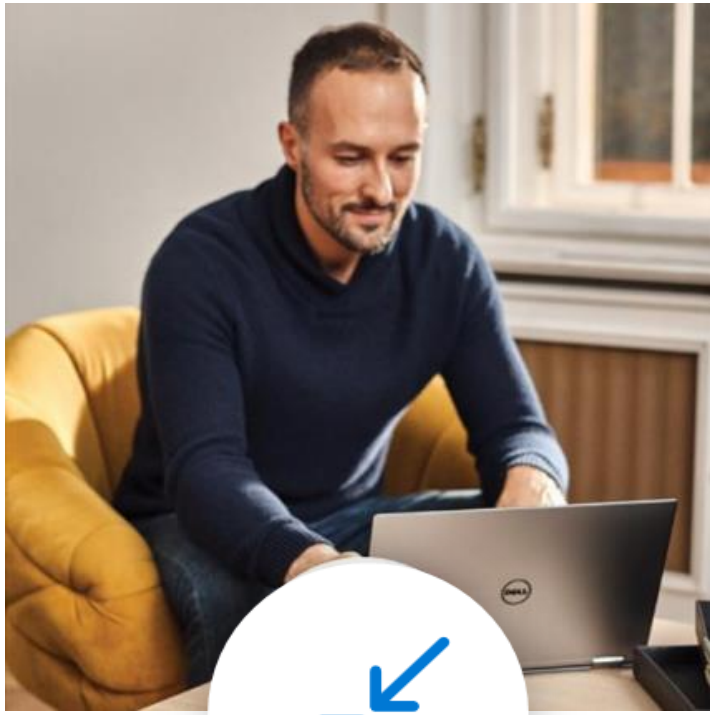
Permitir el acceso seguro a los recursos y datos desde cualquier lugar tomando decisiones en tiempo real basadas en el riesgo y el contexto.



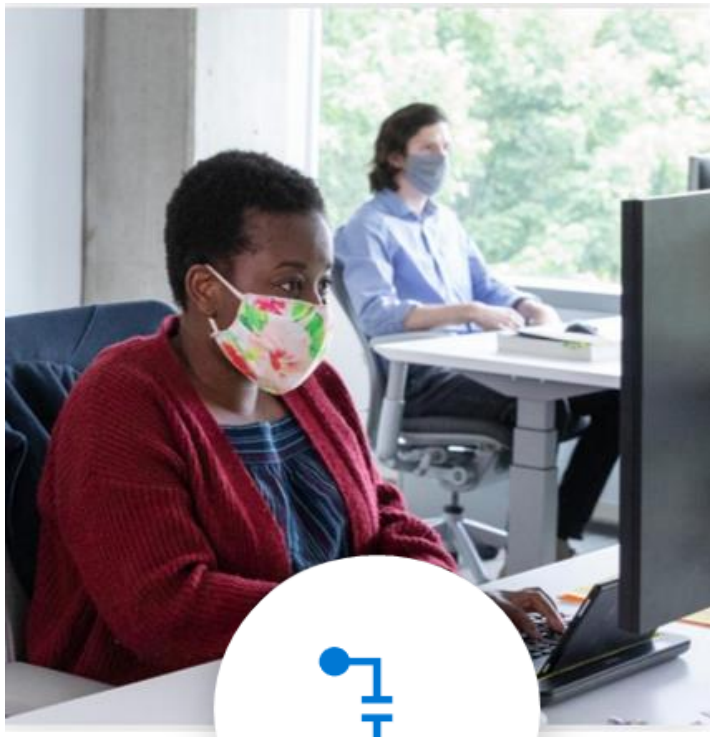
Principios ZERO TRUST



Verificar explícitamente



Acceso con privilegios mínimo



Asumir que hay brechas

Pilares core ZERO TRUST

Identidad

Verifique y **proteja** cada identidad con una autenticación

Gestión Endpoint

Obtenga visibilidad de los dispositivos que acceden a la red y garantice el cumplimiento y estado de salud antes de otorgar acceso

Aplicaciones

Descubra Shadow IT y controle el acceso con **análisis y monitoreo en tiempo real**

Infraestructura

Emplear detección de amenazas en tiempo real, bloquear y marcas riesgos automáticamente y **aplicar principios de acceso con priv. mínimos**

Red

Cifre todas las comunicaciones internas**, limite el acceso según políticas** y emplee segmentación y detección de amenazas en tiempo real

Datos

Clasifique, etiquete y **proteja datos con cifrado de extremo a extremo**

¿Qué es Zero Trust?

