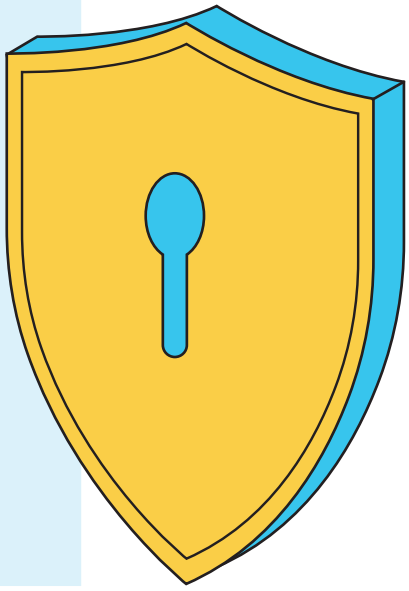
Alcanzando Zero Trust

El método de ManageEngine para mejorar la seguridad informática

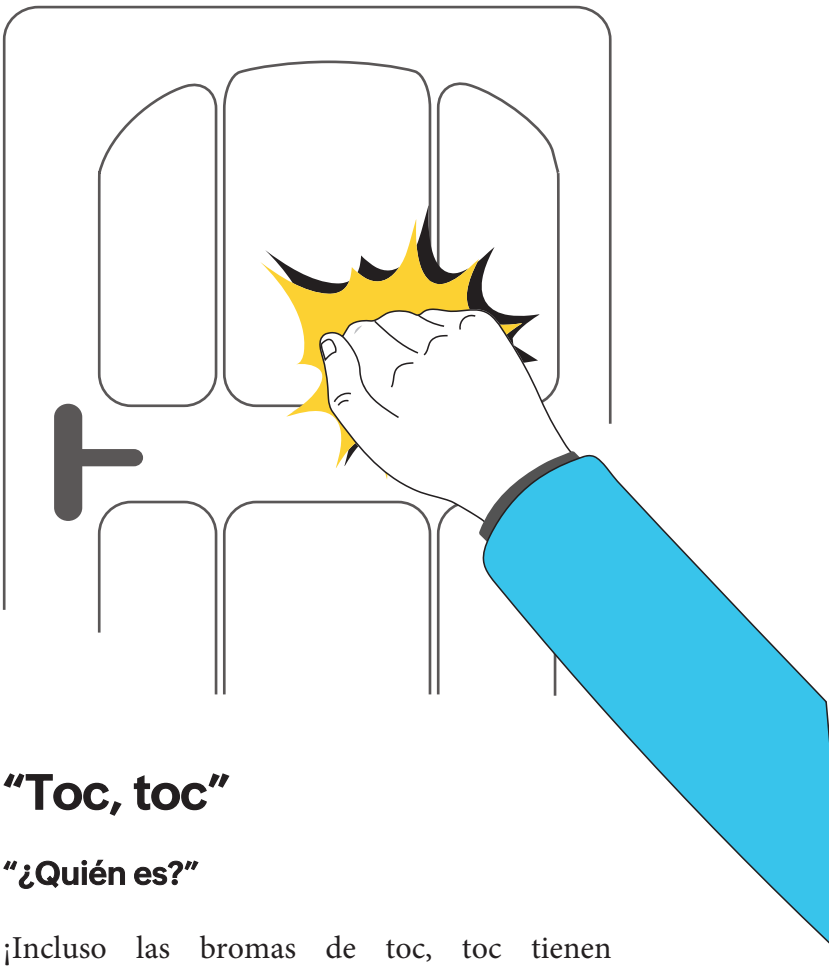
CONTENIDO



Glosario

Abreviaturas (en inglés)	Significado
DLP	Prevención de pérdidas de datos
MFA	Autenticación multifactor
MDM	Gestión de dispositivos móviles
2FA	Doble factor de autenticación
UEBA	Análisis del comportamiento de entidades y usuarios
ZTA	Arquitectura de Zero Trust
ZTNA	Acceso a la red de Zero Trust
ZTAA	Acceso a aplicaciones de Zero Trust
ZTDA	Acceso a datos de Zero Trust

Introducción



"Toc, toc"

"¿Quién es?"

¡Incluso las bromas de toc, toc tienen verificación! ¿Qué haría usted? ¿Le daría la bienvenida a un extraño en su casa sin verificación? Es probable que diera un vistazo por la mirilla. Abriría la puerta y preguntaría quién es, con base en lo cual decidiría cuánto acceso podría tener. Un agente de entregas se detiene en su porche. Un plomero puede entrar a su cocina para arreglar el lavaplatos. Un cuidador de casas puede entrar a todas las habitaciones, pero usted mantendría el armario con sus artículos de valor bajo llave. De forma similar las organizaciones tienen varias capas de seguridad que lo cubren todo, desde entrar a la red a acceder a archivos. Todo esto se ve facilitado por los principios guía a los que denominamos Zero Trust.

¿Para quién es este e-book?

Zero Trust puede parecer intimidante sin la guía adecuada. Si su organización está empezando a navegar este océano, este e-book es para usted. Empezaremos con las experiencias actuales de ManageEngine y trabajaremos a nuestra manera para trazar lo que usted puede hacer como líder de TI para su organización.

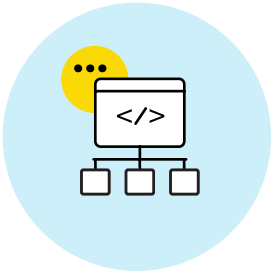
> (Zero Trust) aborda las necesidades dinámicas de las organizaciones modernas y, en última instancia, se volverá la forma en que se construye cualquier marco de seguridad.
>
> **Desde una opción corporativa a un imperativo empresarial, cada uno de nosotros está en el viaje de Zero Trust, lo sepa o no.**

Rajesh Ganesan, Presidente

ManageEngine

En este e-book, abordaremos:

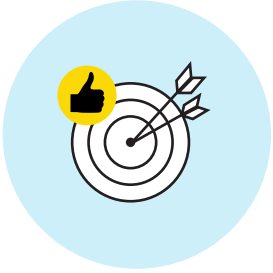
Zero Trust:
qué es y qué no es



Un marco de trabajo que usted puede implementar sin tener que deshacer su sistema actual.

Plan de Zero Trust de ManageEngine.

Casos de uso de la vida real.



Retos y mejores prácticas.

Capítulo 1

Autoevaluación para iniciar

1.1 ¿Qué es Zero Trust?

Zero Trust es más que una expresión de moda. Es el siguiente paso en la seguridad informática. En la última década ha habido un repunte en el número de incidentes de seguridad que las organizaciones enfrentan debido a amenazas internas y externas. En la Encuesta de disposición digital 2021 de ManageEngine dedujimos que el phishing, los ataques a endpoints de la red y los malware fueron las amenazas de seguridad más prominentes, sin embargo, solo el 26% de las organizaciones han optado por la implementación de una red Zero Trust. Zero Trust ya no es una opción, es un imperativo. En ManageEngine hemos empezado a implementar Zero Trust en nuestra red para darnos un escudo extra contra estos ataques prevenibles.

Zero Trust se fundamenta en tres principios.

01. El principio de mínimos privilegios:

También denominado principio de menor autoridad, esta es la práctica de limitar el acceso de los usuarios a los recursos al dar solo la autorización suficiente para que un miembro realice sus tareas. También es aplicable a sistemas, procesos, dispositivos y aplicaciones que requieren autorización.

02. Nunca confíe, siempre verifique:

La confianza implícita ha sido siempre un punto de vulnerabilidad en la seguridad. Sabemos que no podemos confiar ciegamente en todos dentro de una red. Con la confianza cero, reducimos la zona de confianza implícita y aplicamos una verificación explícita continua.

03. Asuma violaciones de la seguridad:

Esta es una de las pocas áreas en las que ser pesimista ayuda: asumir que se ha presentado o está presentando una violación de la seguridad en todo momento. La microsegmentación le permite controlar el radio afectado y evitar que la violación de seguridad se extienda.

1.2 Desmontar los mitos

Mito 01:
Zero Trust es un producto

Realidad:

Zero Trust no es una solución única que usted pueda comprar. Por el contrario, es un marco o conjunto de principios para guiar a las organizaciones para que tomen mejores decisiones de seguridad y se protejan ante violaciones de seguridad. Sin embargo, los proveedores pueden ofrecer varias herramientas, como autenticación de usuarios, que pueden integrarse para apuntalar la confianza cero en una red.

Mito 02:
Una buena estrategia necesita empezar de cero

Realidad:

Google BeyondCorp tuvo que deshacerse y reconstruir toda su arquitectura de red para incorporar Zero Trust, pero usted no tiene que hacer esto. Mejore su red existente paso a paso. Usted puede usar una herramienta de gestión de contraseñas, auditoría y monitoreo en tiempo real, y autenticación multifactor (MFA) como primer paso.

Mito 03:
En verdad significa "Nunca confíe (en sus empleados), siempre verifique"

Realidad:

La seguridad no es personal. Confiar en que todos dentro de su organización tienen buenas intenciones es una vulnerabilidad. Los atacantes pueden estar dentro o fuera de una organización; su trabajo como un líder de TI es mantener siempre la información protegida. Sin embargo, esto no significa que se deba tratar a los empleados como amenazas. Se puede usar el análisis del comportamiento de entidades y usuarios (UEBA) para asignar puntuaciones de confianza con base en varios parámetros y para otorgar a los usuarios acceso personalizado.

Mito 04:
Zero Trust es para empresas grandes

Realidad:

Usted no necesita gastar todo su presupuesto o dirigir una corporación multinacional para introducir Zero Trust. BeyondCorp creó la idea equivocada de que Zero Trust es costosa y que consume mucho tiempo. Esto se debe a que debía crear algo que no existía antes. Por otro lado, las PyME pueden empezar ahora con su viaje hacia Zero Trust con las sencillas herramientas que están disponibles. De hecho, ahorrará dinero en costos operativos a largo plazo. No olvidemos que los ataques informáticos no son selectivos, le pueden suceder a cualquiera. Tiene sentido invertir un poco más para proteger sus datos que pagar enormes multas por incumplimiento y control de daños.

Mito 05:
Solo funciona on-premises

Realidad:

En los últimos años hemos visto un tremendo crecimiento en la adopción por parte de las organizaciones de soluciones en la nube y pasando a entornos en la nube o híbridos. De la misma forma, Zero Trust implementada en el lugar se puede extender a soluciones en la nube con métodos de seguridad en la nube.

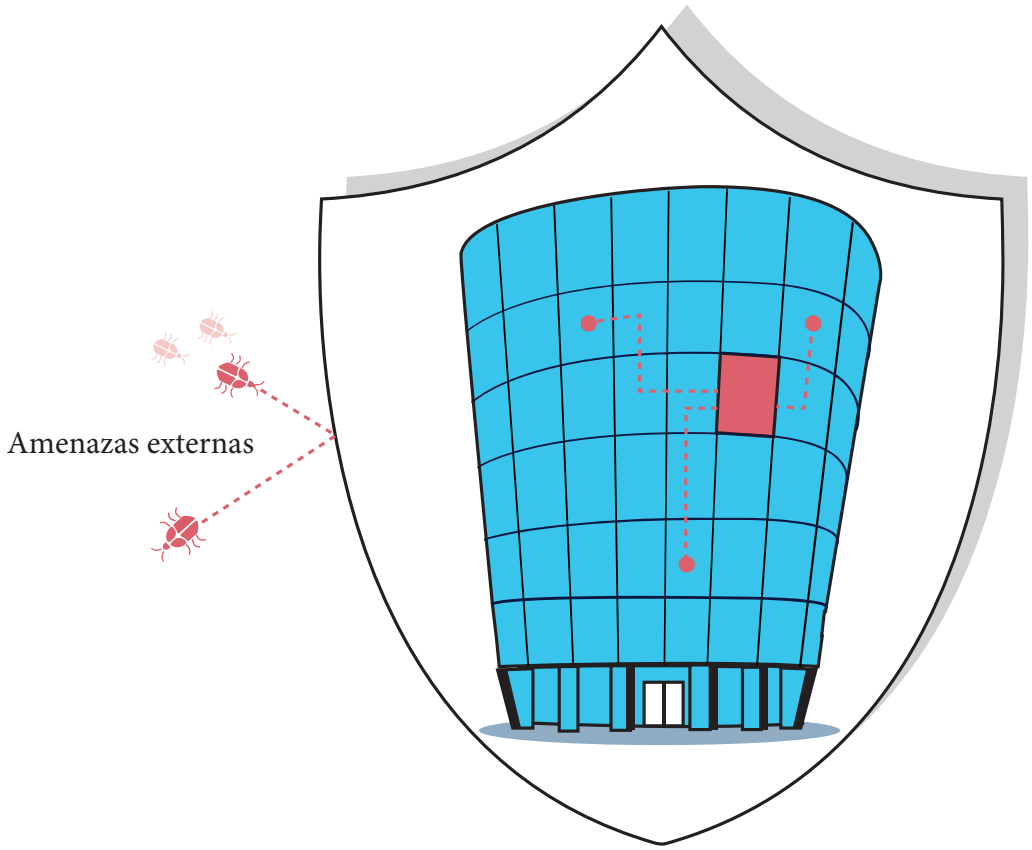
Mito 06:
La experiencia del usuario y la productividad se verán afectadas

Realidad:

Podría parecer una dificultad limitar el acceso y verificar las identidades con cada sesión, pero con las herramientas, flujos de trabajo y políticas correctos, es posible dar una experiencia intuitiva. Estudiar el comportamiento de los usuarios nos permite eliminar solicitudes de autenticación para perfiles de riesgo bajo y disminuir los tiempos de espera de manera consistente. Además, Zero Trust aumenta la productividad en el lado de los administradores. Una vez que un empleado abandone la organización, garantiza automáticamente que no tenga acceso a recurso alguno. No hay espacio para el error manual. En su lugar, el equipo de administradores puede enfocarse en otras tareas críticas.

