PRACTICA 1

-BRS01-

PARADIGMA “ZERO TRUST”

JOSE ANTONIO MORENO ARANDA

Indice:

1- ¿Qué dicen las redes sobre Zero Trust?

Si hacemos una búsqueda para empezar a ampliar nuestro conocimiento sobre Zero Trust en internet, encontraremos noticias como esta:

Ej1: *por Forrester Research notica de ejemplo*

Fuente: https://www.interempresas.net/Zero Trust-acceso-seguro.html

Ej2: *Notica de ejemplo.*

Fuente: https://www.arubanetworks.com/es/productos/seguridad/

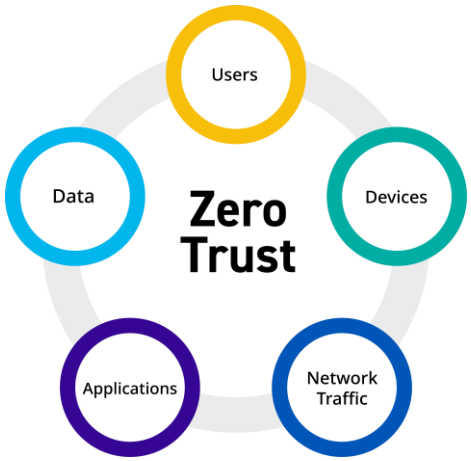
Ej3: *Noticia de ejemplo.*

Fuente: https://ciberseguridad.blog/que-es-zero-trust-en-ciberseguridad

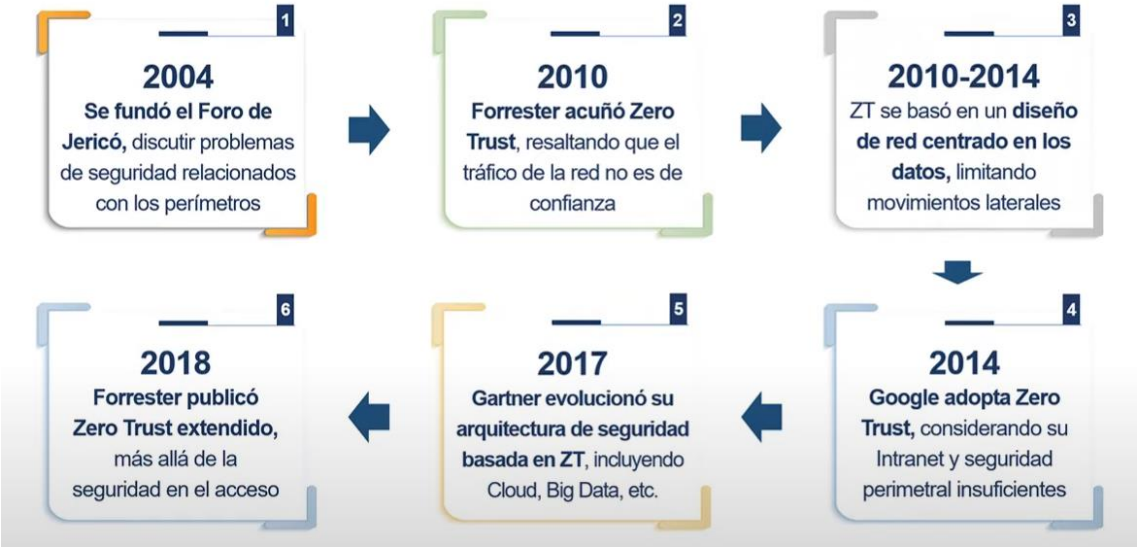
Es lógico que se generen dudas acerca de Zero Trust, ¿qué es? Son muchas las preguntas que nos abordan y que mediante esta práctica intentaré dejar solucionado.