Permitir el acceso seguro a los recursos y datos desde cualquier lugar tomando decisiones en tiempo real basadas en el riesgo y el contexto.

Garantizar que se accede a los recursos de forma segura, independientemente de la ubicación, la red o la tecnología de la nube. **Los usuarios, los dispositivos, las redes y los recursos nunca son de confianza hasta que se verifica el contexto** a través de la autenticación, la autorización y una evaluación de la postura (Control de Acceso Contextual). **En ningún momento se concederá el acceso simplemente** porque un usuario, una red o un recurso privilegiado asuma la **confianza**. ***"Never trust, always verify"***

User Context: Admin user or regular user, employee or a contractor + **Application Context:** Application Type, Risk Classification, Internal or External + **Device Context:** Operating System, Managed Device, Jailbroken, Security Software in place + **Location Context:** Access from Office/Home, Restricted hours, Restricted country + **Network Context:** Known bad IP address, Specified IP Zones, Network anonymizers + **Data Context:** Data classification, data sensitivity, volume of data being accessed = **Contextual Response:** Step Up Authentication prompted based on risk score (Allow/Deny Access)

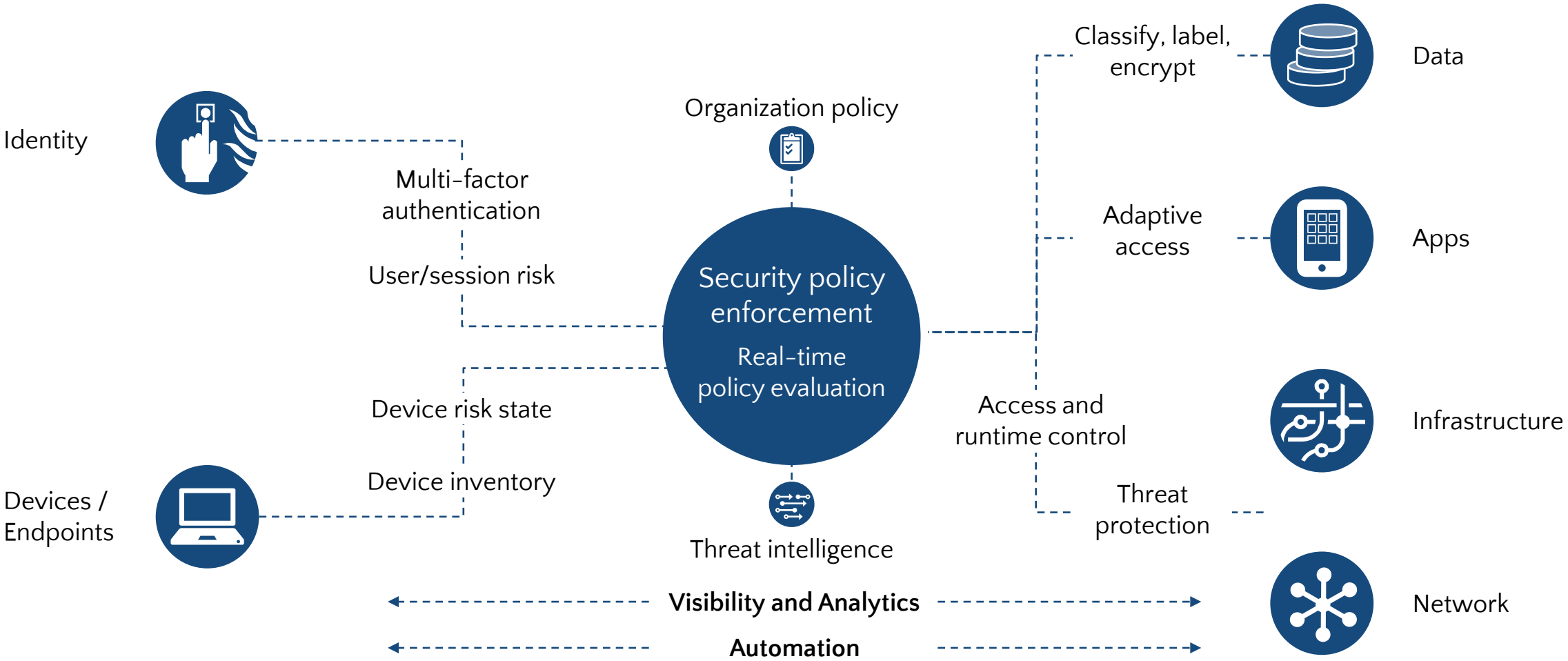
Adoptar una estrategia de privilegios mínimos. Alto grado de segmentación para imponer estrictamente el acceso basado en la necesidad. Esto incluye tanto a los usuarios que acceden a las aplicaciones ("Norte/Sur") como a los servidores y aplicaciones que se comunican dentro del centro de datos ("Este/Oeste").