1.3 Evaluar el modelo de seguridad de ManageEngine

El modelo tradicional de castillo y foso funciona bajo el supuesto de que todos en la red son de confianza. Elimina amenazas y vulnerabilidades externas, pero toma en cuenta a los usuarios o dispositivos internos. Esta fue la estrategia estándar por casi 20 años. Ahora está desactualizada.



El modelo tradicional de seguridad basado en el perímetro

El modelo de seguridad basado en el perímetro funcionaba cuando ManageEngine tenía empleados trabajando en la oficina todos los días. Se otorgaba acceso a la información solo mediante el Wi-Fi corporativo. Antes de la pandemia, trabajar desde casa no era aún la moda. Aparte de los equipos de desarrollo y algunos empleados remotos, ManageEngine no tenía un requisitos importante para la VPN. Cuando la pandemia llegó, todos pasaron a trabajar remotamente. Al mismo tiempo, contratamos nuevos empleados para varios equipos.

En este punto ManageEngine enfrentó cinco retos principales:

1. Capacidad

Hubo un surgimiento sin precedentes de usuarios de la VPN. Enfrentamos inconvenientes como rendimiento lento y problemas de conectividad cuando usábamos datos móviles. En una semana, debimos bloquear algunos sitios no relacionados con el trabajo para optimizar el ancho de banda.

2. Verificación limitada

Se otorgaba el acceso a la VPN con solo el nombre de usuario y contraseña. ¿Era esta una forma segura de verificar la identidad del usuario? Por supuesto que no. Incluso si un empleado descuidado usaba una aplicación de notas para almacenar sus contraseñas o tenía una contraseña genérica como “ManageEngine123”, éramos vulnerables a ataques.

3. Visibilidad

Los logs de la VPN no son exhaustivos, por lo que no podíamos saber quién accedía a qué, una función esencial que no podíamos comprometer.

4. Control de acceso

No pudimos retirar privilegios de dispositivos o cuentas comprometidas. La carga recayó en la aplicación como tal.

5. Costos

Durante la pandemia, Zoho inauguró más de 30 oficinas de distribución en India como parte de nuestra iniciativa de recuperación rural. Escalar la VPN para todas las oficinas de distribución fue costoso debido a que usábamos el servicio de un tercero.

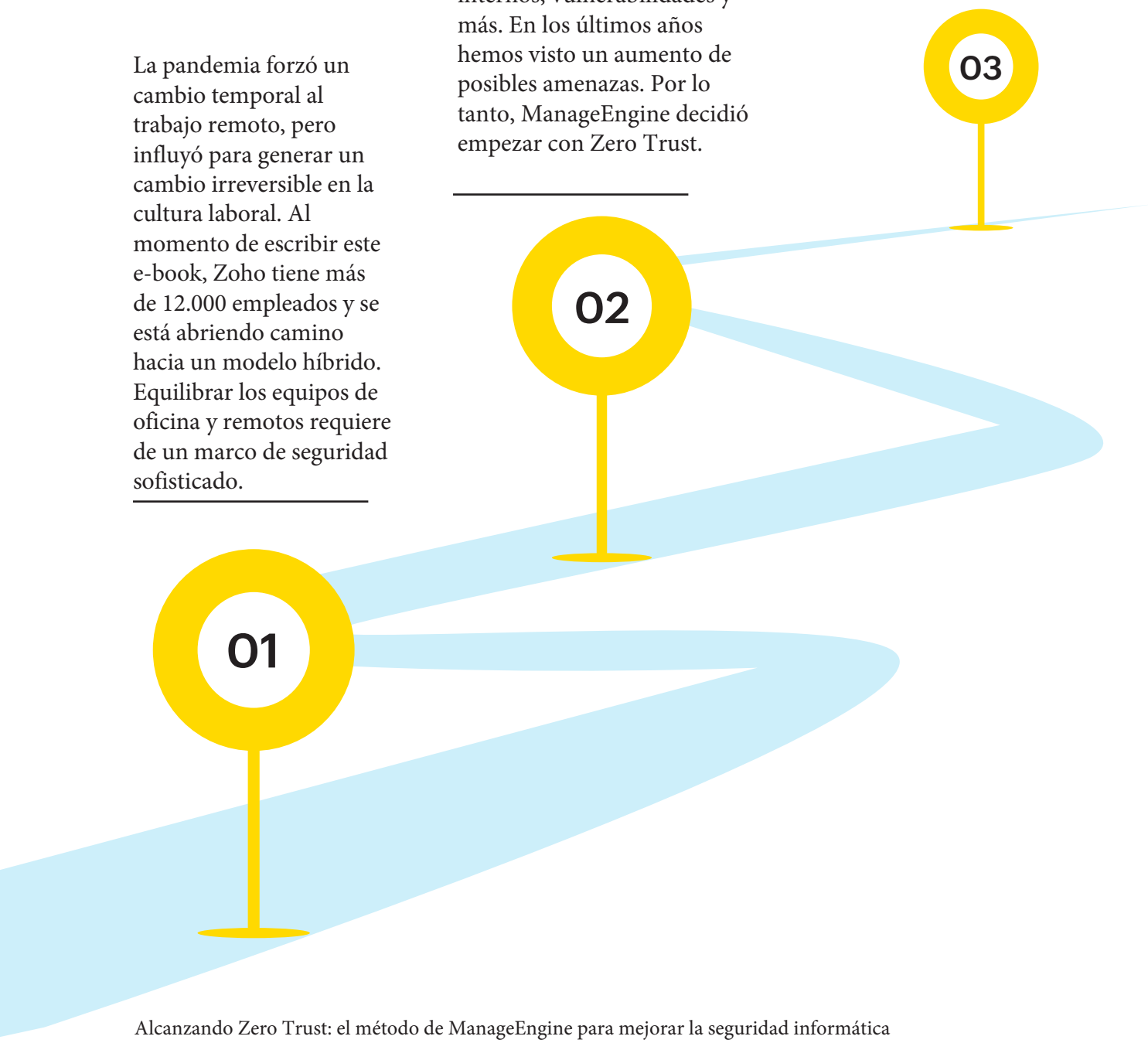
Se hizo evidente para el equipo de administradores que teníamos que ir más allá en su seguridad para mantener la compañía en su movimiento usual. Nuestro equipo de seguridad se puso manos a la obra, era tiempo de encontrar una alternativa más segura que la VPN.

1.4 ¿Por qué decidimos iniciar ahora nuestro viaje hacia Zero Trust?

La pandemia forzó un cambio temporal al trabajo remoto, pero influyó para generar un cambio irreversible en la cultura laboral. Al momento de escribir este e-book, Zoho tiene más de 12.000 empleados y se está abriendo camino hacia un modelo híbrido. Equilibrar los equipos de oficina y remotos requiere de un marco de seguridad sofisticado.

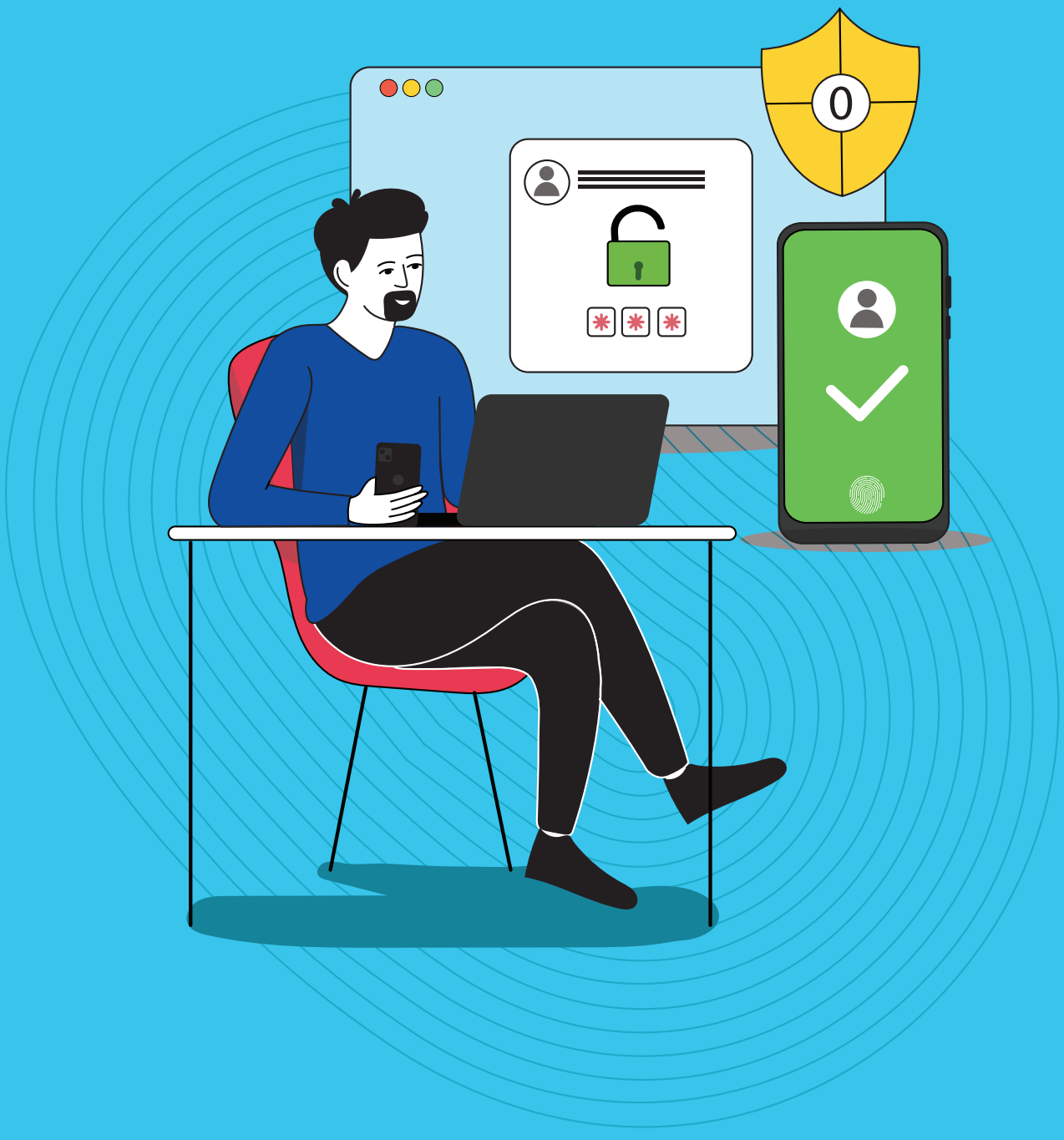
Una empresa exitosa siempre es el objetivo más grande de los ataques informáticos; esto es inevitable. Está en riesgo de amenazas externas siempre cambiantes, ataques internos, vulnerabilidades y más. En los últimos años hemos visto un aumento de posibles amenazas. Por lo tanto, ManageEngine decidió empezar con Zero Trust.

Zero Trust no es infalible. Aún hay espacio para ataques, pero Zero Trust es una forma adicional de protección en la que toda organización debe invertir.

