Informe técnico sobre la seguridad Verify Zero Trust

Contenido

Introducción

Este documento describe la información relacionada con Zero Trust y cómo se puede utilizar para proteger la empresa.

Resumen ejecutivo

Zero Trust representa un modelo que supone que ningún usuario, dispositivo o aplicación, ya sea fuera o dentro de la red, puede considerarse seguro, y que cada uno debe validarse antes de que se le permita acceder a los recursos de la red.

Este concepto ha adquirido más importancia en la virtualización y en el rápido movimiento de los recursos in situ a las nubes públicas, privadas e híbridas.

El término Zero Trust fue creado por Forrester en 2010 con la publicación de su informe Zero Trust Network Architecture Report.

Es importante comprender que Zero Trust debe comenzar como una estrategia a nivel empresarial para proteger intereses e iniciativas empresariales vitales.

Pilares de confianza cero

¿Qué es Zero Trust?

Zero Trust es un enfoque estratégico que abarca diversas tecnologías para ayudar a conseguir una seguridad más práctica para la infraestructura actual. Se trata de una arquitectura de seguridad y una metodología empresarial diseñadas para organizar de forma eficaz la combinación actual de tecnologías, prácticas y políticas.

Representa una evolución de nuestro enfoque de seguridad y ofrece una solución integral, interoperable y holística que incorpora productos y servicios de varios proveedores.

Zero Trust se basa en muchas tecnologías establecidas, como la segmentación de la red, la autenticación multifactor y el control de acceso a la red.

¿Por qué es importante la confianza cero?

La confianza cero ayuda a proteger la empresa frente a usuarios no autorizados, brechas de seguridad y ciberataques. Puede comprobar continuamente la identidad de los usuarios y dispositivos y concederles únicamente los permisos que necesitan para realizar su trabajo con el fin de minimizar el riesgo de un evento de seguridad.

Los estudios de mercado han demostrado que se espera que el tamaño del mercado mundial de seguridad de confianza cero crezca de un valor estimado de 27 000 millones USD en 2022 a alrededor de 60 000 millones USD en 2027/2028, con una tasa de crecimiento anual compuesta de alrededor del 17% en ese momento.

Motivos:

- Mayor frecuencia de ciberataques basados en objetivos.
- Crecimiento de la normativa sobre protección de datos y seguridad de la información.
- Mayor necesidad de reducir los riesgos empresariales y organizativos.
- A medida que se migran más servicios a la nube, la implementación de datos centralizada supera los límites de los datos y aumenta los riesgos de seguridad.
- La necesidad de confirmar la identidad del usuario a lo largo de todo el proceso de acceso y no solo inicialmente.

Un único ataque de ransomware cuesta 5 millones de dólares. Los ciberdelincuentes no discriminan cuando se dirigen a las empresas.

Recientes encuestas de CIO y CISO muestran que la confianza cero es una de las 5 prioridades principales. Los CISO afirman que el cambio al trabajo remoto, la escasez de mano de obra y el gran aumento de los ataques de ciberseguridad exigen que sus sistemas existentes en la empresa estén protegidos.

Modelo tradicional frente a modelo de confianza cero

Los entornos tradicionales son los que se han añadido funciones de seguridad después de crear el entorno. Normalmente, se trata de redes planas en las que las defensas se construyen alrededor del perímetro de la red para evitar ataques desde Internet.

Generalmente, se reconoce que Zero Trust se centra en la necesidad de proteger los sistemas y los datos de una organización en varios niveles con una combinación de cifrado, protocolos informáticos seguros, carga de trabajo dinámica y autenticación y autorización a nivel de datos, y no depende únicamente de un límite de red externo.

La arquitectura de seguridad tradicional centrada en el perímetro es menos eficaz, ya que las cargas de trabajo se distribuyen cada vez más desde la nube, y los terminales móviles se convierten en la norma para el acceso a las aplicaciones y los datos.

Marco arquitectónico de confianza cero

Un marco arquitectónico de confianza cero aborda la restricción del acceso a los sistemas, aplicaciones y recursos de datos a aquellos usuarios y dispositivos que necesitan específicamente acceso y que han sido validados. Deben autenticarse continuamente para comprobar su identidad y condición en materia de seguridad a fin de garantizar la autorización adecuada para que cada recurso proporcione acceso.

El marco es proporcionar una hoja de ruta para migrar e implementar conceptos de seguridad de confianza cero en un entorno empresarial y se basa en la publicación especial NIST 800-207.

Un marco arquitectónico de confianza cero efectivo coordina e integra estos siete componentes principales.