Registro e inspección de todo el tráfico. Supervisión y visibilidad de todo el tráfico que entra y sale del entorno. Verificar el acceso y la identidad continuamente.

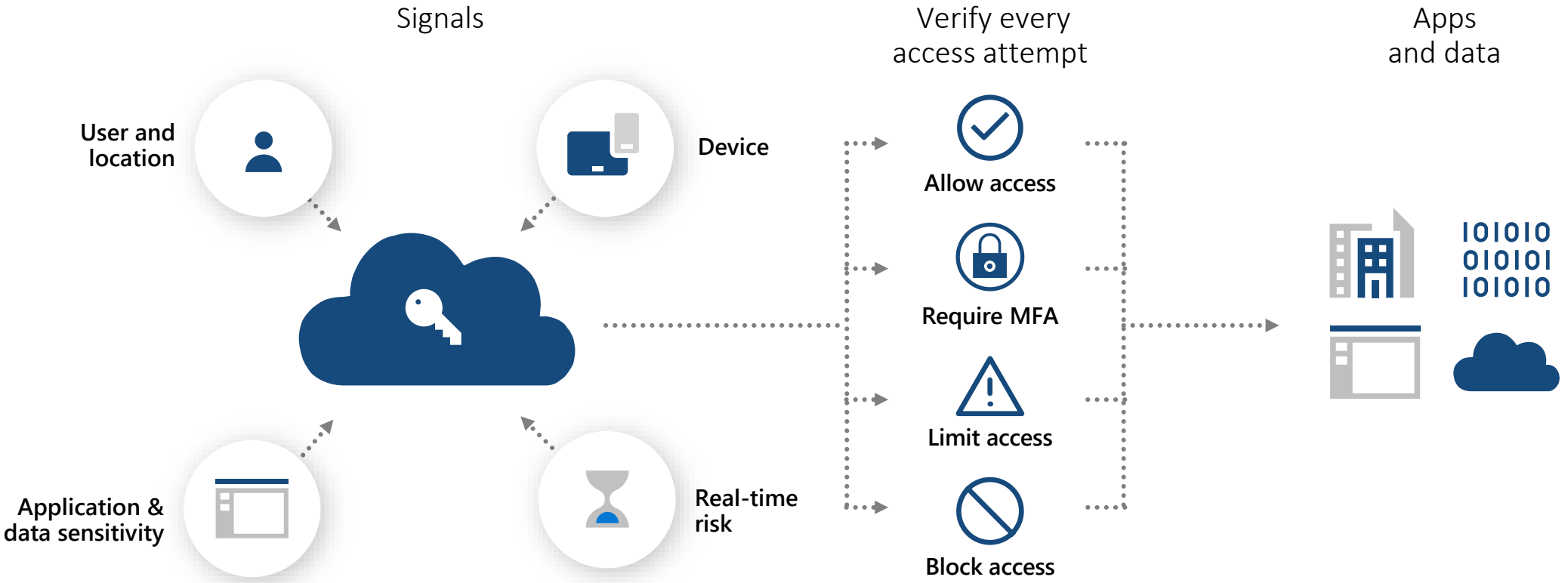
Una implementación exitosa de **Zero Trust se basa en una estrategia de seguridad centrada en los datos**, políticas de seguridad, estándares de clasificación de datos y una solución de Gestión de Identidad y Acceso para identificar a los usuarios y dispositivos, así como los recursos a los que necesitan acceder.