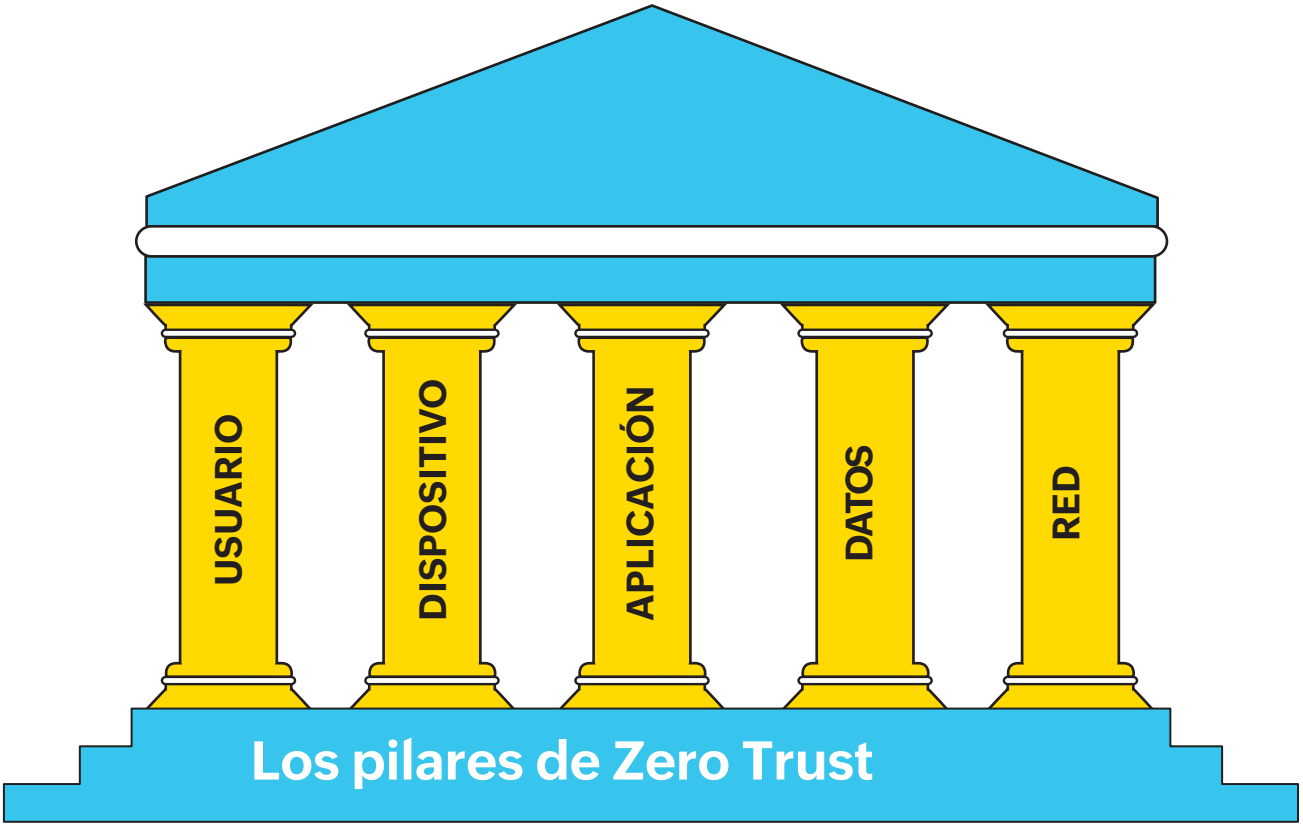


Capítulo 2

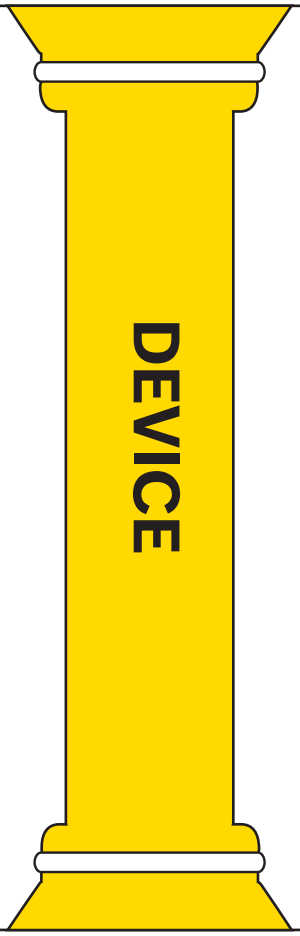
Marco de Zero Trust de ManageEngine.



2.1 Los pilares de Zero Trust



La autenticación, autorización y el constante monitoreo son nuestros enfoques con la identidad de los usuarios. Validamos la honradez de los usuarios para tomar decisiones sobre privilegios. Nuestro sistema de Zero Trust, conocido como 0Trust, mantiene una lista de empleados y sus departamentos al sincronizarse con nuestra herramienta de RR. HH. Cuando los empleados se unen a la compañía, cambian de roles o la dejan, los cambios se reflejan en el sistema 0Trust mediante webhooks. Se les da a los empleados acceso a los recursos con base en sus roles. Los proveedores de identidad ayudan en el proceso de verificación al proporcionar una lista de usuarios para que el sistema los valide.



Como con la identidad de los usuarios, los dispositivos se deben verificar cada vez que haya una solicitud de acceso. En Zoho tenemos más de 12.000 empleados, y cada usuario tiene al menos dos dispositivos. El sistema 0Trust de Zoho mantiene un inventario de estos dispositivos. Cada dispositivo tiene una identificación única mediante un certificado instalado a nivel raíz. Los empleados no tienen acceso de raíz. Para identificar las solicitudes de conexión de dispositivos gestionados, aplicamos una autenticación de SSL de dos vías, en la que el cliente y el servidor validan la identidad del otro.

Se monitorean los dispositivos mediante nuestra solución para la gestión unificada de endpoints. La verificación de los dispositivos depende de dos cosas: evaluaciones de riesgos y prevención de pérdida de datos (DLP). Las soluciones para DLP buscan proteger los datos a como dé lugar. Esto se logra mediante los siguientes métodos:

- Auditoría y análisis de archivos: monitoreo de la actividad de los usuarios en los archivos y evaluación de las vulnerabilidades
- Descubrimiento y clasificación de datos: ubicación y etiquetado de datos sensibles
- DLP para endpoints: monitoreo de transferencias de datos

- **2FA**

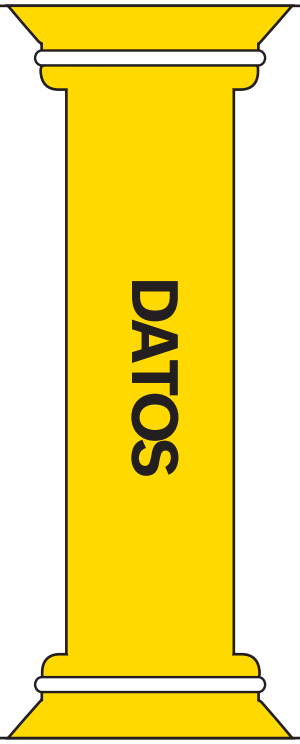
Usar herramientas de MFA como 2FA es una forma de garantizar que los empleados tienen permisos adecuados y de evitar el acceso no autorizado. La capa de aplicación depende del usuario, dispositivo y datos de la red. Para proteger más las identidades, pasamos hacia un inicio de sesión sin contraseñas junto con una verificación biométrica para empleados en nuestra aplicación interna de MFA.

- **SSO**

Los empleados se deben autenticar con factores primarios y secundarios, y se les asignará tokens temporales después de la autorización para acceder a recursos específicos.

- **CASB**

Monitoreamos cargas y descargas en aplicaciones web y restringimos el uso de aplicaciones ocultas no autorizadas al validarlas con respecto a listas de aplicaciones permitidas, listas de bloqueo y puntuaciones de reputación.



Los recursos se identifican, categorizan y encriptan de extremo a extremo. Luego, habilitamos el acceso con mínimos privilegios para todos los datos de la organización. Los datos se pueden calificar con base a su propósito, confidencialidad y otros factores.

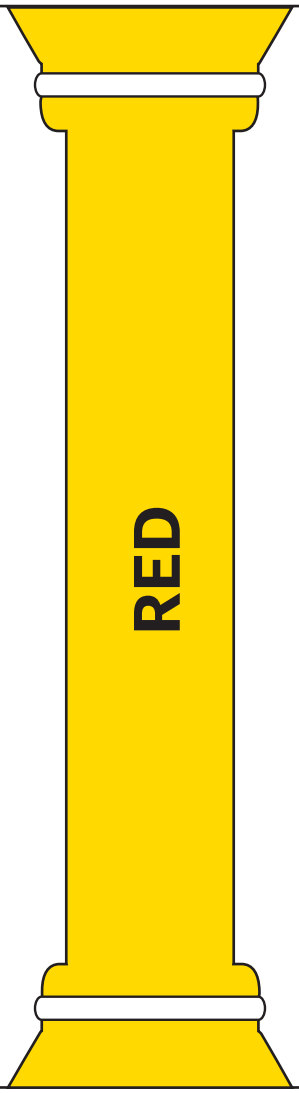
Por ejemplo:

- **Propósito:**

Todos los empleados pueden acceder al correo electrónico, mientras que las políticas organizacionales y SOP deberían ser de solo lectura con acceso restringido a la edición.

- **Confidencialidad:**

Los salarios de los empleados, datos de los clientes y códigos fuente de productos son ejemplos de datos que deberían restringirse.



- **Microsegmentación:**

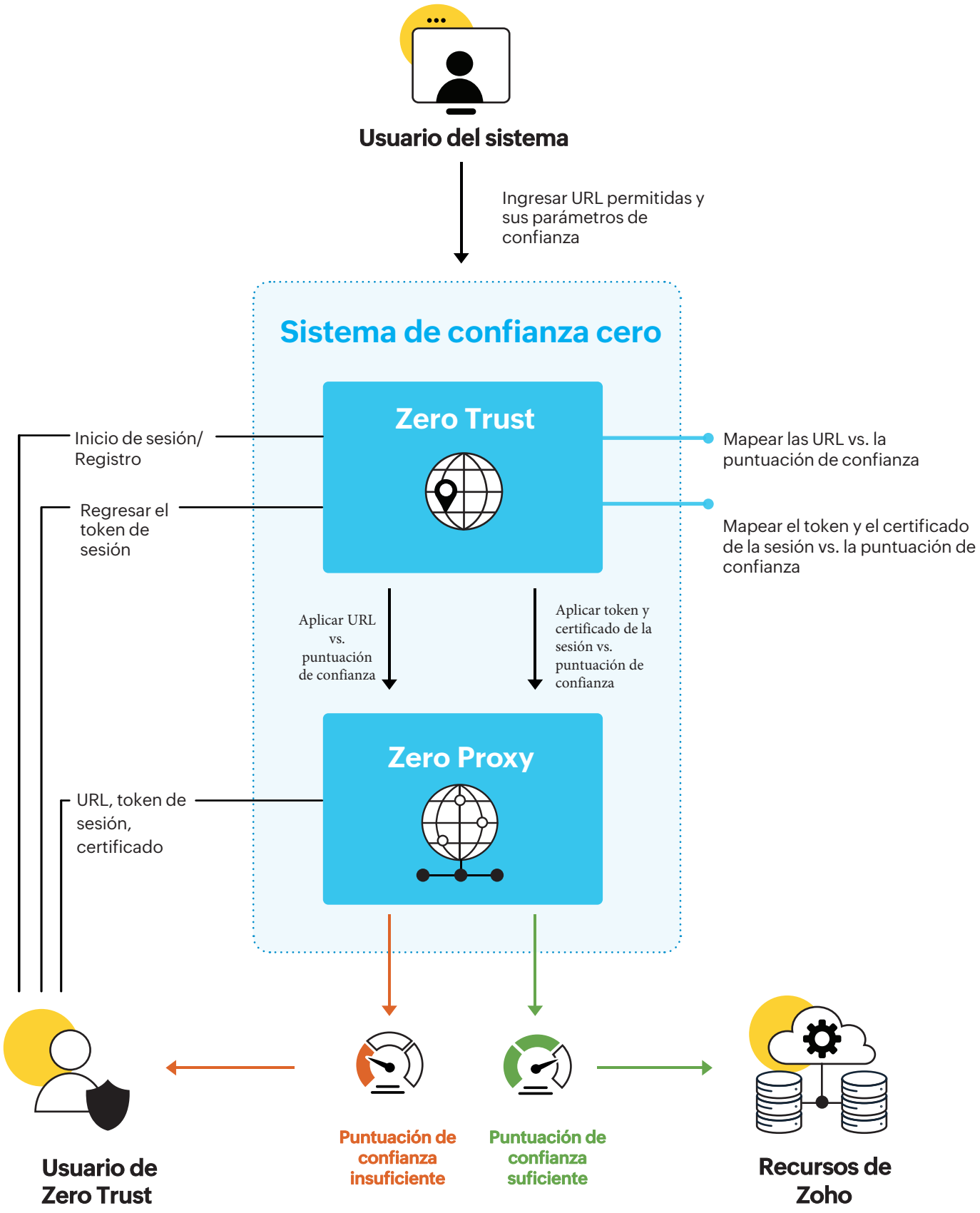
Una de las ventajas de la confianza cero es la capacidad de segmentar y monitorear el perímetro de su red. La microsegmentación es la práctica de dividir una red grande en segmentos más pequeños y aislados, de forma que las compañías puedan monitorear y controlar fácilmente el tráfico.

- **0Proxy:**

0Proxy es un proxy inverso hacia la internet. Se asume que el tráfico siempre proviene de una red no confiable y se enruta mediante 0Proxy, que filtra las solicitudes con base en sus puntuaciones de confianza asociadas.

- **Puntuaciones de confianza:**

Se utiliza un sistema de puntuaciones de confianza para evaluar si se le debería dar a una persona acceso a la red y datos de la organización, y si es así, cuánto. Los administradores pueden usar una escala de 0-1 o de 0-100 para calificar las actividades de cada solicitud de acceso de usuarios, dispositivos y redes con base en cualquier número de parámetros. En ManageEngine usamos una escala de 0-100 para puntuar cada inicio de sesión.