Si podemos saber ya que Zero Trust se basa en:

- Usuarios
- Dispositivos
- Red
- Aplicaciones
- Datos



2- Origen y Evolución de Zero Trust



- En 2004 en el Foro de Jericó se cuestionó, sobre las problemáticas y soluciones entorno a los perímetros en la red.
- En 2010 un analista de Forrester Research acuñaron el termino de Zero Trust por primera vez. Consideraron que el tráfico de una red no era seguro.
- En 2010-2014 Zero Trust se focalizó en un diseño de red focalizado en los datos, con el objetivo de limitar el movimiento de los atacantes dentro de nuestra red.
- En 2014 Google consideraba que sus redes no eran seguras, debido a que, aunque disponen de seguridad perimetral, no era suficiente segura.
- En 2017 Google evolucionó su arquitectura basada en Zero Trust e incorporó nuevas arquitecturas de redes, como entornos Cloud por ej.
- En 2018 Forrerester Research fueron mas allá en lo que refiere a la seguridad del acceso y sacaron un modelo nuevo llamada Zero Trust Extendido

3- Aproximación a Zero Trust

Según Gartner Zero Trust es un paradigma, una iniciativa estratégica que tiene en cuenta, estos elementos identidades, redes, datos y aplicaciones.

Zero Trust no es una arquitectura de red única, sino un conjunto de principios y enfoques, y además debe de implementarse de manera gradual.

Tradicionalmente la seguridad de una empresa se basaba en el concepto del “foso y castillo”, todo lo que estaba dentro de nuestro perímetro de red es una zona segura y todo lo que estaba era una amenaza.

En la actualidad en muchas compañías, el cambio es sustancial ya que disponemos de diferentes puntos de acceso de valor a nuestras redes, desde puntos externos que también deberían ser seguros, pero no en todos los casos lo son, por lo que estamos mas expuestos a diferentes tipos de ataques.

<< Zero Trust es una iniciativa estratégica que debe integrar políticas, buenas prácticas y tecnologías >>

Principios de Zero Trust:

- Privilegios mínimos
- La red privada no es segura
- No existen recursos de confianza
- Ningún acceso se considera seguro
- No confiar en la conexión a la red
- Recopilar información

Desafíos de Zero Trust

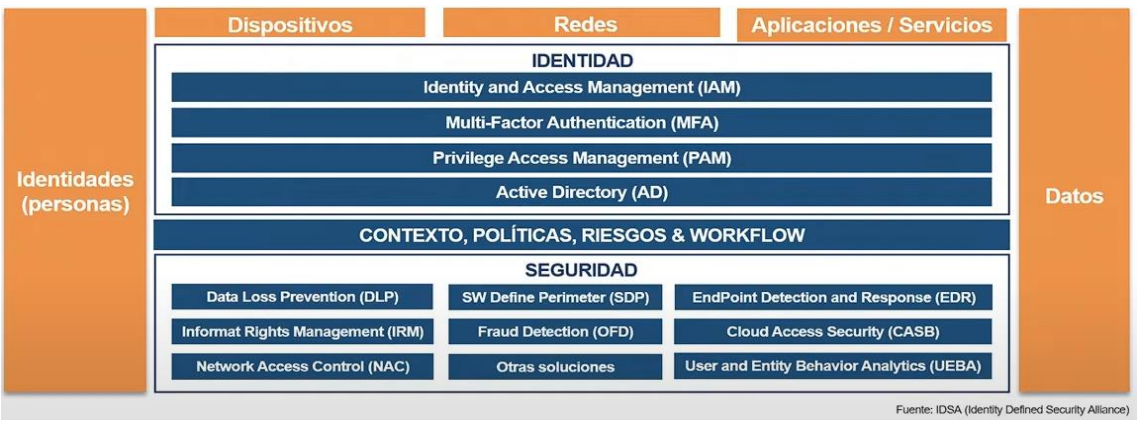
- Cambio de mentalidad, ninguna parte de red es confiable
- No existe zona de confort en la red, dentro y fuera de nuestra nada es seguro
- No existe la confianza, hay que verificar
- Privilegios mínimos, los que realmente se requieran
- Políticas dinámicas
- Analítica y Coordinación de nuestra red

4- Arquitecturas de Zero Trust

Detallo a continuación los diferentes tipos de arquitecturas:

a) Arquitectura Base según el NIST, donde primó principalmente mediante políticas
   a. Motor de políticas (PE)
   b. Administrador de políticas (PA)
   c. Punto Cumplimiento de política (PDP)
   d. Los 3 anteriores alimentados en sí, por fuentes de datos externas

b) Posteriormente el IDSA, le dio una vuelta mas e identifico una serie de elementos claves:
   a. Identidades
   b. Dispositivos
   c. Redes
   d. Aplicaciones
   e. Datos



5- Más allá de las arquitecturas: Enfoques de Zero Trust

Desde este punto tratamos de enfocar-englobar la seguridad de la empresa en 360 grados.