Acceso de bajo riesgo puede verse **mínimamente interrumpido,** permitiendo al usuario experimentar una **sesión rápida, fluidad y sin obstáculos.**

Arquitectura ZERO TRUST



Control de Acceso con políticas inteligente y evaluación del riesgo



¿Cómo previene Zero Trust los nuevos ataques?

Zero Trust puede prevenir significantemente los vectores de ataque multivariables por el mismo gasto estratégico que las soluciones tradicionales

		Prevencción Zero Trust
1	**Compromiso de terceros** Los atacantes utilizan credenciales robadas de un tercero de confianza, eludiendo los controles perimetrales.	Las credenciales robadas de terceros no permitirían a los atacantes acceder a la red, ya que el contexto del usuario y del dispositivo **activaría un requisito de autenticación multifactor basado en el riesgo.**
2	**Ingeniería Social** Los atacantes utilizan *spear-phishing* y ingeniería social para sortear el perímetro, ya que los empleados internos son de confianza.	El tráfico web saliente está restringido en función del principio de privilegio mínimo, y **los dispositivos de trabajo comprometidos no tienen permitido acceder a aplicaciones sensibles ni a servidores dentro del CPD**.
3	**Ransomware** El malware se propaga a través de la red debido a la falta de segmentación. Todos los equipos internos confían entre sí.	Los equipos no pueden propagar *ransomware* a otros equipos en el mismo segmente de red, ya que no existe un camino de comunicación entre ellos.
4	**Exposición de datos en la nube** La fuga de datos ocurre cuando el perímetro del Cloud no está adecuadamente protegido. El servidor de DB en la Cloud confía en las solicitudes provenientes de otros servidores de DB.	El servidor de DB alojado en Cloud no confían en las solicitudes provenientes de otros servidores de DB que no forman parte del flujo de datos necesarios.
5	**Movimiento Lateral** Los atacantes comprometen un servidor web vulnerable orientado hacia el exterior y luego se desplazan lateralmente dentro del CPD porque el servidor web de confianza.	La **microsegmentación evitará el movimiento lateral** entre aplicaciones y servidores dentro del CPD.
6	**Amenazas internas** Los *insiders* maliciosos aprovechan su derecho de confianza y su acceso privilegiado para hacer cosas que no deberían.	**Los empleados internos solo pueden acceder a los recursos necesarios para realizar su trabajo.** El análisis de comportamiento permite el registro reactivo y la alerta para identificar el abuso de estos permisos de menor privilegio.

Zero Trust

Al aplicar ciertos controles que permiten la **Arquitectura Zero Trust**, su organización podrá abordar los desafíos de seguridad de la red

Facilitadores

Descubre y perfila cada *endpoint* y aplicación en tu red, On-Premise y Cloud. Averigua quienes, que y cómo están conectados los usuarios y dispositivos, y evalúa continuamente los comportamientos de los dispositivos y usuarios conectados mediante el monitoreo y el log.

Mejora la autenticación y la autorización aprovechando el contexto del usuario, el dispositivo, la ubicación y el comportamiento para establecer una conexión segura solo con los recursos autorizados.

Implementa la segmentación adaptative con políticas de seguridad sólidas para restringir o aislar los activos y usuarios no conformes. Segmenta los usuarios y activos según su identidad y automatiza y estandariza la gobernanza y la orquestación.

Resultados

Implementa la seguridad sin perímetro

Garantiza que los recursos acceden de manera segura independientemente de la ubicación o la tecnología

Aplica el acceso de privilegios mínimos

Permite el acceso basado en la necesidad a través de altos grados de segmentación.

