Diseño de una base de seguridad con la confianza cero y la automatización

Formas de operar en un contexto de confianza cero

Índice

Introducción

La actividad de su empresa no termina a las 17 h, así como tampoco lo hace la actividad de los cibercriminales ni de los demás agentes malintencionados que buscan oportunidades para robar datos o causar daños que puedan poner en peligro a su empresa, sus partners y clientes.

Actualmente, las empresas enfrentan una enorme tormenta de amenazas de ciberseguridad que mantienen a los equipos de TI, seguridad y operaciones en alerta máxima. Estas amenazas afectan a empresas de todos los tamaños y pueden costar miles de millones. Según un informe de IBM, el costo promedio de una filtración de datos a causa de un ataque cibernético fue de USD 4,24 millones en 2021, frente a los USD 3,86 millones de 2020[1].

Estas amenazas no solo provienen de atacantes externos; en el informe 2021 Data Breach Investigations Report de Verizon, se descubrió que el 30 % de los casos de filtraciones correspondió a empleados que accedieron a sistemas que estaban fuera de la órbita de sus funciones y permisos establecidos[2].

El aumento de la cantidad y la gravedad de los ataques se debe a varios factores, entre los que se encuentran los rápidos cambios en la infraestructura de las redes, las migraciones de las soluciones en las instalaciones a la nube y el incremento de los modelos de trabajo remoto y de trabajo desde el hogar desde el año 2020.

El cambio que implica el entorno de trabajo remoto de los empleados amplió la superficie expuesta a ataques, ya que se accede a los sistemas confidenciales de la empresa a través de dispositivos propios y del personal mediante conexiones de Internet personales y públicas. También hubo un aumento en la cantidad y la sofisticación de los ataques de suplantación de identidad generales y específicos, ya que los empleados trabajan con colegas que no conocen.

El traslado a las soluciones basadas en la nube presenta muchos beneficios para las empresas, desde el ahorro en los costos hasta una reducción importante en el almacenamiento físico de documentos. Sin embargo, estos beneficios conllevan un costo general de la gestión de la seguridad de los usuarios, las aplicaciones y la infraestructura para una gran cantidad de usuarios de los sistemas heredados en las instalaciones y en la nube.

La combinación del trabajo remoto y el traslado a la nube dejó obsoleto el enfoque tradicional cerrado de seguridad de VPN. Tanto el acceso de los empleados a más sistemas desde más dispositivos como la incorporación del IoT y el edge computing presentaron nuevos vectores de ataque potenciales a los atacantes cibernéticos.

Además de las formas en las que los empleados acceden a los sistemas, las empresas también adaptaron la actividad de los equipos para que gestionen diversos sistemas de redes y seguridad. Los equipos de InfoSec, SysOps y NetOps, entre otros, suelen trabajar de forma simultánea, pero también lo hacen independientemente entre sí, para aplicar las políticas de seguridad y responder a las

1 "Cost of a Data Breach Report 2021", IBM, consultado el 16 de junio de 2022.
2 "2022 Data Breach Investigations Report", Verizon, consultado el 16 de junio de 2022.

Si desea obtener más información sobre la confianza cero, continúe leyendo.

Si ya conoce la confianza cero pero desea obtener más información sobre su automatización, pase directamente a Ajuste de la confianza cero con la automatización.

amenazas. De todas maneras, muchas veces estos equipos trabajan por separado y utilizan sistemas distintos sin compartir procesos que afecten su capacidad de coordinar una respuesta. Cuando se trata de amenazas de seguridad, cada segundo cuenta en la velocidad de respuesta.

Otro desafío que implica riesgos de ciberataques es la falta de integración entre las soluciones que permiten el funcionamiento de la infraestructura de la empresa y la protegen. Este aspecto genera obstáculos adicionales para la respuesta eficaz a los incidentes de seguridad cuando los equipos que gestionan estas soluciones no pueden comunicarse de manera eficiente.

Estos riesgos de ciberataques no solo llaman la atención de los encargados de la seguridad. Las empresas y los proveedores se han adaptado para respaldar las regulaciones, como la Ley de Privacidad del Consumidor de California (CCPA) y el Reglamento General de Protección de Datos (RGPD) de la Unión Europea. En 2021, el Gobierno de Estados Unidos reconoció este aumento de amenazas y presentó el decreto para mejorar la ciberseguridad de la nación.