Además, para adoptar ZT en su globalidad hay que tener en cuenta todas estas visiones de la seguridad.

Enfoque Basado en la Red

Se basa en poder controlar y organizar los accesos a la red, principalmente descubriendo, perfilando y autentificando los accesos de entidades

Casos de uso:

- Control de los accesos vía VPN
- Control de accesos vía inalámbrica
- Control accesos vía cableada
- Control del Data Center

Enfoque Basado en las Identidades:

3 características de este enfoque:

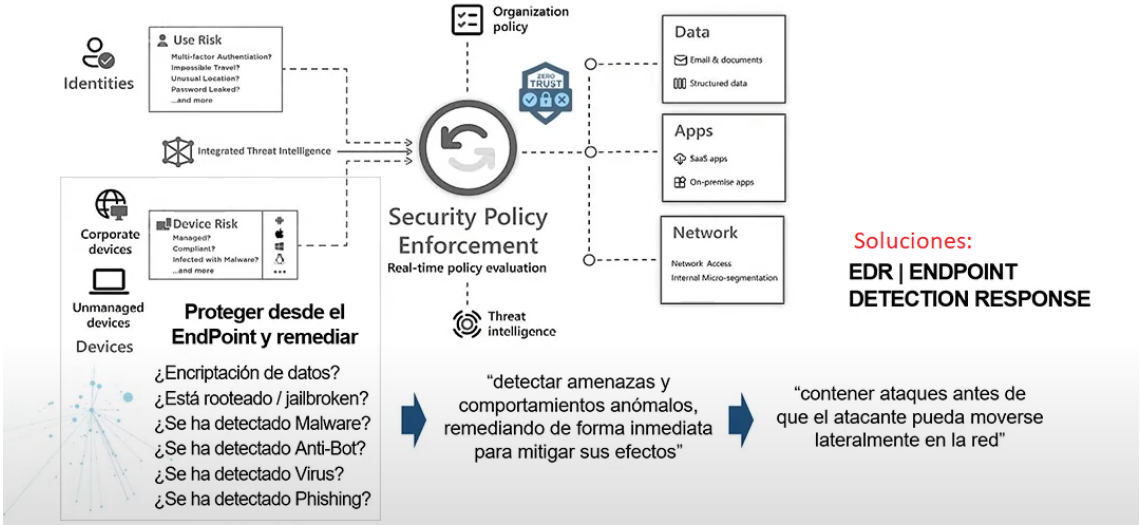
- Gestión de los accesos
- Gestión de las identidades
- Control del comportamiento anómalos de los usuarios

Casos de uso:

- Detectar vulnerabilidades
- Sincronizar identidades
- Control identidades
- Cumplimiento normativo

Enfoque de los dispositivos:

Nos preocupamos de la seguridad desde el propio dispositivo con la finalidad de detectar las amenazas y poder detectarlas en tiempo real, para evitar ese movimiento lateral de nuestra red.

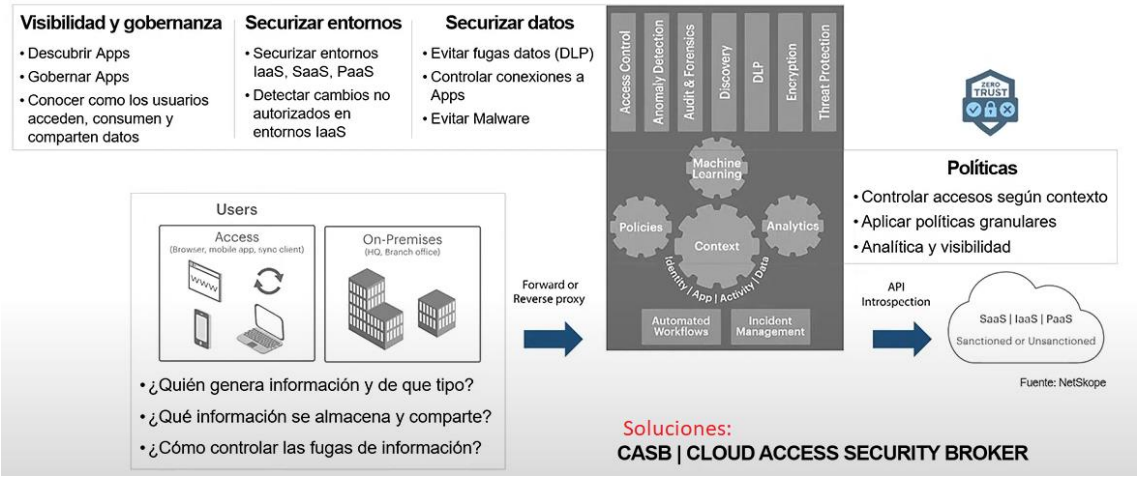


Casos de uso:

