ManageEngine

Los pilares de Zero Trust

El modelo de seguridad moderno de Zero Trust no se limita a la microsegmentación de la red, control de identidades o perímetros definidos de software. Estas son partes clave de su modelo de Zero Trust, según el método que usted utilice.

No obstante, Zero Trust no es solo la segmentación de la red o la gestión de accesos e identidades. Se construye sobre cinco pilares clave, sin los cuales su estrategia de seguridad seguirá estando incompleta:

1

Seguridad de los datos

Los datos son el nuevo oro, y es lo que normalmente buscan los atacantes. Por eso es por lo que identificar, clasificar, gestionar y proteger sus datos en reposo y en movimiento es una parte clave de cualquier método de seguridad Zero Trust.

2

Redes

Este pilar o control se enfoca en la segmentación, aislamiento y control de la red, resultando en un posible punto de inicio para una implementación de Zero Trust.
Al ser capaz de monitorear y controlar su red, usted puede limitar los riesgos que suponen los ataques informáticos.

3

Identidades
(personas y dispositivos)

Este control se enfoca en gestionar, monitorear y proteger el acceso de usuarios y dispositivos, el cual representa el núcleo de los métodos de Zero Trust centrados en la identidad. Esto puede reducir el riesgo que supone credenciales robadas, infiltrados maliciosos y otras amenazas.

4

Cargas de trabajo*

Proteger todas las aplicaciones, recursos de informática y otros componentes asociados con sus cargas de trabajo puede contribuir a mitigar los riesgos de seguridad en su organización.

5

Endpoints

Los endpoints de la organización, incluyendo los dispositivos IoT, con frecuencia son el objetivo de los atacantes. Para reducir el riesgo que estos suponen, necesita ser capaz de monitorear, gestionar y proteger cada dispositivo en su red, y aislarlos de ser necesario.

Estos pilares no son el final del entorno de Zero Trust. Para garantizar un cubrimiento holístico también necesita tener:

Herramientas para visibilidad y análisis que le permitan a su equipo de seguridad saber qué está pasando en su red.

Esto puede ayudar a detectar ataques informáticos en curso, señales de cuentas comprometidas, actividades de infiltrados maliciosos y más.

Automatización y orquestación

La automatización es el objetivo, y para la seguridad no es diferente. Tener funciones de automatización y respuesta para la orquestación de la seguridad a su disposición puede acortar los tiempos de respuesta ante incidentes y actuar como una fuerza multiplicadora para sus equipos de seguridad.

Referencias

The Zero Trust eXtended (ZTX) Ecosystem, Forrester Research (Agosto 23, 2021)

The path to Zero Trust starts with identity, Identity Defined Security Alliance

Obtenga más información sobre la confianza cero en

manageengine.com/latam/seguridad-zero-trust/