Para abordar estas amenazas, las empresas deben adoptar un enfoque que priorice la seguridad en todas sus políticas, redes y aplicaciones. Muchas empresas recurren a la arquitectura de confianza cero como una manera de proceder, incluso el Gobierno federal de Estados Unidos con su iniciativa de avanzar hacia la aplicación de esta arquitectura en todas sus redes.

Pero la implementación de la confianza cero solo representa el principio, en especial en las grandes empresas con varios sitios y una combinación de sistemas en las instalaciones, la nube y el extremo de la red. La adopción de esta arquitectura requiere implementar la automatización en toda la empresa. En este ebook, conocerá las razones por las que Red Hat® Ansible® Automation Platform es la solución adecuada para su empresa.

¿La confianza cero al rescate?

Los modelos de seguridad tradicionales se diseñaron a partir de sistemas a los cuales los empleados accedían desde el interior de una ubicación física. A medida que las opciones de acceso remoto evolucionaban de la conexión por línea conmutada a la de alta velocidad permanente, se regulaba el acceso externo con las redes privadas virtuales (VPN). Si bien las VPN brindan autenticación segura a la red, también exponen más recursos y sistemas a los usuarios que aquellos a los que se necesitaría acceder, lo cual genera riesgos de seguridad potenciales.

En la actualidad, las VPN y los permisos estándares basados en usuarios ya no pueden brindar el nivel de seguridad que se necesita para la complicada arquitectura de soluciones en las instalaciones, de nube e híbridas de la cual depende la empresa para llevar a cabo sus negocios. Se necesitaba un nuevo modelo, uno que realizara un cambio básico con respecto al enfoque de la seguridad. Este cambio se logró con la arquitectura de confianza cero.

La confianza cero, que fue reconocida como patrón de seguridad en 2010, comienza al asumir que existen atacantes dentro y fuera de la red. Este enfoque implica la premisa de que ninguna interacción es confiable desde el principio.

El marco de confianza cero no depende únicamente de la ubicación y la función o de los permisos basados en los usuarios, sino que requiere que el usuario, el dispositivo y la aplicación estén verificados para que se genere un estado de confianza de la interacción. Gracias a su implementación, se presenta un enfoque de seguridad completamente nuevo en el que se indica a los arquitectos del sistema que soliciten autenticación a los usuarios o los dispositivos en cada una de las transacciones, y que solo autoricen su acceso a los datos y los sistemas en función del concepto de privilegios mínimos.

Autenticación de todas las transacciones

La base de la arquitectura de confianza cero es tratar a todas las interacciones como una amenaza potencial, tanto dentro como fuera de la red. Para que pueda continuar la interacción, es necesario autenticar sus elementos. Cada implementación de la arquitectura de confianza cero tendrá sus propios elementos necesarios particulares, pero también tendrá un conjunto básico:

- **Usuario:** se autentica que el usuario que intenta acceder a una red, una aplicación o un sistema basado en la nube cuenta con los permisos correctos.
- **Aplicación:** se comprueba que el usuario tiene los permisos correctos para los datos o la aplicación a los que intenta acceder.
- **Dispositivo:** se confirma que el usuario se conecta al recurso con un dispositivo autorizado para acceder a la red y la aplicación.
- **Estrategia:** se revisa el dispositivo utilizado para confirmar que cuenta con las actualizaciones, los parches y el cifrado necesarios para acceder a la red y la aplicación de manera segura.

El cambio a la confianza cero también se da en el sector público, especialmente en el Gobierno federal de Estados Unidos. El decreto para mejorar la ciberseguridad de Estados Unidos de 2021 incluye varias exigencias desde la migración a las soluciones de nube seguras hasta el avance hacia la arquitectura de confianza cero para toda la infraestructura gubernamental.

Las empresas que venden productos o prestan servicios a los organismos federales deberán asegurarse de cumplir los estándares de la confianza cero a medida que esos organismos mejoren su seguridad e infraestructura.

Desafíos de la implementación de la confianza cero

Con el aumento de los vectores de amenazas y ataques, resulta imprescindible implementar la arquitectura de confianza cero en toda su empresa. Sin embargo, a pesar de las diversas ventajas que presenta la confianza cero en comparación con la seguridad tradicional, se presentan algunos desafíos al implementarla en una infraestructura que ya está en funcionamiento.