Usuario del sistema
Ingresar URL permitidas y sus parámetros de confianza
Sistema de confianza cero
Zero Trust
Inicio de sesión/ Registro
Regresar el token de sesión
Mapear las URL vs. la puntuación de confianza
Mapear el token y el certificado de la sesión vs. la puntuación de confianza
Aplicar URL vs. puntuación de confianza
Aplicar token y certificado de la sesión vs. puntuación de confianza
Zero Proxy
URL, token de sesión, certificado
Usuario de Zero Trust
Puntuación de confianza insuficiente
Puntuación de confianza suficiente
Recursos de Zoho

Sistema de puntuación de la red

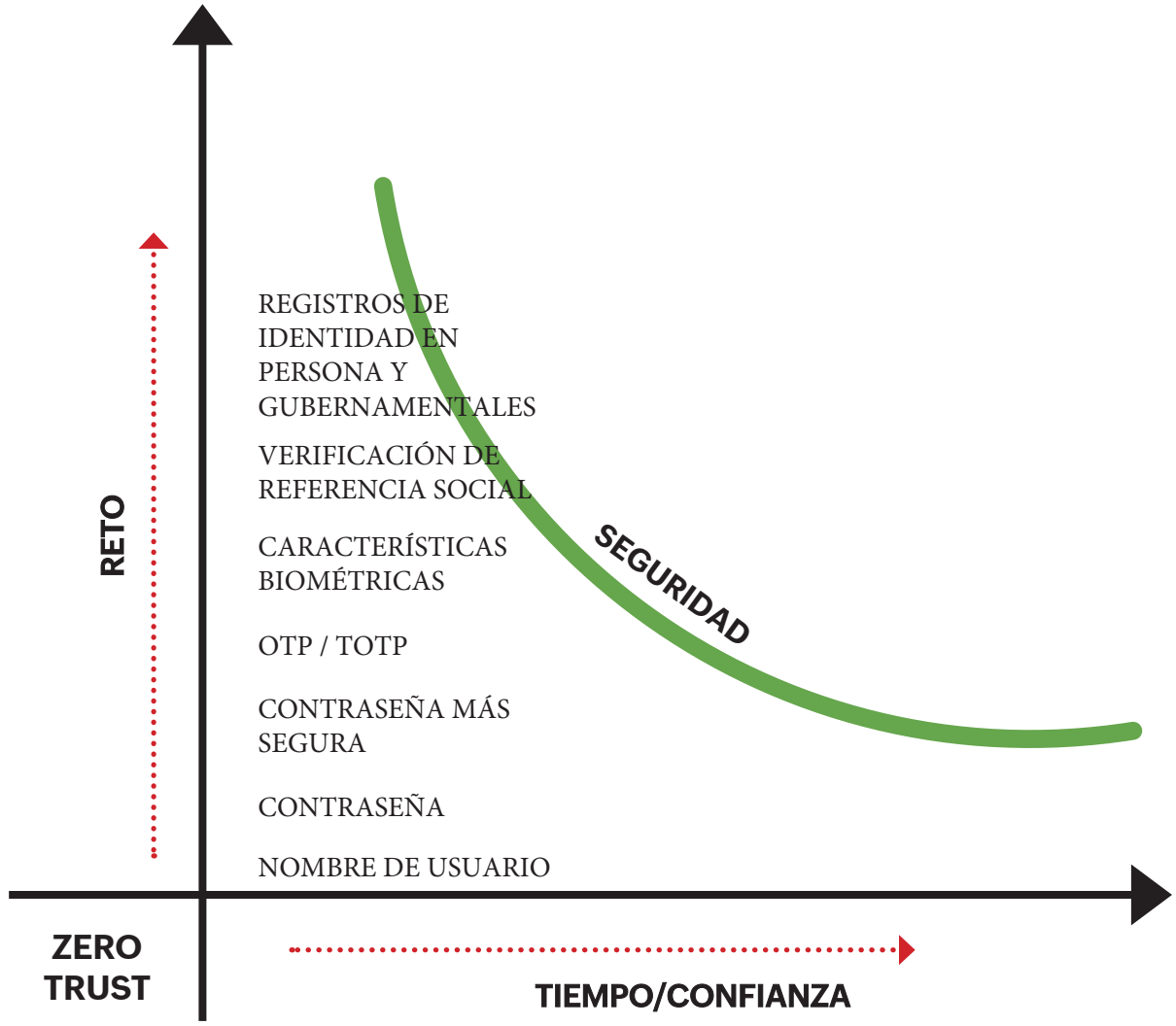
Parámetro	Puntuación de muestra
IP de confianza	40
IP anónima	30
IP sospechosa	30

Sistema de puntuación de usuarios

Parámetro	Puntuación de muestra
Sin intentos inválidos de inicio de sesión	30
Sin credenciales comprometidas	30
Sin tiempo anómalo de inicio de sesión	15
Sin ubicación anómala de inicio de sesión	11
Sin dispositivos anómalos de inicio de sesión	4
Tiene una buena seguridad de contraseña	10

Sistema de puntuación del dispositivo

Parámetro	Puntuación de muestra
Requiere una contraseña para desbloquear	10
Tiene una versión de SO no vulnerable	10
No tiene plug-ins, add-ons o extensiones sospechosos	10
No tiene aplicaciones o paquetes sospechosos	10
No tiene versiones vulnerables de aplicaciones o paquetes	10
No tiene procesos o servicios sospechosos en ejecución	10
No ha visitado ningún sitio vulnerable o sospechoso	8
No está disponible el acceso jailbreak o rooteado	8
Se instala y ejecuta software de antivirus	6
El firewall está habilitado	6
No hay puertos de escucha abiertos	4
El arranque seguro está habilitado	3
La verificación de la integridad del driver está habilitada	3
El almacenamiento de datos está encriptado en reposo	2



El nivel de acceso que se le otorga a un empleado depende de la puntuación de confianza asignada a cada sesión, la cual se calcula con base en factores como dispositivo, usuario y tiempo.

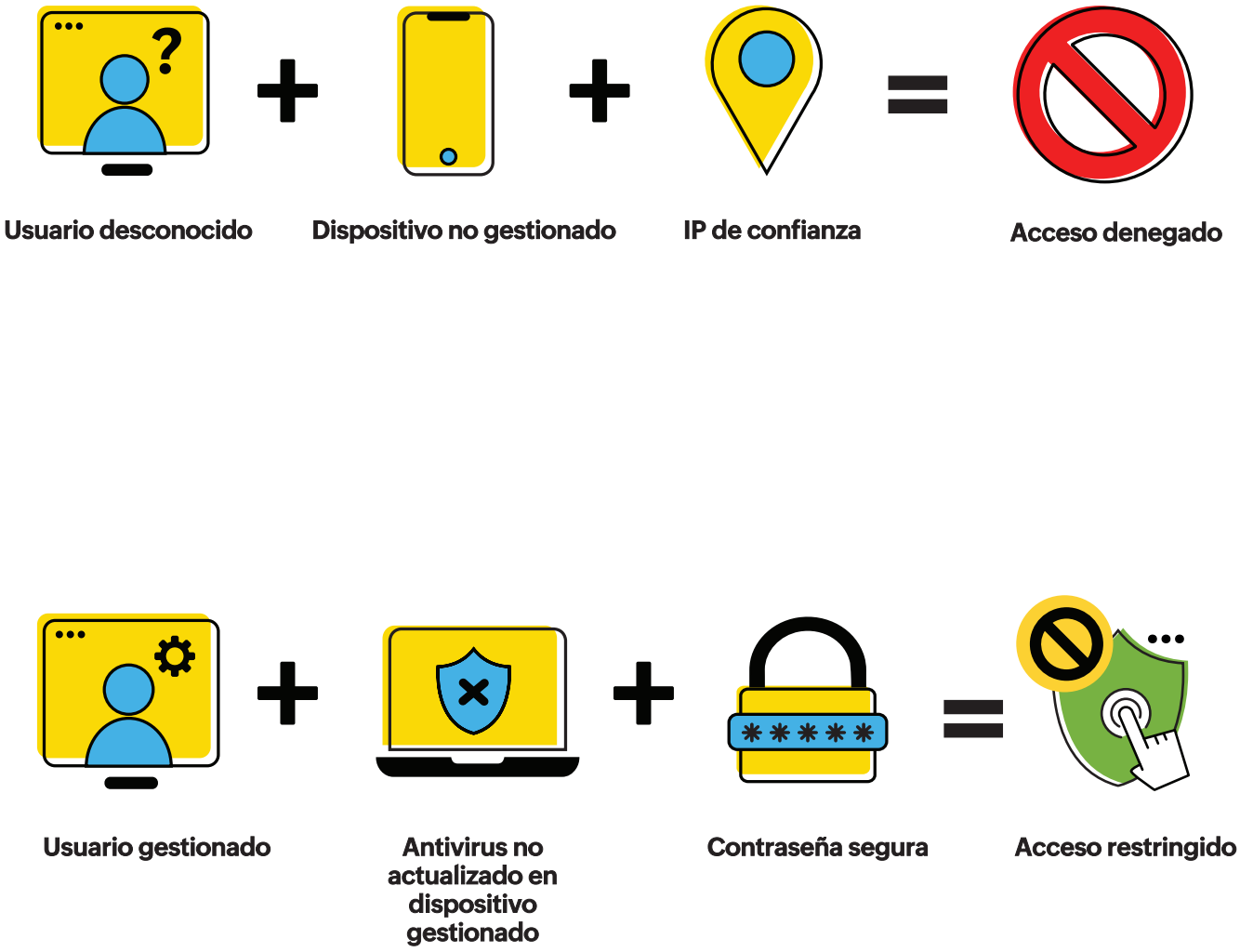
Dispositivo:

Un dispositivo gestionado tendrá una puntuación de confianza mayor que un dispositivo no gestionado. Parámetros como su estado de antivirus, su ubicación de acceso y si su SO tiene el último parche influyen en esto.

Usuario:
Parámetros como los recursos y la severidad de la autenticación (como las características biométricas o 2FA) influyen en el acceso basado en roles.

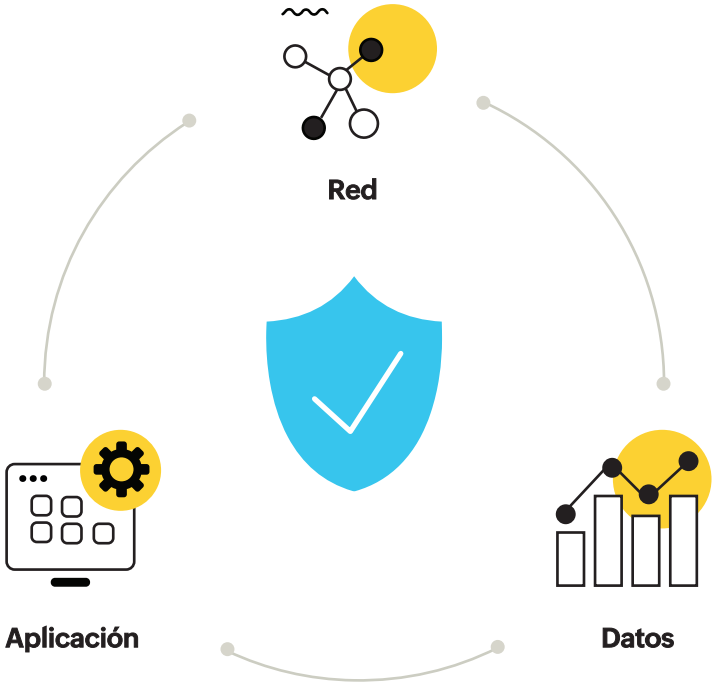
Tiempo:
Las puntuaciones de confianza se modifican periódicamente con base en el tiempo de la sesión.

Incluso si el CEO usa un dispositivo que no está inscrito en la herramienta para la gestión de endpoints, se restringirá el acceso a datos públicos (es decir, los datos que requieren una puntuación de confianza mínima de 10/100). Con el fin de acceder a la información financiera sensible, el CEO debe usar un dispositivo propiedad de la compañía.



Control de acceso basado en puntuaciones de confianza

2.2 Zero Trust y la arquitectura de Zero Trust: ¿Cuál es la diferencia?



Zero Trust y la arquitectura de Zero Trust son conceptos que se usan de manera intercambiable. ¿A qué se refiere exactamente? Zero Trust es un método de seguridad basado en principios guía. La arquitectura de Zero Trust es un concepto más amplio que aplica estos principios para abordar tres modelos de seguridad diferentes:

- Acceso a la red de Zero Trust **(ZTNA)**
- Acceso a los datos de Zero Trust **(ZTDA)**
- Acceso a aplicaciones de Zero Trust **(ZTAA)**

ZTNA	ZTAA	ZTDA
Conexión usuario a red	Conexión usuario a aplicación	Conexión usuario a datos
Se puede considerar un reemplazo evolucionado para una VPN que protege la red	Protege aplicaciones al permitir el acceso solo después de la autenticación del usuario y del dispositivo	Restringe el acceso a los datos hasta que el usuario proporcione la autorización y se verifique su identidad

