ManageEngine

Reafirme la seguridad informática con Zero Trust

Comience su viaje hacia el Zero Trust o resuelva las brechas de su enfoque actual con las soluciones de seguridad informática de ManageEngine.

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

Su enfoque de seguridad informática necesita una actualización

Su superficie de ataque se amplía

Con el 83% de las organizaciones aumentando su dependencia de la nube,1 los días de un perímetro de red bien definido han pasado a la historia. Además, las superficies de ataque de las organizaciones se han ido ampliando con la introducción de dispositivos IoT, el trabajo híbrido, las políticas BYOD, etc.

Su perímetro por sí solo no puede mantener alejados a los atacantes

Los modelos tradicionales de confianza perimetral o implícita se basan en firewalls y VPN para separar a los usuarios legítimos de los adversarios. Las personas dentro de la red, tanto si trabajan on-premises como si están conectadas a través de una VPN, son de confianza.

Sin embargo, este enfoque no tiene en cuenta:

- Robo de credenciales: La segunda causa más común de violaciones de la seguridad de los datos, el robo de credenciales, también es la que más tarda en identificarse y cuesta a las organizaciones un promedio de 4,62 millones de dólares por incidente.2

- Amenazas internas: Los intrusos maliciosos representan una pequeña parte del mundo de las amenazas informáticas (el 83% de las violaciones de la seguridad implican a atacantes externos3), pero aun así pueden costar a las organizaciones un promedio de 4,9 millones de dólares por incidente.2

1Fuente: La encuesta de preparación digital 2021, ManageEngine
2Fuente: Informe sobre el costo de una brecha de seguridad de los datos 2023, IBM Security
3Fuente: Informe sobre investigaciones de brechas de datos 2023, Verizon

¿Por qué adoptar un enfoque de seguridad de Zero Trust?

El Zero Trust complementa y mejora la seguridad tradicional basada en el perímetro. Ayuda a proteger a las organizaciones frente a amenazas de las que los modelos de confianza implícita no pueden defenderse, como los ataques basados en credenciales y los intrusos maliciosos.

La seguridad de Zero Trust también puede ayudar a su organización y a sus empleados a:

- Trabajar de forma segura desde cualquier lugar y en cualquier momento.
- Reforzar su seguridad y defenderse de las violaciones de la seguridad de los datos.
- Defenderse contra el robo de credenciales, las amenazas internas y otros riesgos.
- Cumplir los mandatos gubernamentales e industriales.

El entorno Zero Trust

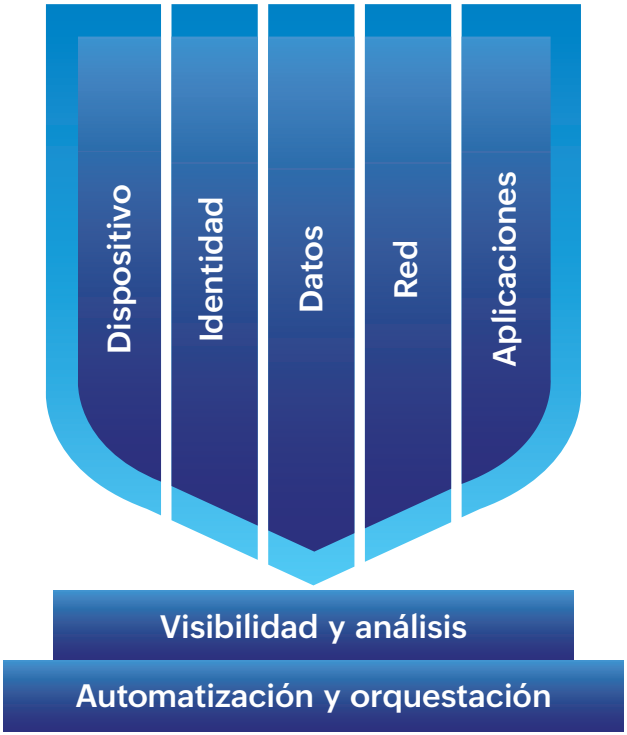
Para garantizar una seguridad completa, usted necesita disponer de procesos y tecnología para proteger, monitorear y gestionar sus identidades, datos, endpoints, red y aplicaciones.

Además, para completar su implementación Zero Trust, también necesita implementar:

- Soluciones de visibilidad y análisis para obtener una visibilidad completa de la red y detectar amenazas potenciales y activas.

- Automatización y orquestación de la seguridad para garantizar tiempos de respuesta más rápidos y garantizar una protección 24x7.

El entorno Zero Trust extendido (ZTX) y los cinco pilares de la seguridad Zero Trust



Implementación del Zero Trust con ManageEngine

La seguridad de Zero Trust puede implementarse de muchas maneras.

En ManageEngine, recomendamos adoptar un enfoque centrado en la identidad. Las empresas que se centran en la seguridad de las identidades y los dispositivos parecen reducir más rápidamente los riesgos de seguridad, según la "Guía práctica para una implementación de Zero Trust" de Forrester.

Sea cual sea el enfoque que usted elija, nuestras soluciones pueden proporcionar la base tecnológica para su modelo de seguridad de Zero Trust o pueden solventar las brechas de seguridad de su enfoque actual.