- Detectar vulnerabilidades en el propio dispositivo
- Identificar y contener ataques
- Capacidad forense, análisis y reporting

Enfoque de las aplicaciones:

Desde este enfoque, ¿quién está generando información y de que tipo?, ¿dónde se almacena y como se comparte?

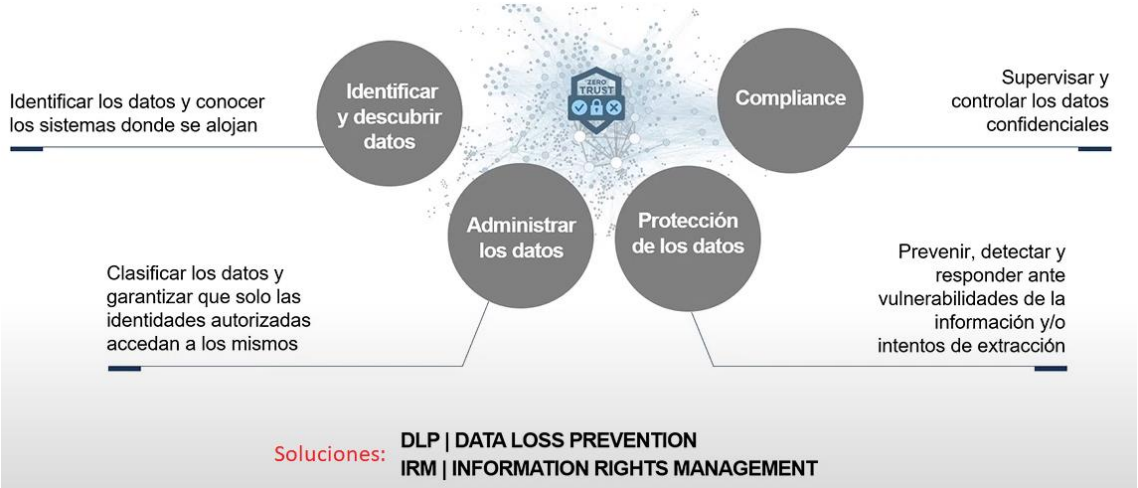


Casos de uso:

- Visibilidad, conocer y gobernar todas las aplicaciones de nuestra compañía
- Controlar y gestionar todas las sesiones
- Prevenir amenazas
- Cumplimiento normativo

Enfoque en los datos:

Nos interesa desde este enfoque identificar y conocer los datos que tenemos y donde se están alojando, administrar esos datos y garantizar que las entidades autorizadas están teniendo acceso a estos.



Casos de uso:

- Identificar y clasificar los datos
- Securizar los datos
- Evitar fugas de información
- Gobernar los datos y cumplir lo normativo

6- Principios de Zero Trust alineados con los requisitos del ENS

Como paradigma se alinea con otro tipo de estrategias como por ejemplo las del tipo ENS, también está en sintonía con otras estrategias como por ejemplo el marco SASI

7- Características del Modelo Zero Trust

- Principio de mínimo privilegio: Acceso limitado solo a lo que es necesario.
- Verificación constante: Todos los usuarios y dispositivos son verificados y autenticados antes de obtener acceso.
- Microsegmentación: División de redes en segmentos más pequeños para limitar el acceso no autorizado.
- Identidad como perímetro: No se basa en la ubicación del usuario, sino en quién es el usuario y si tiene permisos.
- Defensa en profundidad: Múltiples capas de seguridad.