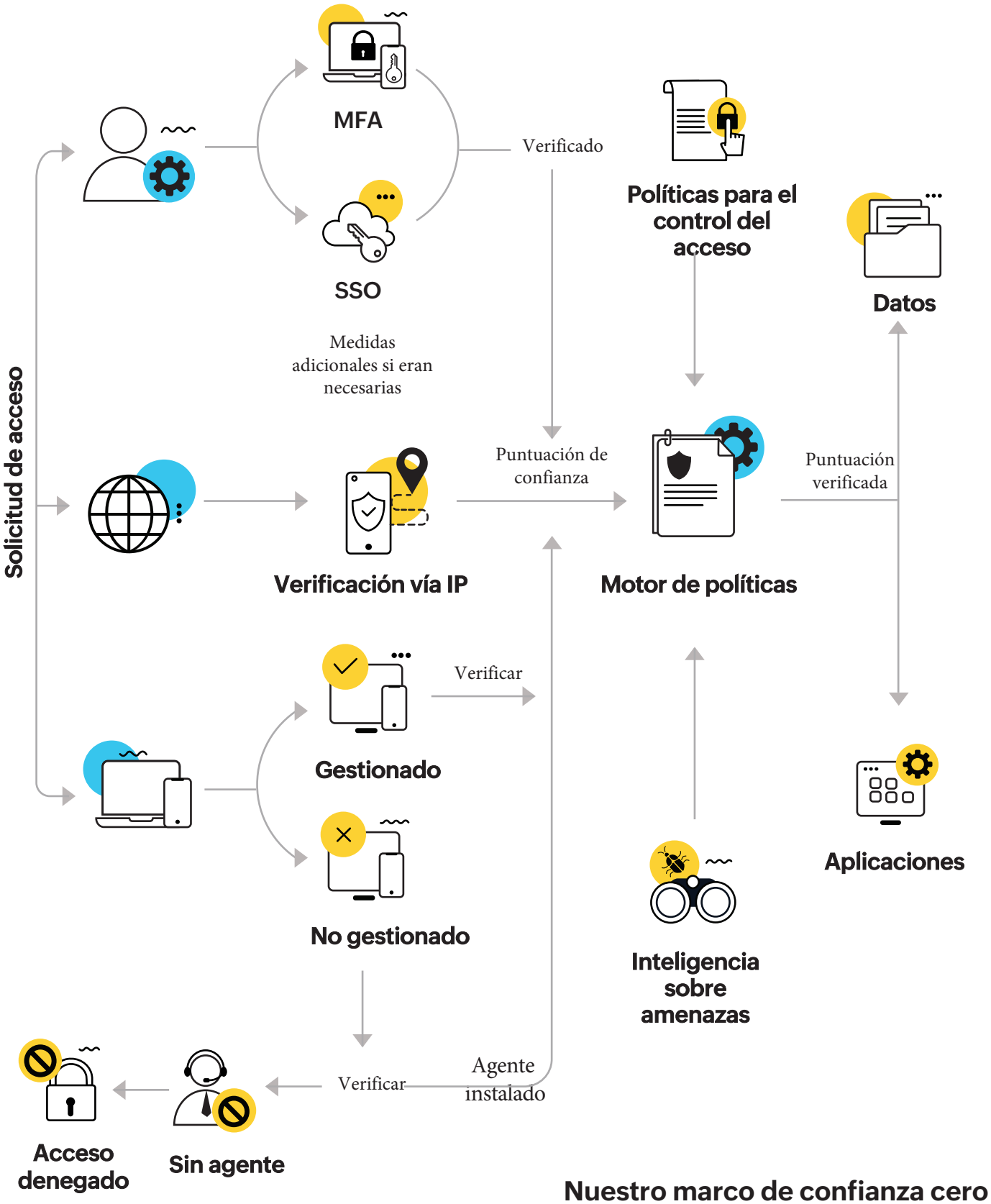
2.3 Migrar a la confianza cero

Hablar a nuestro equipo de Zero Trust nos dio una mejor idea de nuestras metas y hoja de ruta. En palabras del equipo, “Zero Trust es un servicio de front-end, como una puerta que nos lleva a una habitación. No se puede confiar solo en la puerta y no tener muros. Es inútil. Zero Trust es una medida de seguridad adicional que debería combinarse con servicios de protección de back-end”.

Nuestras metas eran:

- Implementar Zero Trust en toda la organización.
- Depender de la identificación del usuario y del dispositivo.
- Hacer que nuestros parámetros de verificación fueran más estrictos.

Alcanzar estas metas tomaría tiempo, por lo que llevamos a cabo nuestro plan de Zero Trust en fases.


MFA
SSO
Verificado
Políticas para el control del acceso
Datos
Medidas adicionales si eran necesarias
Solicitud de acceso
Puntuación de confianza
Puntuación verificada
Verificación vía IP
Motor de políticas
Verificar
Gestionado
No gestionado
Aplicaciones
Inteligencia sobre amenazas
Verificar
Agente instalado
Acceso denegado
Sin agente
Nuestro marco de confianza cero

Fase 1

Objetivos:

- Identificar grupos de usuarios con base en sus roles y acceso requerido.
- Identificar flujos de red y tratar de registrarlos todos en 0Trust.

Primero, establecimos una política de inscripción de dispositivos para los empleados:

1. Deben usarse solo los dispositivos propiedad de la compañía para acceder a los recursos de Zoho.
2. Todos los dispositivo deben inscribirse primero en nuestra solución de gestión de dispositivos móviles (MDM) (en el caso de teléfonos) y nuestra solución para la gestión unificada de endpoints (en el caso de laptops y desktops). Esto es para garantizar que los dispositivos están protegidos de forma predeterminada y monitoreados en busca de vulnerabilidades y posibles intentos de hackeo.
3. Se debe evitar el acceso a los recursos de Zoho usando dispositivos que no sean propiedad de la compañía. Dicho acceso se restringió a recursos que son públicos y en definitiva que no tuvieran que ver con repositorios de clientes y de fuentes.
4. Los empleados que necesitan acceso raíz para sus dispositivos tendrán acceso restrictivo a un entorno no productivo.
5. Si un desarrollador desea acceder a un entorno de producción, debe usar un dispositivo distinto para el cual no tenga acceso raíz. Esto es para garantizar que todos los controles están intactos en el dispositivo utilizado para acceder al entorno de producción.

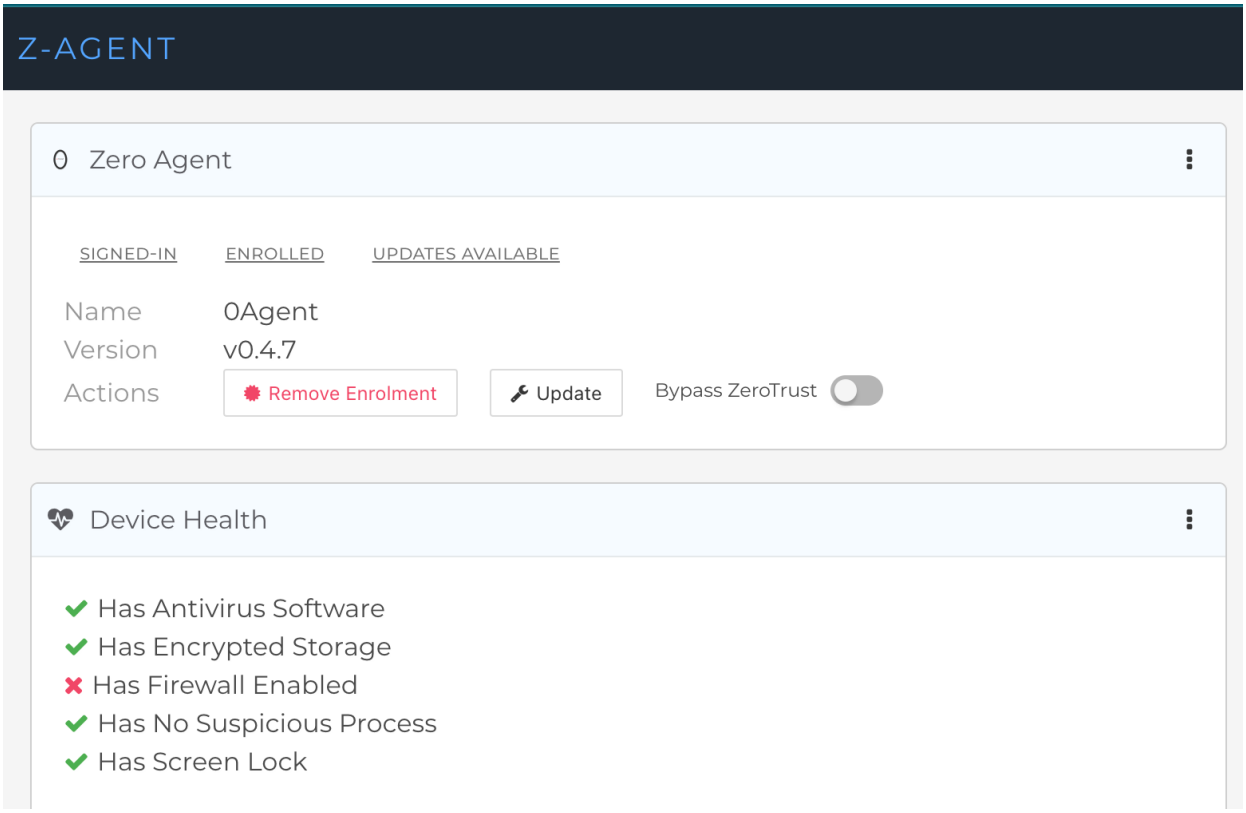
En las etapas tempranas los recursos estaban disponibles mediante 0Proxy y la VPN externamente, y mediante 0Proxy y la red corporativa internamente. Era muy temprano para abandonar la VPN, pero era tiempo para una actualización. En lugar de depender de la tradicional verificación nombre de usuario-contraseña, añadimos 2FA y UEBA.

Nuestro sistema UEBA compila perfiles basados en el comportamiento de los usuarios y entidades en la organización y asigna una puntuación de riesgo cuando el comportamiento se desvía de la referencia normal antes establecida. Esto ayuda a identificar cuentas comprometidas, robo de datos y amenazas internas, lo que sirve como herramienta de diagnóstico y como sistema temprano de advertencia.

El sistema UEBA es altamente personalizable, lo que nos da un control completo sobre los tipos de anomalías que se deben detectar. Se adapta a patrones cambiantes de datos automáticamente sin intervención alguna y puede implementarse en cualquier dominio, en tanto la configuración de los tipos de anomalías que se deben detectar se haga correctamente. ZLabs, el equipo de I+D de Zoho, ha presentado una patente provisional sobre el diseño de nuestro motor de UEBA.

La fase 1 se trató de experimentar. Para empezar con ella tuvimos 250 usuarios voluntarios de los departamentos corporativo y TI de Zoho para evaluar nuestro sistema 0Trust. Por ejemplo, un líder que no requiere acceso a herramientas de desarrollo inició sesión para la prueba de 0Trust en las etapas tempranas. Escogió participar debido a que sentía que usar la VPN para acceder a recursos internos conllevaba un rendimiento insuficiente de las aplicaciones. Todo, desde implementaciones y estadísticas de rendimiento compiladas a reuniones mediante la VPN, con frecuencia causaban problemas como una mala calidad en el audio y video.

Tras la creación de una cuenta de usuario, un usuario puede ver la salud y puntuación de confianza de su dispositivo. Esto les ayudo a entender lo que podían hacer para mejorar su puntuaciones de confianza y cumplir con las políticas.



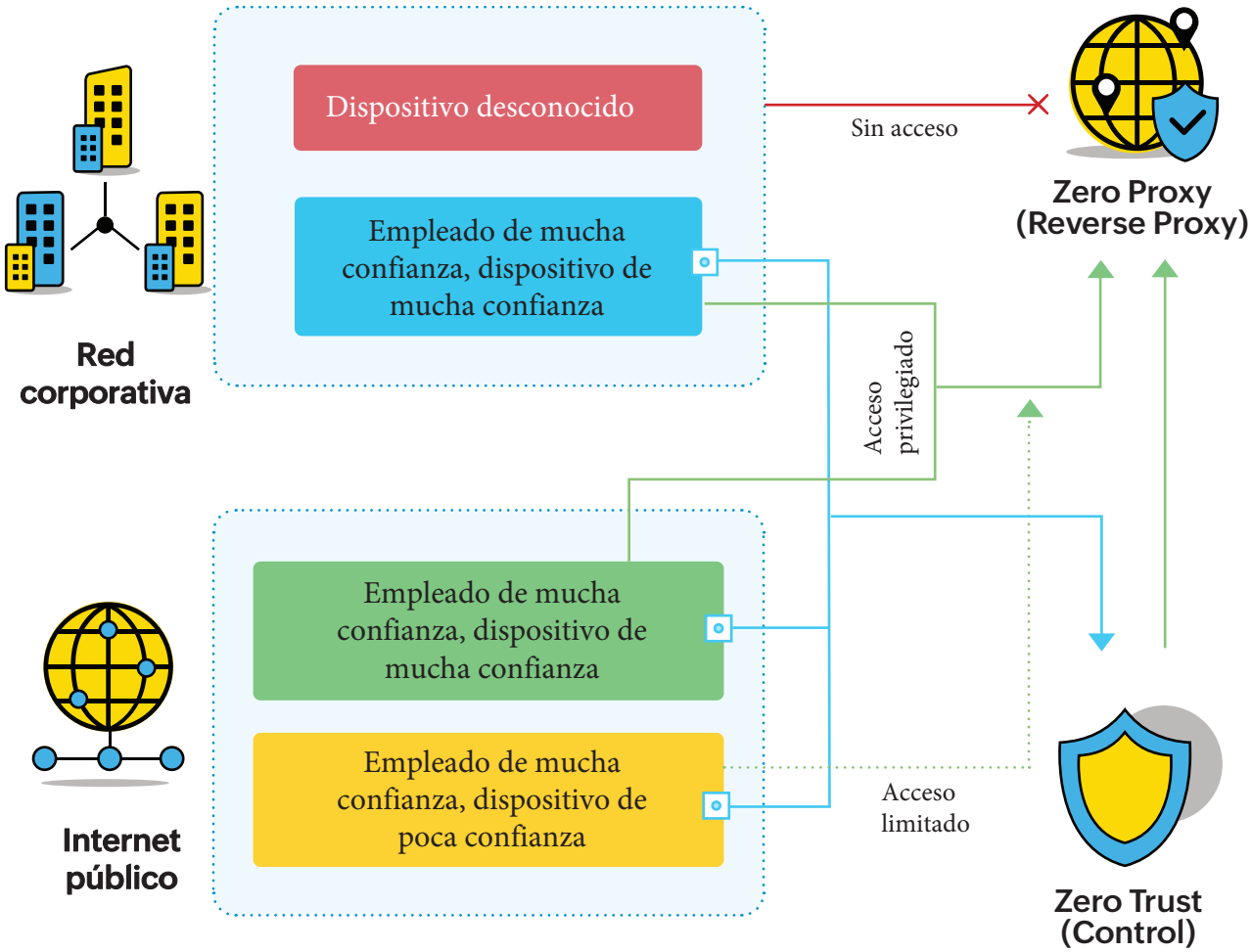
Cuando el usuario inició su sistema, 0trust se activó automáticamente. Si deseaba añadir un dominio específico al sistema 0Trust, debía generar una solicitud al equipo de Zero Trust. Si el equipo de seguridad podía validarlo, el dominio se asignaba al sistema local.