Nuestra oferta

Seguridad de identidades: Obtenga visibilidad de todas sus identidades en sus aplicaciones on-premises y en la nube. Proteja sus identidades con MFA, mínimos privilegios, e implemente controles de acceso basados en políticas (PBAC) y puntuación de confianza para mitigar las amenazas en tiempo real.

Nuestros productos:

AD360: Gestione las identidades y el acceso de los usuarios, implemente MFA adaptable, proteja las cuentas privilegiadas con UBA y garantice el cumplimiento normativo para entornos híbridos. **(On-premises)**

Identity360: Controle por completo sus identidades digitales, proteja el acceso a los recursos de la nube, aplique la seguridad basada en la identidad y mucho más. **(Cloud)**

PAM360: Establezca un control estricto sobre las vías de acceso privilegiadas y evite los riesgos de seguridad mediante una puntuación de confianza en tiempo real y controles de acceso basados en políticas.**(On-premises | MSP)**

Confianza en los dispositivos: Monitoree y realice un control del estado de salud, disponibilidad y seguridad de todos los endpoints que acceden a la red de la empresa. Detecte y aplique parches a las vulnerabilidades de los sistemas operativos y las aplicaciones para reducir la superficie de ataque, y bloquee, ponga en cuarentena o elimine dispositivos de forma remota según sea necesario.

Nuestros productos:

Endpoint Central: Proteja su infraestructura de TI con parcheo automatizado, gestión de la superficie de ataque, protección contra ransomware y mucho más desde una única consola. **(On-premises | Cloud | MSP)**

Mobile Device Manager Plus: Gestione de forma segura los dispositivos corporativos y personales con Apple OS, Android, Windows y Chrome OS. **(On-premises | Cloud | MSP)**

Seguridad de los datos: Localice, identifique y clasifique archivos sensibles y datos vulnerables en toda su red. Monitoree todas las actividades de los archivos en tiempo real, evite acciones no autorizadas en datos confidenciales y detecte y detenga los ataques de ransomware con respuestas automatizadas a las amenazas.

Nuestros productos:

DataSecurity Plus: Audite los cambios en los archivos, analice el almacenamiento y la seguridad de los archivos, descubra y clasifique los datos sensibles, monitoree el tráfico web y evite las filtraciones de datos. **(On-premises)**

Endpoint DLP Plus: Automatice la detección y clasificación de datos confidenciales de endpoints y aplique reglas para un uso y transferencia seguros. **(On-premises)**

Seguridad de la red: Monitoree su red y sus servidores en tiempo real para detectar dispositivos maliciosos y errores de configuración de la red. Realice análisis forenses de la red para detectar amenazas o ataques, y haga copias de seguridad de las configuraciones de red para una rápida recuperación en caso de desastre.

Nuestros productos:

OpManager Plus: Gestione y monitoree sus dispositivos de red, servidores, almacenamiento y aplicaciones y optimice el rendimiento de la red desde una única consola **(On-premises)**

NetFlow Analyzer: Obtenga una visibilidad holística del tráfico de su red y de la utilización del ancho de banda, realice análisis forenses de la red y proteja su red con análisis de seguridad avanzados. **(On-premises)**

Network Configuration Manager: Tome el control total de las configuraciones de su red y automatice las copias de seguridad de las configuraciones. **(On-premises)**

Análisis y automatización de la seguridad (SIEM y SOAR): Analice la actividad de la red y sincronice los datos de los servicios de inteligencia sobre amenazas para detectar y mitigar los ataques cibernéticos. Utilice análisis del comportamiento de usuarios y entidades basados en IA para detectar amenazas internas y cuentas comprometidas, y automatice su respuesta a incidentes con flujos de trabajo predefinidos y personalizados.

Nuestros productos:

Log360: Equipe a su SOC con una visibilidad más profunda de los eventos de seguridad, acelere la detección y respuesta ante amenazas, mejore la postura de seguridad de su red y garantice el cumplimiento. **(On-premises | Cloud | MSSP)**

Cloud Security Plus: detecte y neutralice amenazas en AWS, Azure, GCP y otras soluciones IaaS, SaaS y PaaS. **(On-premises)**

Acerca de ManageEngine

ManageEngine elabora el conjunto de soluciones de gestión de TI más amplio del sector, con más de 60 productos. Tenemos todo lo que necesita para gestionar todas sus operaciones de TI, incluidas redes, servidores, aplicaciones, mesas de servicio, Active Directory, seguridad, desktops y dispositivos móviles.

Desde 2002, los equipos de TI han recurrido a ManageEngine para obtener un software asequible, rico en funciones y fácil de usar. Nuestras soluciones on-premises y en la nube impulsan las TI de más de 280.000 empresas de todo el mundo, incluidas nueve de cada diez empresas de la lista Fortune 100.

Mientras usted se prepara para los retos de gestión de TI que tiene por delante, le abriremos camino con nuevas soluciones, integraciones contextuales y otros avances que solo pueden proceder de una empresa dedicada exclusivamente a sus clientes. Y como división de Zoho Corporation, seguiremos impulsando el estrecho vínculo entre la empresa y las TI.

Escanee este código QR para obtener más información sobre cómo proteger su empresa con la seguridad de Zero Trust

ManageEngine
una división de **Zoho** Corp.