En primer lugar, la infraestructura actual puede estar conformada por varias soluciones de diferentes proveedores. Si bien la mayoría de ellos ha avanzado en la adopción de los principios de la arquitectura de confianza cero, no todos los sistemas ofrecen interoperabilidad con los sistemas de otros proveedores. Los equipos internos, como los de SysOps y NetOps, pueden sufrir problemas cuando las soluciones no funcionan en sintonía con las demás. O peor aún, los equipos y los sistemas desconectados pueden provocar interrupciones en la detección de amenazas cuando se producen problemas de interoperabilidad.

En segundo lugar, la confianza cero requiere de un cambio importante en el modo en el que los encargados de la seguridad piensan en ella y la aplican. Para pasar de un enfoque de castillo y foso a uno de denegación de forma predeterminada, deben comprometerse a que su empresa sostenga los principios y las prácticas de la confianza cero, incluso cuando parezca que estos se interponen en el camino. Sin este compromiso, muchas veces los equipos vuelven a aplicar las prácticas heredadas o desarrollar distintas soluciones de software no aprobado por la empresa que evaden los principios de la arquitectura, las políticas y los procesos de la confianza cero.

Diseño de una base de seguridad sólida con la arquitectura de confianza cero

Los enfoques de seguridad tradicionales, como las VPN con tokens físicos o digitales, se crearon para brindar una ruta remota segura a la red local. Suelen ser identificados como modelo de seguridad de red de castillo y foso y se centran únicamente en un punto de entrada que abre su puerta a todos los recursos que se encuentran del otro lado.

En la seguridad física, esta analogía se aplicaría con el uso de tarjetas de acceso para ingresar a edificios o sus áreas protegidas. Una empresa puede considerar que cuenta con seguridad física si usa un enfoque basado en funciones para que los empleados ingresen al edificio o se desplacen por distintas áreas. Pero esta seguridad puede fallar si un agente malintencionado aplica un truco de ingeniería social, como pretender ser un repartidor para que el personal de seguridad del edificio lo deje pasar.

La confianza cero es el núcleo, no un complemento

Los principios de la confianza cero comienzan por incluir la seguridad como elemento básico de todos los proyectos, ya sea que tengan como objetivo desarrollar nuevos productos o implementar una infraestructura nueva. En lugar de diseñar la estrategia de seguridad en torno al acceso a la red, la arquitectura de confianza cero se aplica a todas las interacciones como práctica en la empresa.

Primeros pasos con la confianza cero

La implementación de esta arquitectura no comienza con la selección de proveedores ni con la migración de las plataformas de seguridad. Lo que deben hacer las empresas es plantearse una pregunta sencilla pero con importantes consecuencias en las estrategias de confianza cero: ¿qué datos, aplicaciones o sistemas se intentan proteger?

- **Cree un inventario:** tener claro lo que se quiere proteger otorga a las empresas un punto de referencia para la creación de las reglas y las políticas respecto de la red, los usuarios, las aplicaciones y las cargas de trabajo para la implementación de la confianza cero. Este punto de referencia también permite que los equipos de SysOps, NetOps e InfoSec conozcan los análisis y las herramientas que se necesitan para detectar e identificar los incidentes de seguridad y responder a ellos.
- **Desarrolle sus procesos y políticas:** una vez que la empresa tiene una idea clara de lo que debe proteger, los equipos internos pueden trabajar juntos para crear los procesos y las políticas de la confianza cero que permitan a los empleados llevar a cabo su trabajo de forma segura.
- **Efectúe pruebas, modificaciones e implementaciones:** a veces las ideas que se anotan en papel pueden resultan de manera diferente cuando se implementan. Al ver los procesos y las políticas en un entorno real, los equipos de operaciones, redes y seguridad obtienen la información necesaria para que la implementación de la confianza cero funcione correctamente en toda la empresa.

La base para ajustar la confianza cero a través de la automatización es comenzar por comprender qué es lo que se quiere proteger.

Ajuste de la confianza cero con la automatización

Obtenga más información sobre la automatización de la seguridad que ofrece Ansible y descubra en qué etapa de este proceso se encuentra gracias a este webinar.