Luego de iniciar sesión en 0Trust, el mencionado líder infirió que el rendimiento de la aplicación había mejorado considerablemente. También redujo la carga en los servidores proxy de Zoho, lo que fue una situación de ganar-ganar.

Fase 2

Objetivos:

- Enrutar el tráfico de todos los empleados mediante 0Proxy.
- Monitorear el tráfico y registrar el tráfico inválido, pero otorgar acceso si un usuario accede mediante la VPN o la red corporativa. Analizar el tráfico fallido e intentar abordar ese caso.
- Monitorear el uso de VPN por parte de los usuarios. Si todo su flujo se puede canalizar mediante 0Trust, los animaremos a usar siempre 0Trust.
- Monitorear el uso de VPN por parte de los usuarios. Si no se accede por un periodo determinado, revoca su acceso.
- Restringir el acceso a VPN a usuarios solo con necesidades comprobadas.



Acceso mediante confianza cero

Nuestra oficina de distribución en Madurai fue una de las primeras en registrarse para la prueba de 0Trust. Tiene cerca de 100 empleados de distintos equipos, fue la ubicación perfecta para empezar debido a su pequeño tamaño.

Antes de la pandemia, los miembros de este equipo trabajaban en nuestra sede de Chennai, por lo que usaban la red local. La mayoría de las personas ni siquiera sabían cómo funcionaba la VPN. Luego de la reubicación a la oficina de Madurai, tuvieron que usar la VPN para sus operaciones diarias. En esta situación, la seguridad se volvió un inconveniente.

Hubo dos problemas al usar nuestra VPN. Uno, hubo problemas de conectividad cuando se accedía a la VPN mediante datos móviles. Dos, los usuarios tenían que iniciar sesión cada vez que desbloqueaban sus dispositivos. Así que, varias veces al día, luego de tomar un descanso, comer algo o tener una charla rápida con un colega, debían iniciar sesión en cada momento. Para evitar esto, algunos empleados dejaban sus dispositivos desbloqueados, lo que va en contra de nuestras políticas de seguridad.

Al mismo tiempo, nuestros líderes de desarrollo empezaron a preguntarse: "¿Se requiere la VPN para que los nuevos empelados accedan?". Los nuevos miembros que se unían a equipos de desarrollo no requerían acceso a todos los recursos internos que la VPN otorgaba.

Presentamos 0Trust. Ahora, el sistema puede mantener las sesiones iniciadas y reconectarlas automáticamente. No obstante, esta transición no se dio de la noche a la mañana. Instalar 0Trust en cada sistema fue tedioso. Aquí fue cuando nuestro administrador de sistemas introdujo 0Agent. Instalar 0Agent (mediante la aplicación de MDM) hizo que el cambio a 0Trust fuera sencillo, casi como trabajar desde la oficina de Chennai. De la misma forma, se les dio acceso a los nuevos empleados con base en sus requisitos, como operaciones Git. Se otorgó el acceso después de una evaluación preliminar de seguridad, para la cual los empleados debían revisar exhaustivamente las políticas de seguridad y realizar una prueba de conciencia de seguridad.

Hoy, la oficina de distribución de Madurai funciona casi completamente con 0Trust. Cerca del 5% de los servicios aún necesita VPN, que se desechará cuando el equipo resuelva los problemas. El éxito de esta prueba fue una indicación de que íbamos en la dirección correcta y que estábamos listos para la siguiente etapa.

Fase 3

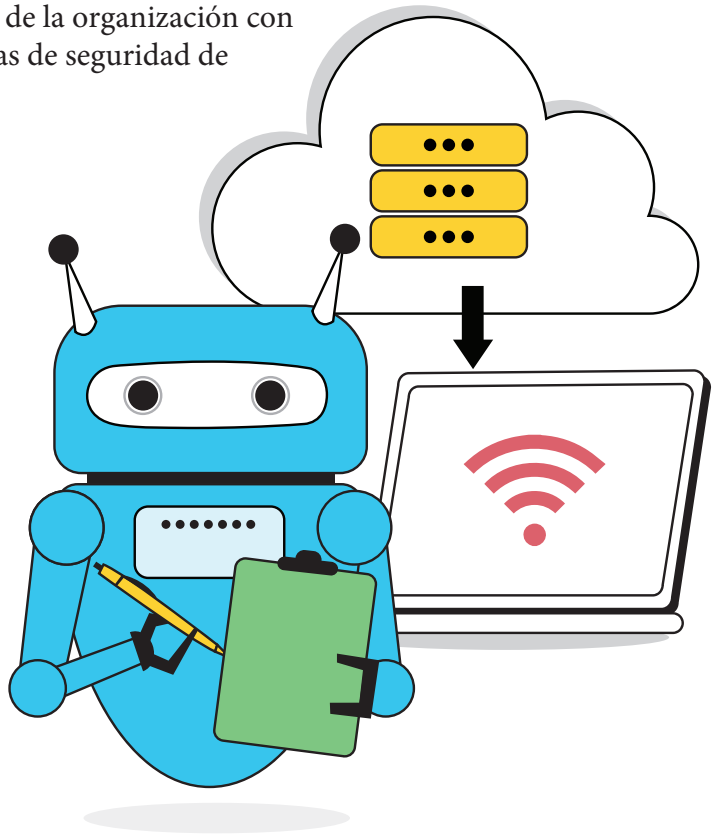
Objetivos:

- Enrutar todo el tráfico mediante 0Proxy en modo bloqueo. Bloquear el flujo si no se cumplen los criterios de confianza.
- Restringir las cuentas de Zoho de nuestros servicios en la nube para aceptar solicitudes solo de IP de 0Trust usando la restricción de IP en nuestra solución para IAM.

Antes, si usted estaba usando el Wi-Fi corporativo, tendría acceso a sitios internos, sin importar su rol. Ahora que estamos en la Fase 3, al continuar trabajando con Zero Trust, buscamos cambiar eso. En última instancia, incluso si un empleado inicia sesión mediante el Wi-Fi corporativo, necesitará 0Trust para acceder a la información confidencial.

Durante la fase de desarrollo el equipo trabaja en arreglar los obstáculos, como el escalamiento para todas las aplicaciones y dispositivos de forma confidencial. Una vez se arreglaron estos problemas, haremos 0Trust obligatorio para todos los empleados. El Administrador instalará 0Agent en todos los sistemas.

El equipo de Zero Trust se ha asociado con un tercero para monitorear las fugas de credenciales. Nuestros administradores también dependen de la inteligencia de amenazas, un servicio independiente desarrollado por el equipo de seguridad y que proporciona información sobre vulnerabilidades para ayudar a mitigar posibles ataques. El objetivo de la inteligencia de amenazas es permitir una resolución rápida de problemas de seguridad. Nuestros equipos se conectan con analistas externos sobre plataformas de inteligencia de amenazas para combinar datos locales de la organización con datos globales y para alinear sus estrategias de seguridad de conformidad.



2.4 Factores que influyen en Zero Trust

1. Políticas para el control del acceso

Para que un sistema de Zero Trust maneje la autenticación y autorización, necesita instrucciones, como políticas de sesiones y contraseñas. El equipo de seguridad suele establecer estas políticas con base en las entradas del administrador de sistemas.

Políticas de sesión

Parámetro	Límite de la muestra
Vida útil de la sesión	Cerrar sesión luego de un día
Pausar sesión inactiva	Eliminar sesiones inactivas luego de un día
Sesiones simultáneas	Permitir cinco sesiones simultáneas

Políticas de contraseñas

A. Complejidad

Parámetro	Instrucción de la muestra
Longitud mínima de la contraseña	Ocho caracteres
Número mínimo de caracteres numéricos	Uno
Número mínimo de caracteres en mayúscula	Uno
Número mínimo de caracteres en minúscula	Uno
Número mínimo de caracteres especiales	Uno

B. Gestión

Parámetro	Instrucción de la muestra
Reutilización de contraseñas	No permitir la reutilización de contraseñas
Vencimiento de contraseñas	Vencen cada seis meses
Intento inválido de inicio de sesión	Nunca bloquear cuentas

2. Integraciones

RR. HH.:

Cuando se añade, actualiza o elimina un usuario de nuestro portal de RR HH., esto también se refleja en el sistema 0Trust. Los detalles del empleado, tales como su nombre, apellido y número de móvil, se recopilan, y se usa el correo electrónico del empleado como el único identificador.

Análisis:

0Trust mantiene logs. Contiene detalles sobre cada usuario, los recursos a los que han accedido y la ubicación de acceso. Generalmente esto se monitorea para análisis de incidentes, por lo que planeamos integrar 0Trust con nuestra herramienta de análisis en el futuro.

3. Automatización y orquestación

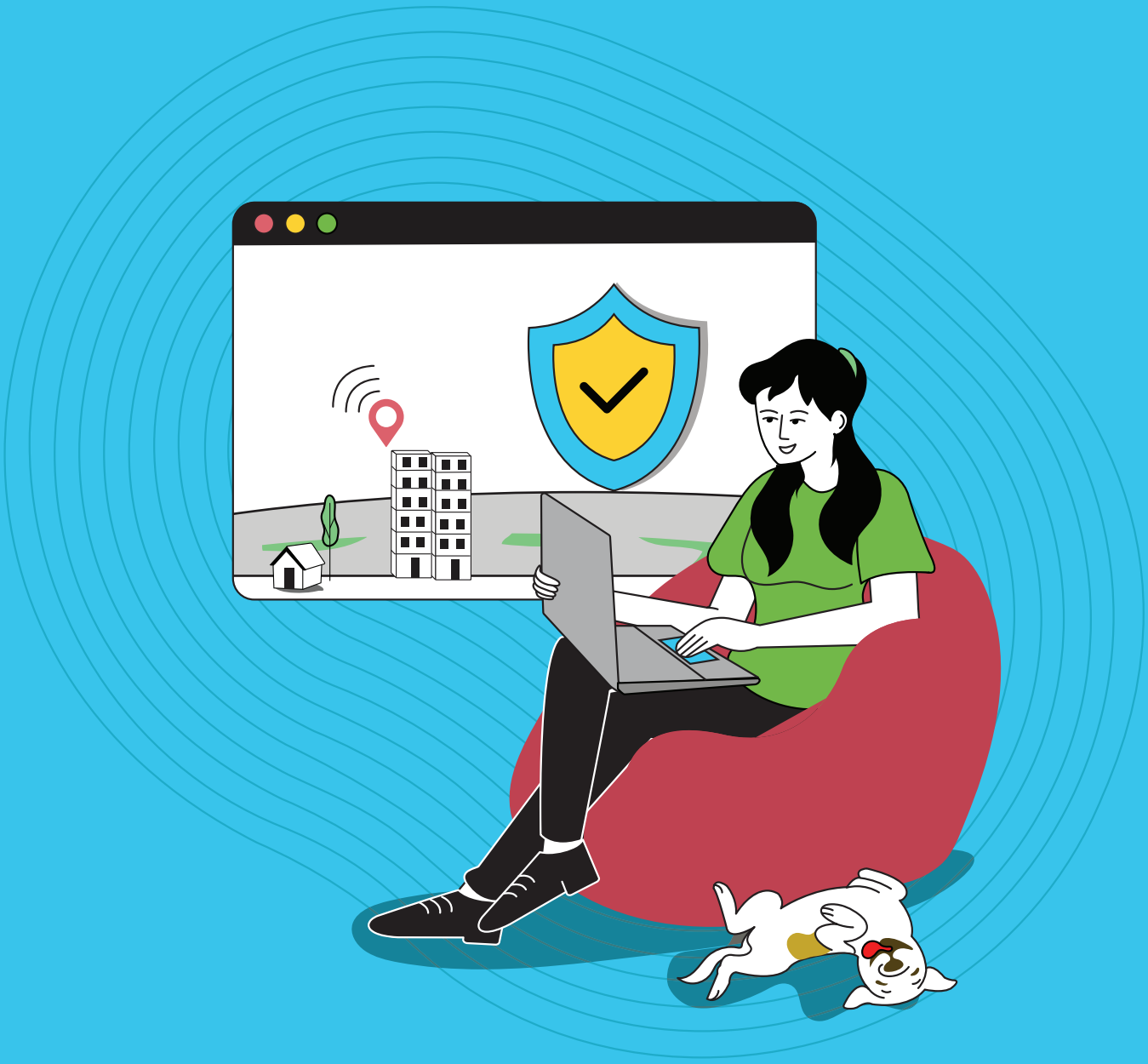
Componentes lógicos de la arquitectura de confianza cero

Fuente: NIST's guidance for a Zero Trust architecture (un e-book de ManageEngine)

Este diagrama representa la arquitectura de Zero Trust de NIST. Sin ir a los detalles técnicos, es importante observar el rol de un motor de políticas. Evalúa la puntuación de confianza para cada solicitud de acceso y la acepta o rechaza automáticamente. El objetivo de la automatización y orquestación es juntar los pilares de Zero Trust, permitiendo que los equipos de TI tomen decisiones confiables y rápidas. Aplicar la automatización y la orquestación al motor de políticas facilita el trabajo del equipo de TI al eliminar la necesidad de evaluar manualmente cada posible amenaza antes de tomar medidas.