8- Proveedores que soportan Zero Trust y servicios

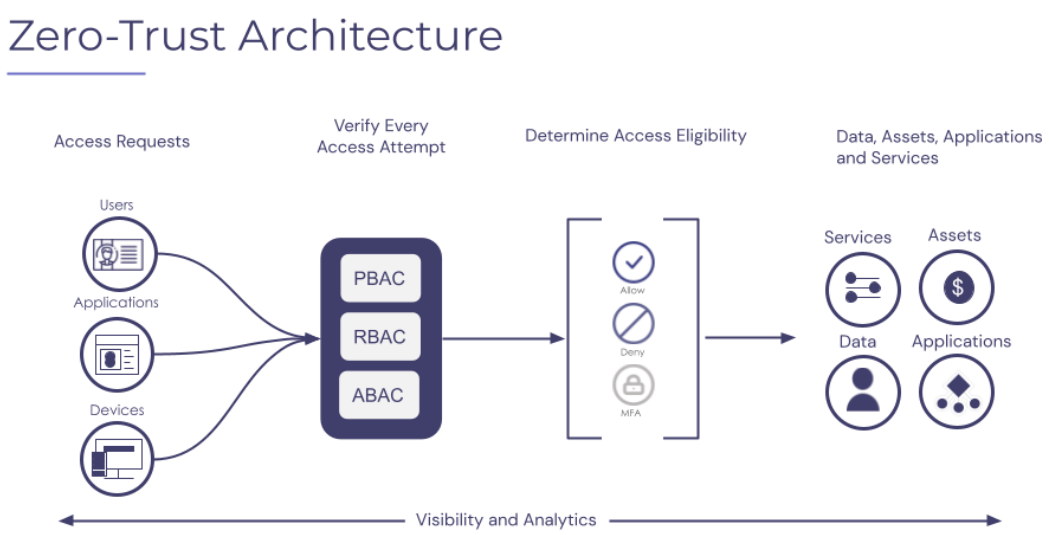
- **Cisco**: Aporta la suite denominada "Cisco Zero Trust", asegurando el acceso de dispositivos, aplicaciones y redes
- **Microsoft**: Ofreciendo su servicio "Azure Active Directory", facilita soluciones de identidad y acceso basadas en Zero Trust.
- **Palo Alto Networks**: "Palo Alto Networks Prisma Access" solución de seguridad de red basada en el modelo Zero Trust. Prisma Acces → SASE
- **Google**: Con su implementación "BeyondCorp", Google desarrolla el enfoque de Zero Trust, centrada la seguridad en la identidad del usuario, y no en el perímetro de red.

Hay otros proveedores no tan conocidos como los anteriores, pero que también entre sus servicios, ofrecen herramientas de Zero trust.

9- Implementación del servicio Zero Trust

La implementación del modelo "Zero Trust" implica:

- Identificar datos sensibles: Saber qué se debe proteger.
- Mapa de flujo de datos: Entender cómo se mueven los datos.
- Micro Segmentar la red: Dividir la red en segmentos más pequeños.
- Establecer políticas de acceso: Definiendo quién puede acceder.
- Monitorización y análisis: Controlar el tráfico de la red y tomar decisiones sobre comportamientos irregulares.



10- Ventajas e Inconvenientes de Zero Trust respecto a modelos de bastionado clásicos

VENTAJAS:

- Mayor seguridad: Cada solicitud de acceso es verificada.
- Reducción del riesgo de ataques internos: Al no confiar en nada dentro del perímetro.
- Adaptabilidad a la nube y movilidad: Compatible con la tendencia actual hacia la nube y el trabajo remoto.

INCONVENIENTES:

- Complejidad: Puede ser complejo de implementar en grandes organizaciones.
- Costo: La implementación y mantenimiento pueden ser costosos.
- Cambio de mentalidad: Requiere un cambio en la forma en que las organizaciones ven la seguridad.

11- Conclusiones

Zero Trust No es un producto de un fabricante, es una solución determinada o un conjunto de capacidades funcionales.

Zero Trust es un Paradigma de ciberseguridad, centrado en la protección de los recursos y en el principio de la “confianza cero”.

Zero Trust debe integrar “políticas, buenas prácticas y tecnologías habilitadoras”.

Zero Trust apuesta por la seguridad desde diferentes puntos de enfoque:

Para finalizar Zero Trust se alinea con una estrategia ENS y otros marcos de seguridad como es el marco SASI

Referencias para desarrollar el trabajo:

- https://www.zscaler.com/resources/security-terms-glossary/what-is-zero-trust
- https://www.netskope.com/es/security-defined/what-is-zero-trust
- https://securityscorecard.com/blog/what-is-zero-trust-architecture
- https://www.fortinet.com/resources/cyberglossary/how-to-implement-zero-trust
- Youtube: https://www.youtube.com/watch?v=On_3ulzCl_4&t=1s