- Las redes de confianza cero son una característica importante de una estrategia de confianza cero que se refiere a la capacidad de segmentar redes o aislar recursos de red y mantener el control de las comunicaciones entre ellos. Además, protege las conexiones de confianza para ampliar el espacio de trabajo para su uso remoto.
- Zero Trust Workforce incluye métodos para limitar y aplicar el acceso de los usuarios, que incluye tecnologías para autenticar a los usuarios y supervisar y controlar continuamente sus privilegios de acceso. Este acceso está protegido por tecnologías como DNS, autenticación multifactor y cifrado de red.
- Zero Trust Devices responde a la necesidad de aislar, proteger y gestionar todos los dispositivos conectados a la red, que han aumentado con la incorporación de la movilidad e Internet of Things, para crear una inmensa vulnerabilidad que los atacantes pueden aprovechar.
- Las cargas de trabajo de confianza cero protegen las pilas de aplicaciones de la parte frontal a la parte trasera que ejecutan procesos empresariales críticos. Se centra en proteger el tráfico horizontal entre aplicaciones, datos y servicios en un Data Center para proteger mejor las aplicaciones críticas.
- Datos de confianza cero hace referencia a metodologías para clasificar y categorizar datos, combinadas con soluciones tecnológicas para proteger y administrar datos, que incluyen el cifrado de datos.
- La visibilidad y los análisis hacen referencia a tecnologías que proporcionan el reconocimiento necesario para la automatización y la orquestación, y permiten a los administradores no solo ver, sino también comprender la actividad en sus entornos, lo que incluye la presencia de amenazas en tiempo real.
- La automatización y la orquestación abarcan herramientas y tecnologías como algoritmos de aprendizaje automatizado e inteligencia artificial para clasificar automáticamente los recursos de la red y del Data Center, así como para sugerir y aplicar medidas, políticas y reglas de segmentación y seguridad que se aplicarán automáticamente; por lo tanto, se reduce la carga de trabajo de los equipos de seguridad y se acelera la mitigación de ataques.

Confianza y segmentación nulas

Todos los recursos basados en la red deben protegerse y segmentarse con el principio de mínimo privilegio. Esto se consigue mejor mediante un sistema de gestión de activos que controla las credenciales y el acceso para todos los fines.

La necesidad de segmentación Zero Trust incluye protección de marca, superficie de ataque limitada, estabilidad de red mejorada y la habilitación de una rápida implementación de servicios.

Para ayudar a lograr una mayor protección de los recursos individuales, se puede utilizar la microsegmentación. Las etiquetas de grupo escalables (SGT) se pueden utilizar cuando se inserta un valor de etiqueta en la trama Ethernet para identificar de forma exclusiva un recurso. Además, los dispositivos de infraestructura incluyen switches, routers o firewalls de última generación inteligentes que se pueden utilizar como dispositivos de gateway para proteger cada recurso.

Visibilidad, análisis y automatización

Es importante tener una visibilidad completa de todos los activos de la organización y de todas las actividades asociadas a dichos activos. Esta es la base de Zero Trust.

Para proporcionar políticas dinámicas y decisiones de confianza, debe haber una recopilación continua de análisis. Nuestro enfoque arquitectónico de confianza cero se centra en los componentes lógicos centrales de una estrategia de SDN con un motor de políticas y un administrador de políticas para formar un plano de control que restrinja el acceso a los recursos a través de los puntos de aplicación de políticas en un plano de datos.

Las capacidades necesarias para que la arquitectura Zero Trust proporcione un mayor contexto de red, aprendizaje y garantía para cumplir su misión de forma segura:

- Microsegmentación granular del acceso a usuarios, dispositivos, aplicaciones, cargas de trabajo y datos.
- Aplicación de políticas de seguridad en cualquier lugar en el que se lleve a cabo el trabajo, lo que incluye LAN, WAN, Data Centers, nubes y el perímetro.
- Gestión completa de identidades: para ampliar la gestión de identidades y accesos a fin de incluir las identidades de los usuarios, los dispositivos, las aplicaciones, las cargas de trabajo y los datos que se convierten en nuevos microperímetros mediante el acceso definido por software.
- Defensa integrada contra amenazas que aprovecha la información y la inteligencia de amenazas globales.
- Control ágil y totalmente automatizado de la red de su organización para funcionar de forma segura a la escala, el rendimiento y la fiabilidad deseados necesarios para lograr el objetivo.