Reducir la superficie de ataque

Detener la propagación de malware y la amenaza interna, incluido ransomware y la exfiltración, de manera proactiva

Endpoints Seguros

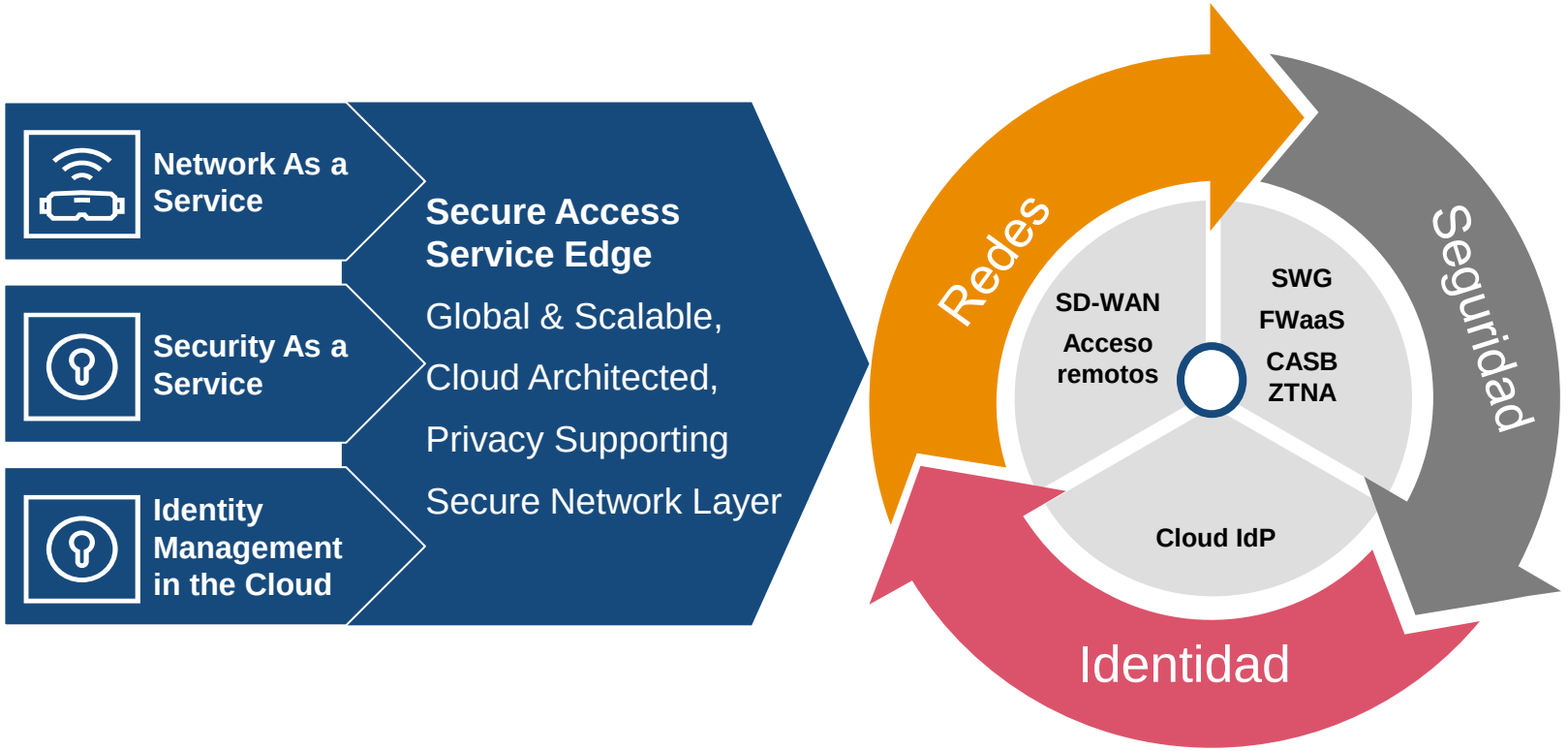
Controles de seguridad de Endpoints aplicados a usuarios y dispositivos antes de acceder al CPD o recursos de Cloud

Mejorar la gobernanza y el cumplimiento

Disminuir el tiempo y los gastos de cumplimiento (PCI, HIPAA, GDPR, etc.) y organizar los datos por criticidad o sensibilidad