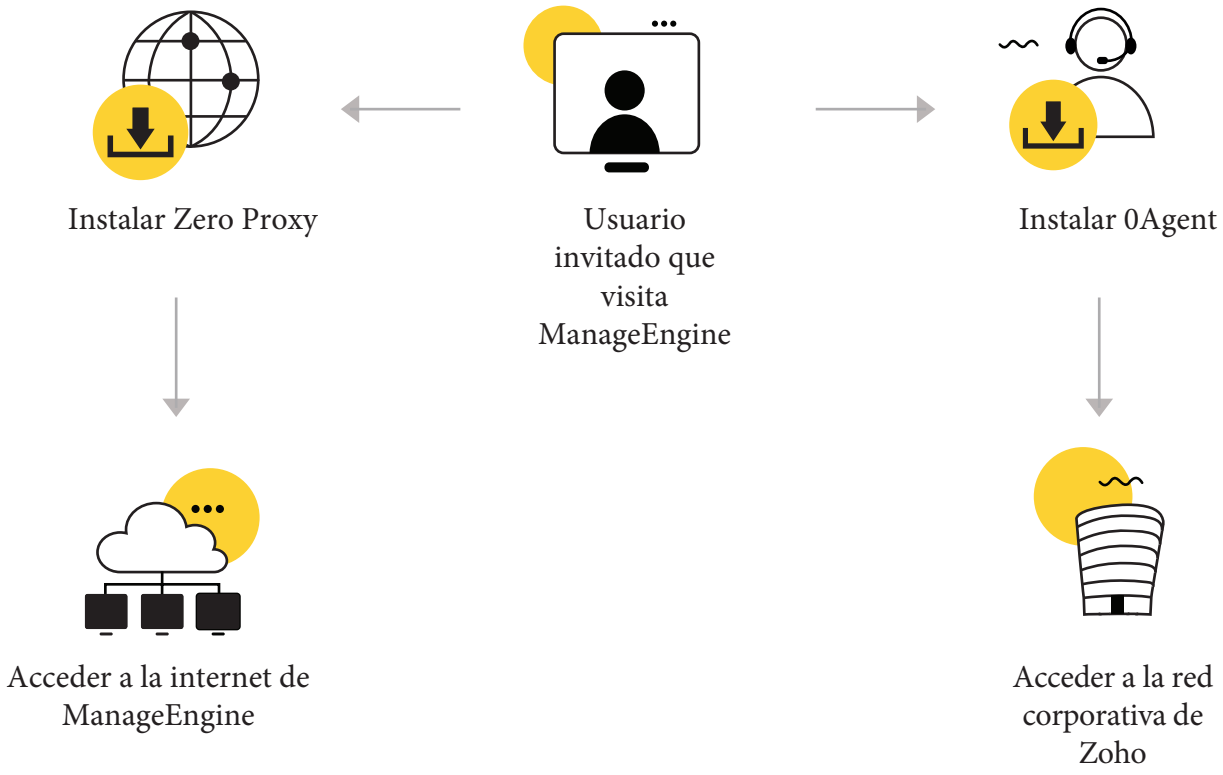
Capítulo 3

Proteja el acceso remoto con principios de Zero Trust



Caso de uso 1:
Usuarios invitados que visitan ManageEngine

En una situación en la que tuvimos visitantes on-premises que accedieron a nuestros recursos, ellos debieron instalar 0Agent. El administrador de sistemas puede hacer esto; el administrador también termina sesiones y bloquea usuarios y dispositivos que no cumplan con nuestras políticas. Sin embargo, si un invitado necesita acceder a la intranet de su propia organización, debe instalar el servidor de 0Proxy.



Caso de uso 2:

Restringir el acceso a aplicaciones empresariales de alto valor

Zorro es nuestro equipo de operaciones en el centro de datos. Maneja todos los procedimientos involucrados en mantener nuestros centros de datos, mejorando su rendimiento y mitigando posibles amenazas. Una de sus responsabilidades clave es realizar actividades de mantenimiento en servidores de aplicaciones, como actualizar las configuraciones y parcheo de firewalls.

Para que un analista de sistemas de Zorro acceda al servidor, estos son los pasos que usualmente debe seguir:

Paso 1: Conectarse a la VPN.
Paso 2: Iniciar sesión mediante nuestra herramienta para la gestión de acceso privilegiado.
Paso 3: Conectarse al servidor de aplicaciones.
Paso 4: Realizar las actualizaciones.

Desde que implementamos 0Trust, nuestro analista de sistemas ha encontrado más fácil acceder al servidor de aplicaciones. Se pueden conectar directamente a nuestra herramienta para la gestión de acceso privilegiado y realizar las actualizaciones.

Caso de uso 3:
Acceder a herramientas de desarrollo

Las herramientas de desarrollo tiene más requisitos que otras herramientas. Un líder de desarrollo tiene que revisar y evaluar distintas funciones compiladas por su equipo. Estas funciones se alojan en el servidor local distribuido, de forma que no puedan acceder a él solo mediante Wi-Fi.

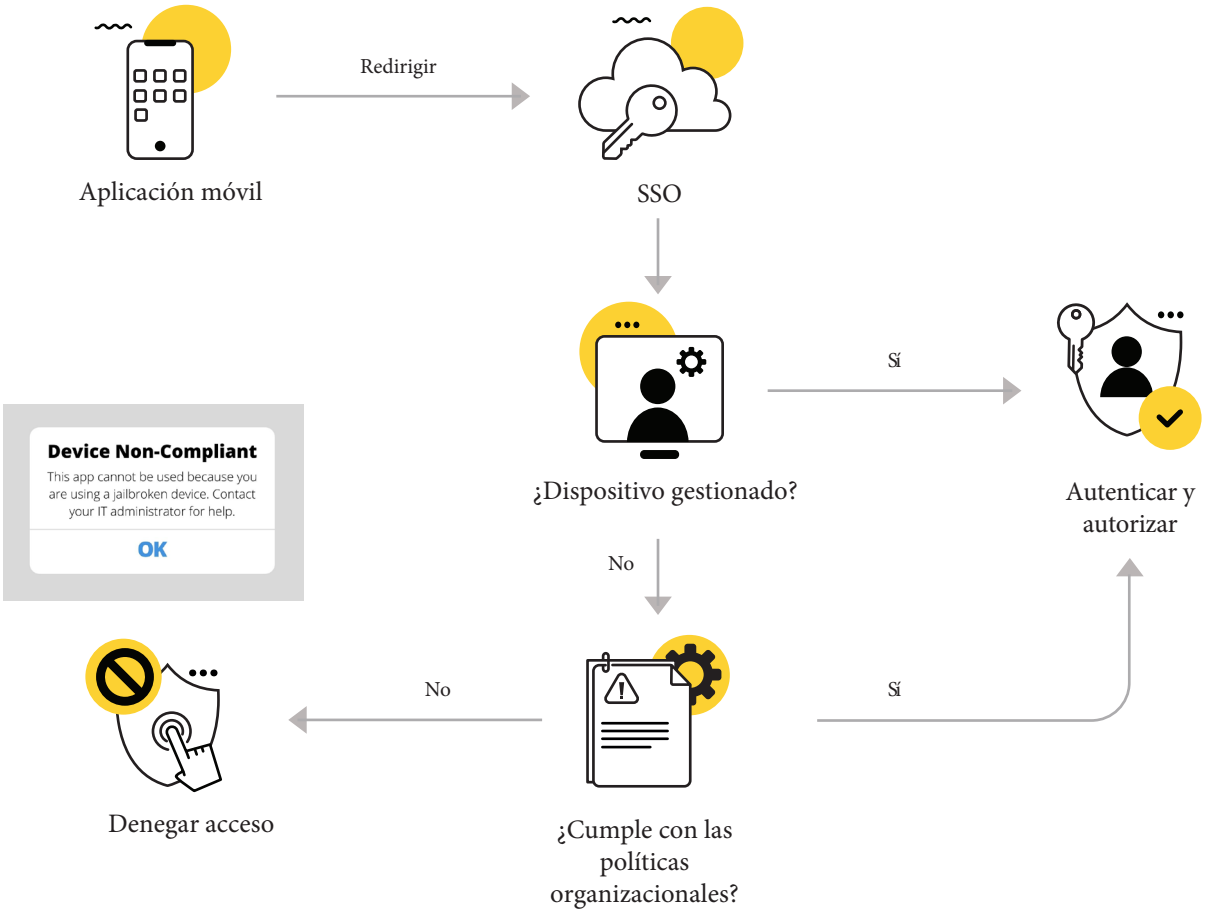
Ahora mismo, los líderes de equipo deben conectarse a la VPN para acceder a las compilaciones locales. Esto con frecuencia afecta la velocidad de conectividad debido a que todo el acceso se canaliza mediante la VPN. Algunas veces requiere varios inicios de sesión después de que la sesión de VPN quede inactiva. Luego de implementar Zero Trust, serán capaces de conectarse directamente a las herramientas sin necesidad de iniciar sesión en la VPN cada vez.

Caso de uso 4:
Acceso desde un dispositivo no conforme

Imagine que un miembro del personal administrativo intenta iniciar sesión para una aplicación corporativa desde su dispositivo móvil personal, que es está jailbroken. Al integrar un sistema de Zero Trust con una herramienta de IAM, usted puede verificar la identidad del usuario e identificar y detectar anomalías, si las hay. Una herramienta de gestión de endpoints verifica la identidad del dispositivo.

	Atributos		Información del usuario	Postura de riesgo	Acciones para mejorar la seguridad
Evaluar atributos de usuario dinámicos	Usuario	ID del usuario	Gestionado	Bajo	N/A
		Comportamiento	Sin anomalías		
		-Tiempo	Usual		
		-Ubicaciones	Usual		
		-Frecuencia	Usual		
	Dispositivo	Device ID	No gestionado	Alta	El dispositivo no es conforme, por lo que se le deniega el acceso
		Device Status	Alto riesgo		
	Red	Network ID	No gestionado	Medio	
		Status	Protegido		
Evaluar atributos de los recursos empresariales	Aplicación	App ID	Gestionado	Bajo	
		Status	Protegido		
		App Access	Autorizado (temp)		
	Datos	Data Type	Protegido	Medio	N/A
		Data Access	Autorizado		
			General	Alto	Denegar acceso

En este caso, el dispositivo no está gestionado y viola las políticas de la organización, por lo que se deniega el acceso.



Caso de uso 5: Dispositivos de empleados con malware

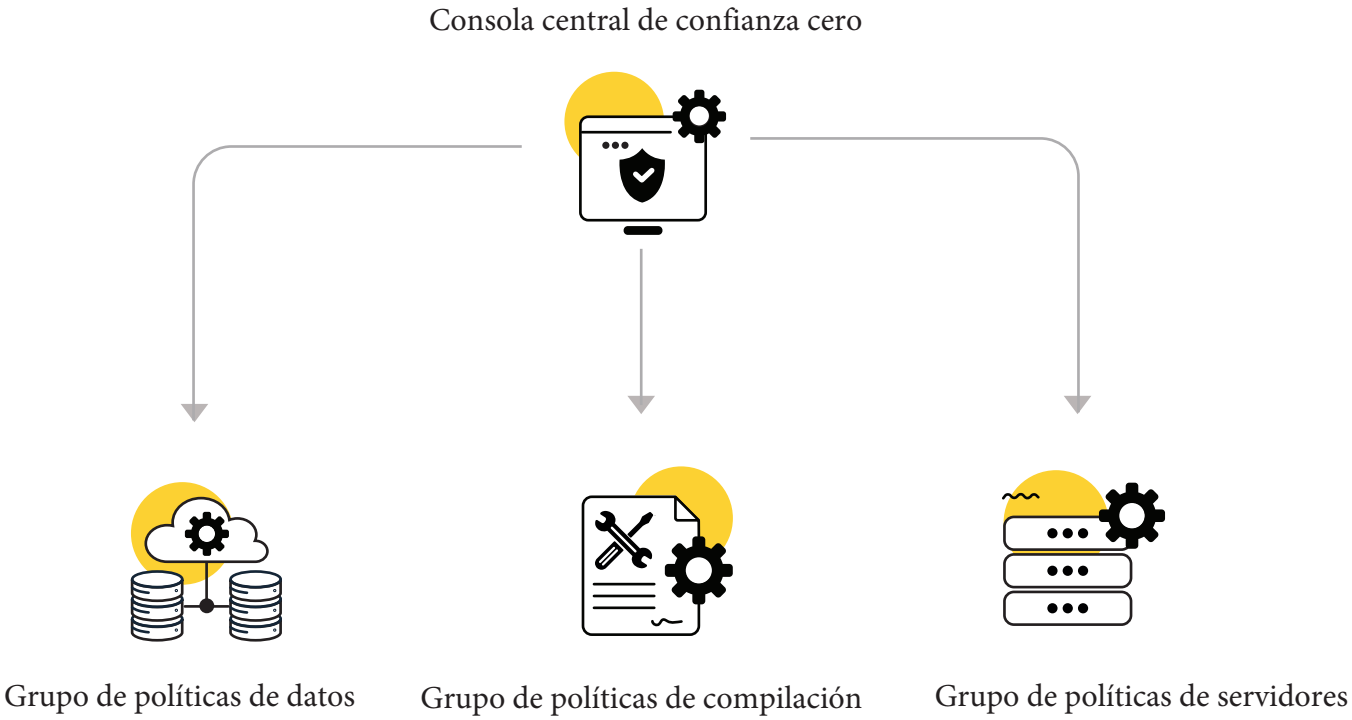
En el caso de que el sistema de un empleado esté infectado con un malware, el objetivo es aislar dicho sistema rápidamente y detener todas las sesiones activas del usuario. Usualmente, un ingeniero de seguridad de sistemas tendría que usar nuestra herramienta de MDM para iniciar medidas con el fin de cortar el acceso a los recursos, lo que toma tiempo.