Pasos hacia la confianza cero

La clave de la seguridad integral de confianza cero es ampliar la seguridad a todo el entorno de red, ya sea la LAN, el Data Center, el perímetro de la nube o la nube. Por supuesto, el cumplimiento es obligatorio.

Esta seguridad debe incluir una visibilidad total del entorno de red de su organización. Los pasos clave para lograr una confianza cero integral se centran en:

- Identifique los dispositivos y los datos confidenciales. Realice la identificación y clasificación de dispositivos, datos confidenciales y cargas de trabajo.
- Conozca el flujo de sus datos confidenciales.
- Diseñe su política de segmentación de confianza cero. Cada recurso basado en la red debe protegerse y segmentarse adecuadamente con el principio de menor privilegio, así como aplicarse de forma estricta controles granulares para que los usuarios solo tengan acceso a los recursos necesarios para realizar su trabajo.
- Implementar políticas y estados. Esto se puede realizar con plataformas como Cisco DNAC o ISE.
- Supervisar continuamente el entorno de confianza cero. Implemente análisis de seguridad

para supervisar y analizar en tiempo real los incidentes de seguridad e identificar rápidamente la actividad maliciosa. Inspeccione y registre continuamente todo el tráfico, tanto interno como externo.

Lograr un acceso de confianza

Para lograr una seguridad completa sin confianza, las organizaciones deben ampliar su enfoque de confianza cero a toda su plantilla, lugar de trabajo y cargas de trabajo.

- Zero Trust Workforce: los usuarios y los dispositivos deben autenticarse y autorizarse, y el acceso y los privilegios se supervisan y controlan continuamente para proteger los recursos.
- Zero Trust Workplace: el acceso debe controlarse en todo el espacio de trabajo, incluidos la nube y el perímetro.
- Cargas de trabajo de confianza cero: el control de acceso granular se debe aplicar a todas las pilas de aplicaciones, que incluyen contenedores, hipervisores y microservicios en la nube, así como Data Centers de agencias tradicionales.

Cisco, líder de confianza cero reconocido por Forrester, es un firme defensor de la habilitación de confianza cero en toda su red, tanto en las instalaciones como en la nube. No solo puede aprovechar su infraestructura de red de Cisco como base fundamental de su arquitectura Zero Trust, sino que también puede conocer otras funciones de seguridad clave de Cisco Zero Trust que pueden ayudar a su organización en su transición a Zero Trust.

Cartera segura de Cisco

Se pueden utilizar para crear un marco de confianza cero con éxito:

- Acceso seguro y sin fricciones para usuarios, dispositivos y aplicaciones mediante Cisco Duo
- Seguridad flexible en la nube mediante Cisco Umbrella
- Inspección inteligente de paquetes mediante Cisco Secure Firewall
- Protección frente a malware avanzado mediante un terminal seguro (anteriormente AMP)
- VPN segura y acceso remoto mediante Cisco AnyConnect
- Protección integral de cargas de trabajo mediante Cisco Secure Analytics (anteriormente conocido como StealthWatch)
- Segmentación de red protegida con Cisco Identity Services Engine (ISE)
- Visibilidad de aplicaciones y microsegmentación mediante Cisco Secure Workload
- Plataforma de seguridad integrada mediante Cisco SecureX
- Solución Unified SASE con suscripción como servicio mediante Cisco Secure Connect
- Asesoramiento experto del servicio Cisco Zero Trust Strategy
- Asistencia y servicios integrales a través de los servicios de consultoría, asesoramiento y soluciones

Summary

Una de las formas más simples de pensar en Zero Trust es "Nunca confiar Y siempre verificar".

Esto se aplica a todas las conexiones de red, todas las sesiones y todas las solicitudes de acceso a aplicaciones, cargas de trabajo y datos críticos.

Los marcos de seguridad de confianza cero crean defensas de microperímetro localizadas en torno a cada recurso de la red de la organización. Si se diseñan correctamente, los marcos pueden proteger los recursos independientemente de dónde se encuentren.

Una forma eficaz de reducir el riesgo es controlar el acceso a los datos privilegiados y compartidos y adoptar el principio de menor privilegio. Este modelo de seguridad permite la orquestación a través de las API, así como la integración con plataformas de automatización de flujos de trabajo que proporcionan visibilidad de los usuarios y las aplicaciones.

Si se implementa correctamente, Zero Trust puede ayudar a garantizar la seguridad y la fluidez de las operaciones en todo el entorno de tecnología de la información de una organización y generar un acceso de confianza continuo a las cargas de trabajo, aplicaciones y datos críticos de una organización, con el fin de mejorar las misiones de su organización.

Acerca de esta traducción
Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).