SASE

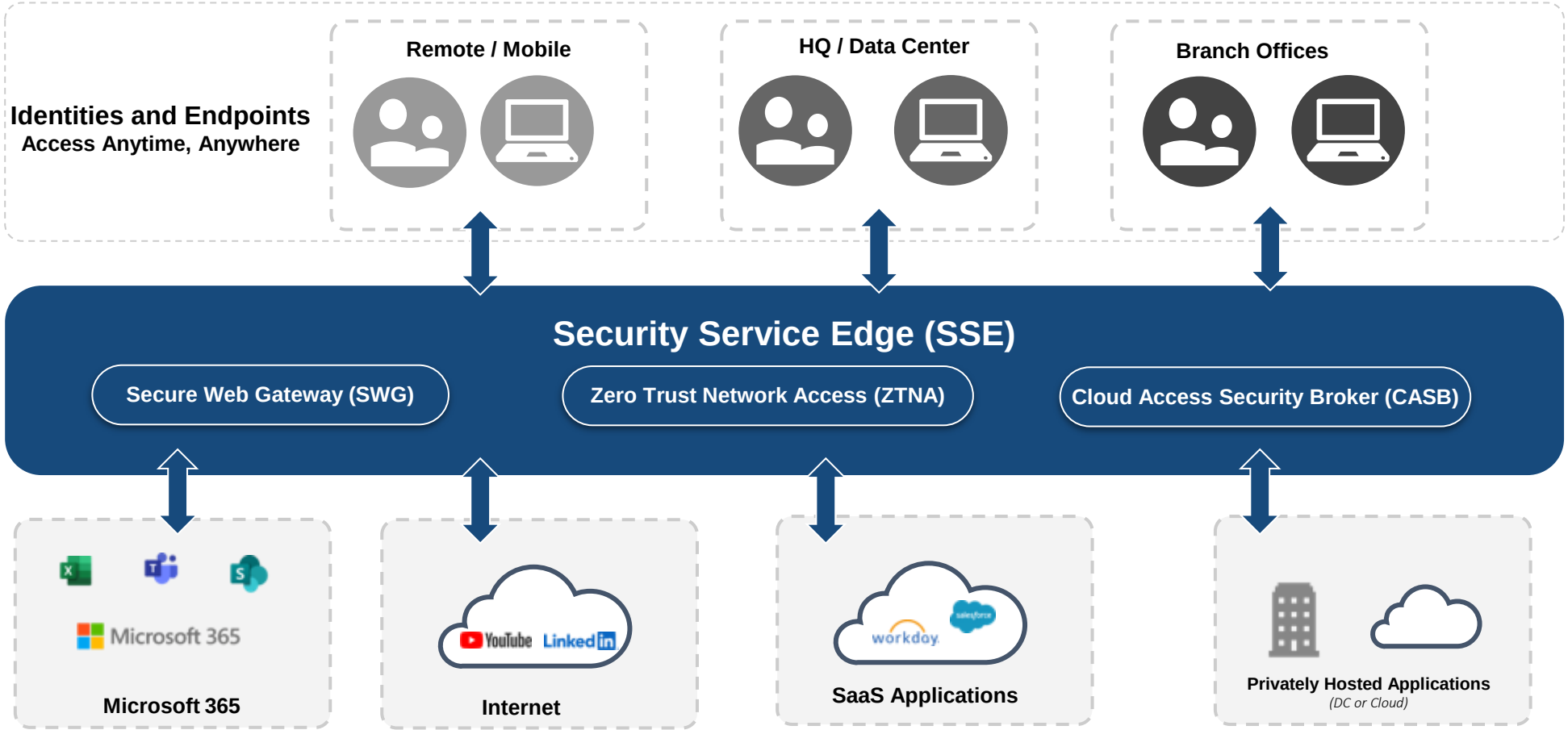
Secure Access Service Edge (SASE), es un modelo que integra funcionalidades red y servicios de seguridad (como SWG, CASB, FWaaS y ZTNA) para respaldar las crecientes y dinámicas necesidades de acceso seguro de las empresas digitales.



- Posiciona la adopción de soluciones basadas en la nube para aprovechar los beneficios de la nube.
- Permite que el personal de IT pase de gestionar redes y cajas de seguridad a ofrecer servicios y controles de seguridad basados en políticas.
- Permite el acceso a la red Zero Trust para todos los entornos y aplicaciones empresariales para mejorar la seguridad y el rendimiento.
- Centraliza el control de políticas con aplicación local y reduce la complejidad, los gastos generales operativos y los costes comerciales generales.
- Admite requisitos normativos y de cumplimiento a través de controles granulares y de privilegios mínimos para el acceso a Internet/SaaS y aplicaciones privadas.