La arquitectura de confianza cero exige que los recursos, como los dispositivos, los datos y las aplicaciones, se protejan de la misma manera dondequiera que estén ubicados. Por ejemplo, si una carga de trabajo se traslada de un centro de datos en las instalaciones a una nube privada o pública, la arquitectura de confianza cero requerirá que se apliquen las mismas reglas sobre la gestión de la seguridad. Con esta arquitectura, las decisiones se abstraen de la carga de trabajo, de manera que no cambie el código.

En las grandes empresas o aquellas de rápido crecimiento, la automatización puede resultar útil para ajustar las políticas, las reglas y los procesos a medida que se incorporan nuevas herramientas o infraestructura. Antes de analizar la automatización de la arquitectura de confianza cero que ofrece Red Hat® Ansible® Automation Platform, presentamos cinco beneficios de este proceso:

Beneficios de la automatización

- **Conocimiento de lo que se debe proteger:** saber qué recursos se van a proteger es la clave para aplicar la confianza cero en los dispositivos, las redes y las aplicaciones de una empresa. La automatización le permite realizar un seguimiento y llevar un registro de estos recursos en diversas ubicaciones y en la nube.
- **Cumplimiento normativo permanente:** el uso de bots y otras herramientas de automatización por parte de los cibercriminales crea la necesidad de contar con un sistema de seguridad que esté atento a las amenazas en todo momento. La automatización de la confianza cero garantiza que las políticas se apliquen las 24 horas de los 365 días del año.
- **Reducción de los riesgos:** los equipos de InfoSec pueden adoptar políticas y reglas cuando se producen incidentes de seguridad. Luego estos procesos se pueden codificar como flujos de trabajo y ejecutar mediante la automatización, lo que reduce el riesgo de que un administrador cometa un error humano al implementar un cambio.
- **Mejora de la capacidad de respuesta:** mientras más se demore en responder a un riesgo de seguridad, más posibilidades habrá de que se produzca un fallo de seguridad o un ciberataque. La automatización de la confianza cero permite que las empresas respondan a los incidentes con rapidez, ya sea que tengan 1000 o 100 000 usuarios, al crear acciones automatizadas que se pueden ejecutar según se requiera o según la automatización basada en eventos.
- **Creación rápida de prototipos:** la automatización permite que las empresas creen prototipos, los prueben e implementen cambios en el marco de seguridad, independientemente de lo complejo que sea.

La automatización de la confianza cero implica más que la seguridad

Si las empresas no se limitan a aplicar la confianza cero solo en el ámbito de las redes y la seguridad, verdaderamente podrán establecer la seguridad como la base de todos los proyectos y los sistemas. La automatización de estos procesos realza los beneficios de la confianza cero al garantizar que las políticas y los procesos se apliquen y revisen para reducir el riesgo de que se produzcan ciberataques u otros fallos.

Cumplimiento normativo y seguridad uniformes

La automatización ayuda a aplicar las reglas de seguridad y cumplimiento normativo al gestionar las configuraciones, la implementación de las aplicaciones y las comprobaciones de cumplimiento normativo que se incorporan a los procesos de desarrollo. Las empresas pueden automatizar la preparación, la configuración, la implementación de aplicaciones y otras áreas.

La automatización no se limita solo a proteger las aplicaciones y sus elementos, sino también se puede utilizar para mantener esos elementos y realizar comprobaciones de cumplimiento normativo y verificaciones periódicas. Se trata de la aplicación integral y permanente de la estrategia de seguridad del ciclo de vida de integración y distribución continuas (CI/CD) de las empresas.

Seguridad integral del software

Los principios de la confianza cero también se pueden aplicar al software y a los sistemas dentro de una empresa. Los equipos y los departamentos suelen necesitar diferentes aplicaciones, hardware y soluciones que no incluyen interoperabilidad desde un primer momento. La automatización ayuda a integrar varios sistemas de distintos proveedores gracias a la creación de flujos de automatización para organizar una interoperabilidad eficiente y segura.

Un aspecto aún más importante es que las soluciones que se desarrollan tanto interna como externamente pueden incluir elementos open source que podrían crear un nuevo vector de ataque para los cibercriminales si no se supervisan para detectar cualquier punto vulnerable. Las mismas automatizaciones creadas para gestionar la interoperabilidad se pueden utilizar para mantener el estado de seguridad correcto de las aplicaciones.