Con 0Trust podemos evitar esa situación por completo. Un agente monitorea constantemente la postura de seguridad de cada dispositivo. Cuando la puntuación del dispositivo disminuye por debajo de la cifra requerida, se termina inmediatamente. Si hay otras sesiones abiertas, también se pueden terminar sin importar la puntuación de confianza. Esta acción la lleva a cabo un ingeniero de sistemas desde el dashboard de gestión de 0Trust.

Caso de uso 6:
Políticas personalizadas para distintos equipos

Los equipos de productos constan de miembros con distintos roles y requisitos. Algunos miembros necesitan acceder a servidores o bases de datos, mientras que otros necesitan acceder a compilaciones locales o de producción. Los recursos se alojan con frecuencia en distintas redes internas. Aquí, necesitamos aplicar uno de los pilares de Zero Trust: mínimos privilegios. Los empleados necesitan un acceso mínimo a recursos específicos con base en sus roles.

Sin 0Trust, los propietarios de productos tendrían que configurar individualmente los permisos de acceso. Esto podría funcionar para equipos pequeños, pero no para una empresa con cientos de miembros en un equipo de productos.



Con 0Trust los propietarios de productos pueden crear un grupo de políticas para cada equipo en la consola central de 0Trust y distribuir cada configuración. Mientras que esta función no está disponible en nuestro sistema ahora, está en nuestra hoja de ruta, y esperamos implementarla pronto.

Capítulo 4

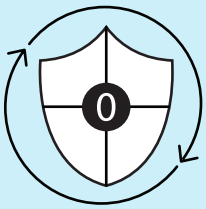
Retos y mejores prácticas

4.1 Retos y mejores prácticas

Reto #1

La confianza cero es un proceso continuo

Si solo pudiéramos arreglar nuestros problemas con apretar un botón. La confianza cero no termina con su implementación, especialmente para organizaciones en crecimiento. Los controles de acceso se deben actualizar para alinearse con los cambios en los roles. Por ejemplo, alguien que ha dejado la organización debe perder sus privilegios de inmediato. Si su cuenta sigue activa, está en riesgo de exponer información sensible. Este requisito continuo y complejo es la razón por la que algunas organizaciones abandonan a mitad de camino sus esfuerzos de confianza cero.



Mejor práctica:

Junte a un equipo dedicado

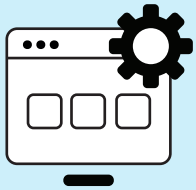
El mantenimiento perpetuo solo se puede realizar con la ayuda de un equipo. En Zoho, tenemos un pequeño equipo cuyo propósito es implementar la confianza cero y monitorear actividades relacionadas. Los dispositivos y wearables IoT se están volviendo populares en el lugar de trabajo, por lo que nuestras políticas para el control del acceso deben reflejar dichos cambios.

Reto #2

Encontrar un equilibrio entre la seguridad y la productividad

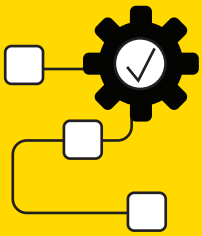
Aplicar políticas de seguridad estrictas podría verse como un impedimento a la productividad. Imagine tener que iniciar sesión cada vez que abre cualquier aplicación en su teléfono o verificar su identidad cada vez que hace una llamada. Esto podría ser seguro, pero es irracional.

Reto #3



Aplicaciones heredadas

Pasar a Zero Trust con aplicaciones heredadas es más complicado. Estas aplicaciones no están diseñadas en torno a los requisitos actuales de tecnología y seguridad. Los principios fundamentales de la confianza cero son los mínimos privilegios y el control de acceso, los cuales no se pueden llevar a cabo con sistemas antiguos. Algunas organizaciones van tan lejos como para ignorar los sistemas heredados y generar Zero Trust alrededor de aplicaciones modernas, dejando brechas de seguridad.



Mejor práctica:

Un paso a la vez

No salte a Zero Trust o haga cambios drásticos a la vez. Incursione lentamente con un sistema híbrido que tenga el equilibrio entre Zero Trust y los sistemas heredados. Evalúe primero su sistema existente. Luego, cree una hoja de ruta como hicimos nosotros, trazando sus prioridades y los pasos que necesita dar para lograr sus metas de seguridad.

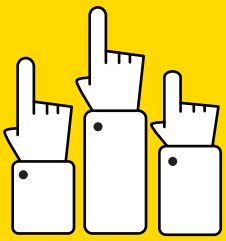
Reto #4

Zero Trust =/= 100% de seguridad

Zero Trust le ayuda a bloquear amenazas con base en dónde, cuándo y cómo un usuario accede a información confidencial. Incluso así, no tiene en cuenta ataques de ingeniería social. No hay una estrategia a prueba de fallos que evite el phishing, ataques internos, ransomware u otros ataques similares.

Mejor práctica:

Zero Trust = 100% de participación

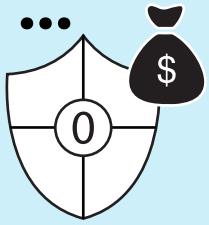


¡No puede haber eslabones débiles! Zero Trust una vez adoptada, debería ser obligatoria para todos en la organización, sin importar su rol o ubicación. En ManageEngine tenemos empleados en todo el mundo trabajando desde la oficina y desde casa. Usan un amplio rango de dispositivos, aplicaciones y servicios. Aunque es mucho trabajo, nuestro equipo de seguridad trabaja activamente con el equipo de confianza cero para implementarla en toda la organización tan pronto como sea posible.

Reto #5

Zero Trust es costosa

Alcanzar Zero Trust requiere hardware y software compatibles. No obstante, como mencionamos antes, es más barato invertir en lZero Trust que pagar por los daños. Considérela un seguro a largo plazo o un activo para el futuro. Agradecerá haberlo hecho.



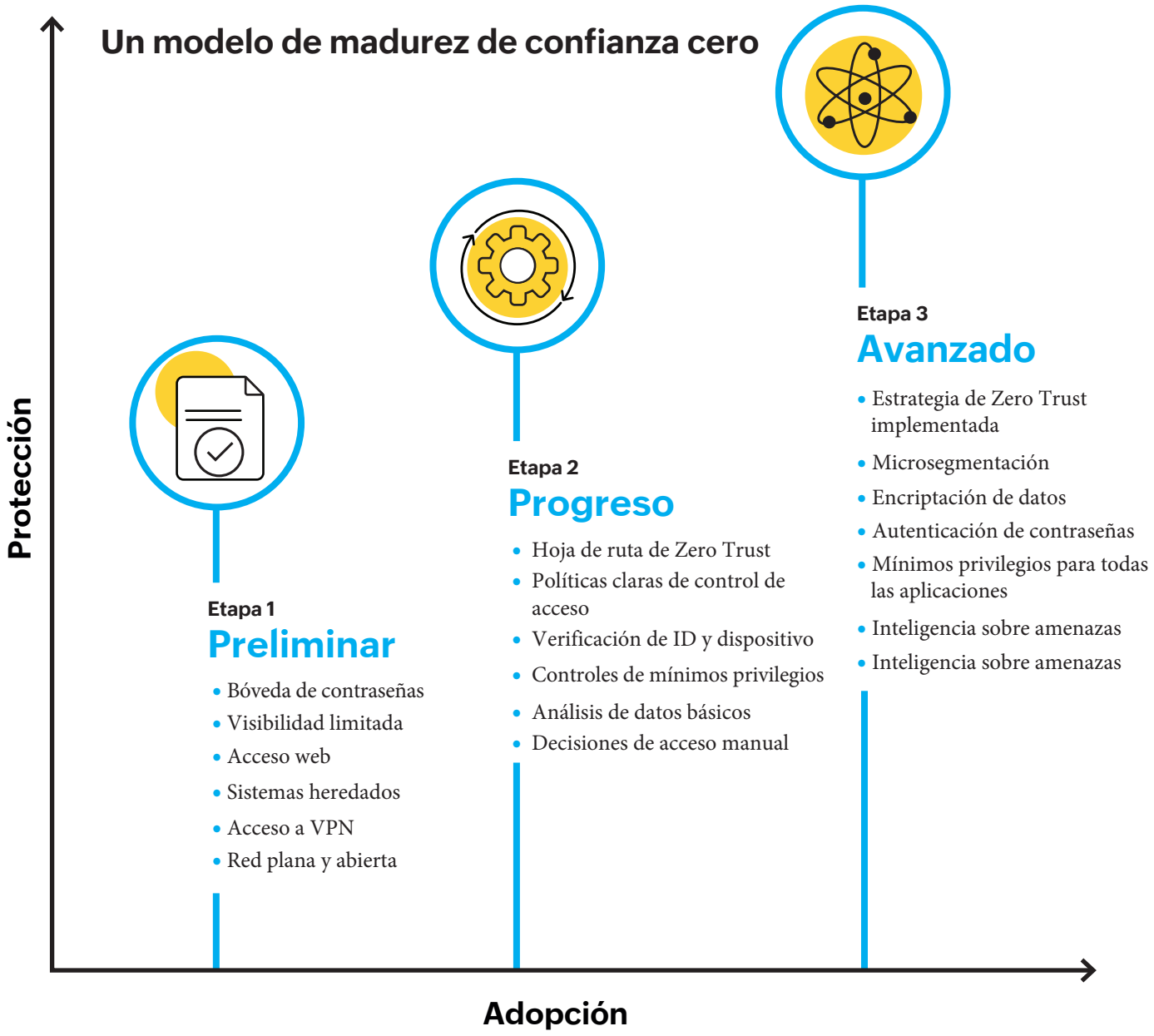
Mejor práctica:

Invierta en una herramienta para IAM segura

Las soluciones de IAM pueden ayudar a los usuarios a acceder a recursos al analizar la postura de cada solicitud y determinar el siguiente paso (es decir, otorgar acceso, denegarlo o solicitar una verificación adicional antes de acceder).

4.2 ¿Qué sigue?

Antes de empezar con su viaje de confianza cero, debe tener un modelo de madurez de confianza cero para su organización que trace dónde está y dónde debe estar en términos de la disposición para la confianza cero. Este modelo se ve influenciado por requisitos de seguridad, políticas y tecnología preexistente, y limitaciones.



Ahora mismo, ManageEngine está todavía en la etapa de progreso, trabajando para llegar a tener un sistema de Zero Trust óptimo. Planeamos desechar el servicio de VPN pronto. Además, estamos buscando proveer 0Trust como una solución para los clientes.

Otra función emocionante que ansiamos es el 5G. Ha sido un tema de discusión por años, y estamos anticipando su lanzamiento en nuestros sistemas pronto, así como un aumento subsecuente en los dispositivos IoT. ¿Qué significa esto para Zero Trust? ¿Cómo los servicios de 5G impactarán nuestras operaciones? Probablemente el 5G ofrezca un control mejor y más detallado sobre la identidad de las redes y dispositivos. Como empresa el 5G nos ofrece una vía para fortalecer nuestra seguridad como nunca, si implementamos la confianza cero de la manera correcta.

Conclusión

Zero Trust es un concepto en desarrollo y necesita tiempo para evolucionar a un sistema de seguridad completo. Aún estamos pensando en cómo afinar nuestro proceso y alcanzar el nivel de Google y Microsoft. Esperamos que en unos pocos años tengamos una segunda edición de este e-book con más información sobre cómo estamos llevando a ManageEngine al siguiente nivel de Zero Trust.

Sobre ManageEngine

Como la división de gestión de TI de Zoho Corporation, ManageEngine prioriza soluciones flexibles que funcionan para todas las compañías, sin importar el tamaño o el presupuesto. ManageEngine diseña software integral para la gestión de TI con un enfoque en facilitar su trabajo. Nuestros más de 120 productos y herramientas gratuitas con reconocimientos cubren todo lo que su TI necesita. Desde la gestión de redes y dispositivos a software de seguridad y de mesa de servicio, juntamos la TI para un método integrado y dominante para optimizar su TI.

Sobre la autora

Mahanya es una especialista de contenido aquí en ManageEngine. Ha sido parte de ManageEngine Academy desde 2020, compartiendo historias y recursos internos a líderes de TI. Cuando no está creando contenido, pasa el tiempo con perros rescatados.