SSE

Security Service Edge (SSE), es el componente de seguridad de SASE que unifica todos los servicios de seguridad, incluidos Secure Web Gateway (SWG), Cloud Access Security Broker (CASB) y Zero Trust Network Access (ZTNA), para proteger el acceso a la web, servicios en la nube y aplicaciones privadas.



¿Cómo se ve en la práctica?

Escenario 1: Un empleado de la empresa, Juan, está en la cafetería y le gustaría utilizar el portátil que le proporciona la empresa para acceder a su historial de pagos almacenado en la aplicación de RRHH de su empresa.

	Actividad a Realizar	Contexto de Usuario	+ Contexto de Aplicación	+ Contexto de Dispositivo	+ Contexto de Ubicación	+ Contexto de red	= Respuesta contextual (Permitir/Denegar el acceso)
Baja madurez	Juan abre un cliente VPN, se conecta y abre un navegador para acceder a la aplicación de RRHH	Juan valida su identidad con un nombre de usuario, una contraseña y un token de autenticación multifactor.	Juan es miembro de un grupo de AD que le da acceso a la aplicación de RRHH.			Juan viene de un rango de VPN por lo que se le permite acceder a la aplicación.	Juan tiene acceso a la aplicación de RRHH.
Alta madurez	Juan abre un navegador para acceder a la aplicación de RRHH e iniciar la sesión	Juan es un empleado.	La aplicación está alojada internamente y contiene datos sensibles.	Juan utiliza un portátil gestionado por la empresa y contiene parches de seguridad actualizados.	La cafetería no es una oficina corporativa, pero está en el mismo estado y país que la oficina.	Juan no está utilizando una red maliciosa conocida.	La solicitud de acceso de Juan se considera de riesgo moderado y se le da una solicitud de autenticación escalonada antes de obtener el acceso.

¿Cómo se ve en la práctica?

Escenario 2: Un grupo de hackers malintencionados ha puesto en peligro una popular tecnología de autenticación de dos factores y está planeando utilizar las credenciales robadas para acceder al historial de pagos de Juan almacenado en la aplicación de recursos humanos de la empresa.

	Actividad a Realizar	Contexto de Usuario	+ Contexto de Aplicación	+ Contexto de Dispositivo	+ Contexto de Ubicación	+ Contexto de red	= Respuesta contextual (Permitir/Denegar el acceso)
Baja madurez	El atacante abre un cliente VPN, se conecta y abre un navegador para acceder a la aplicación de RRHH.	✓ El atacante valida la identidad de Juan con un nombre de usuario, una contraseña y un token de autenticación multifactorial.	✓ Juan es miembro de un grupo de AD que le da acceso a la aplicación de RRHH.			✓ El atacante viene de un rango de VPN por lo que se le permite acceder a la aplicación.	El atacante tiene acceso a la aplicación de RRHH como Juan.
Alta madurez	El atacante abre un navegador para acceder a la aplicación de RRHH e iniciar sesión con las credenciales robadas.	✓ Juan es un Empleado.	? La aplicación está alojada internamente y contiene datos sensibles.	✗ El atacante no utiliza un portátil gestionado por la empresa.	✗ El atacante reside en un país extranjero.	✗ El atacante está usando un anonimizador de red.	STOP La solicitud de acceso del atacante se considera de alto riesgo y ha violado varias políticas de aplicación y se le niega el acceso a la aplicación de RRHH.

Fabricantes para la adopción Zero Trust

IAM/PAM	Acceso Definido por Software	Segmentación	Endpoints seguros	Red Definida por Software	Redes Seguras en la Nube	Gobernanza y Gestión
SailPoint	portnox™	paloalto NETWORKS	CORTEX BY PALO ALTO NETWORKS	PRISMA BY PALO ALTO NETWORKS	Microsoft	illumio
CYBERARK	FORESCOUT	FORTINET			aws	ordr
okta	Cisco ISE	APPGATE			Google Cloud	Cisco Tetration
transmit SECURITY	aruba a Hewlett Packard Enterprise company	CISCO	TANIUM	Akamai	netskope	
ForgeRock		vmware	Microsoft	zscaler™		
		CITRIX				

Muchas gracias

ANDORRA DIGITAL

ANC-AD

@anc_ad

@anc-ad

csirt.anc@govern.ad