Automatización del cumplimiento

La automatización se puede usar para reducir los errores humanos en las tareas relacionadas con el cumplimiento normativo. Por ejemplo, en una empresa que procesa transacciones de tarjetas de crédito, se deben llevar a cabo varios procesos y revisiones de los sistemas de software y hardware para auditar el cumplimiento del Estándar de Seguridad de Datos (DSS) para la Industria de Tarjetas de Pago (PCI). En estas auditorías también se requiere obtener datos oportunos y precisos de todos los sistemas. La automatización puede supervisar estos procesos, en lugar de que un empleado o un equipo tengan que hacerlo. De esta manera, se reducen los errores humanos y el personal puede dedicarse a llevar a cabo proyectos más estratégicos.

Automatización de la confianza cero y más con Red Hat Ansible Automation Platform

Obtenga más información sobre las formas en que la automatización puede ayudarlo en Red Hat Ansible Automation Platform: guía para principiantes.

La confianza cero funciona cuando las empresas pueden supervisar cualquier transacción que se produzca. Red Hat Ansible Automation Platform incorpora la confianza cero y otras funciones de automatización a su empresa. La plataforma brinda un rápido retorno sobre la inversión (ROI) disminuyendo los obstáculos que se interponen a la automatización en las áreas de seguridad, redes, aplicaciones, nube y edge computing.

Confianza cero	**Automatización de la confianza cero con Red Hat Ansible Automation Platform**
La confianza cero usa un enfoque de denegación de forma predeterminada.	Red Hat Ansible Automation Platform permite que los administradores apliquen controles de acceso para asignar permisos, privilegios y funciones a los usuarios. También automatiza el cifrado, lo cual incluye la función de seguridad de la capa de transporte de autenticación mutua (mTLS), el seguimiento de auditorías y los controles de inventario.
La confianza cero utiliza las políticas de autorización para restringir el acceso a las aplicaciones o los recursos.	Red Hat Insights for Ansible Automation Platform ayuda a las empresas a supervisar los sistemas e identificar las fallas y los riesgos potenciales en los que podrían tener que intervenir los equipos de SysOps o NetOps.
La confianza cero garantiza que se apliquen los parches correspondientes a los recursos antes de que se acceda a ellos.	Red Hat Ansible Automation Platform garantiza que se apliquen los parches de seguridad y las actualizaciones a los recursos de las aplicaciones en toda la infraestructura de la empresa.

Red Hat Ansible Automation Platform conecta las tecnologías dispares que, de otro modo, no se comunicarían entre sí de manera adecuada. Existen más de 100 conjuntos Red Hat Certified Content Collections que cuentan con el soporte de Red Hat y sus partners y están disponibles para implementar la automatización de manera uniforme en todos los elementos de la infraestructura, ya sea que se encuentren en las instalaciones, en la nube o en entornos híbridos.

¿Está listo para comenzar con el proceso de automatización de la confianza cero?

Red Hat Consulting puede ayudarlo en el proceso de automatización para la adopción de la confianza cero. Realice una autoevaluación breve o póngase en contacto con el equipo de Red Hat Consulting ahora mismo.

Obtenga más información sobre la automatización de la TI y comience una prueba hoy mismo.

Acerca de Red Hat

Red Hat es el proveedor líder mundial de soluciones de software open source para empresas, que ha adoptado un enfoque impulsado por la comunidad para ofrecer tecnologías confiables y de alto rendimiento de Linux, nube híbrida, contenedores y Kubernetes. Red Hat ayuda a que los clientes desarrollen aplicaciones en la nube, integren las aplicaciones de TI nuevas y actuales, y automaticen y gestionen los entornos complejos. Es un asesor de confianza de las empresas de la lista Fortune 500 y brinda servicios galardonados de soporte, capacitación y consultoría para que obtenga los beneficios de la innovación abierta en todos los sectores. Es un centro de conexión en una red internacional de empresas, partners y comunidades, a los que ayuda a crecer, transformarse y prepararse para el futuro digital.

Argentina
+54 11 4329 7300

Chile
+562 2597 7000

Colombia
+571 508 8631
+52 55 8851 6400

México
+52 55 8851 6400

España
+34 914 148 800

facebook.com/redhatinc
@RedHatLA
@RedHatIberia
linkedin.com/company/red-hat

es.redhat.com
F32053