DELL Technologies

5 Recomendaciones para satisfacer sus necesidades de confianza cero

1	2	3	4	5
Planifique el cambio de paradigma para "nunca confiar, siempre verificar"	**Determine la ruta deseada**	**Será la organización la que impulse el entorno de confianza cero, no al revés**	**Céntrese en los datos**	**Aplique la máxima "Nunca confíe, siempre verifique" en todo el ecosistema de TI**
Determine el equilibrio aceptable entre la mitigación de riesgos y el impacto en el negocio	Mejora incremental de la seguridad	Genere controles en torno a las necesidades empresariales	Asegúrese de que toda la actividad de la red, los dispositivos y los usuarios se registre de forma continua	Las actividades de confianza cero, como la autenticación multifactor y la gestión de identidades, deben aplicarse universalmente para evitar brechas críticas
Tenga en cuenta los costes, el impacto para las operaciones y las partes interesadas, así como los requisitos normativos y de cumplimiento	Hiperescaladores	Documente procesos, funciones, responsabilidades y clasificaciones de datos	Utilice la IA y el ML para analizar los datos e identificar anomalías que puedan indicar amenazas	Incluya cadenas de suministro físicas y digitales de terceros en el marco de confianza cero
Evolucione de una seguridad basada en el perímetro a un modelo microsegmentado y centrado en los datos	Entorno específico	La experiencia del usuario sigue siendo esencial	Tenga en cuenta que la protección de datos y aplicaciones es la función clave de la arquitectura de confianza cero	
Cuente con ayuda externa si es necesario	La identidad es el nuevo perímetro	Las mejoras de seguridad, como la confianza cero, no pueden ir en detrimento de la facilidad de uso		
		Los objetivos de la organización, como el crecimiento y la innovación, siguen siendo primordiales		

En general, se considera que la confianza cero es la práctica recomendada para la arquitectura de seguridad.

Los datos indican que la mayoría de las empresas han empezado a plantearse implementar la confianza cero o están en proceso de implementarla[1]. Aunque el cambio a la confianza cero es importante, existen algunas consideraciones prácticas que guiarán el camino.

Los expertos en la materia de Dell Technologies, Tracy Emmersen (directora de adopción de soluciones de Project Fort Zero, y Justin Vogt (ingeniero jefe de seguridad), compartieron sus recomendaciones e información con Ash Lakshmanan, gestor de productos de servicios de seguridad. Sus sugerencias clave se resumen a continuación, o puede ver su conversación completa en dell.com/cybersecuritymonth.

> "Cuando consideramos la confianza cero desde un punto de vista integral, cuando damos un paso atrás, lo importante son los datos".
>
> ***Tracy Emmersen***
> *Directora de adopción de soluciones para el Project Fort Zero, Dell Technologies*

Planifique el (gran) cambio de paradigma para "nunca confiar, siempre verificar"

En su forma más fundamental, avanzar hacia un entorno de confianza cero representa un cambio importante con respecto a los modelos de seguridad tradicionales que se basan en los principios de "nunca confiar, siempre verificar" y acceso con privilegios mínimos. "Debemos abordar nuestro estado de seguridad de forma diferente a como lo hacíamos en el pasado, alejándonos de las soluciones tradicionales de seguridad de la red basadas en el perímetro y acercándonos más a una arquitectura microsegmentada y centrada en los datos", señala Emmersen.

Determine la ruta deseada

Emmersen explicó tres rutas distintas para lograr los beneficios de la confianza cero:

- **Incremental:** un enfoque iterativo que incorpora los principios clave de confianza cero al entorno actual
- **Hiperescalador:** aprovecha las funciones de confianza cero de los principales proveedores de cloud
- **Entorno específico y totalmente compatible:** entorno privado en las instalaciones creado desde cero, que cumple estrictamente los estándares de confianza cero

Además de estas tres rutas, las pequeñas y medianas empresas virtualizadas también pueden adoptar un enfoque denominado "la identidad es el nuevo perímetro". Esta metodología se centra en la gestión del acceso y las identidades y aprovecha las herramientas de SaaS para lograr una protección basada en la confianza cero. Un componente esencial de este método es la implementación de la autenticación multifactor (MFA) en todas partes, lo que ilustra el impacto de esta capacidad de confianza cero.

Los enfoques de hiperescalador e identidad suelen tener un coste más bajo, mientras que los entornos incrementales y específicos requieren una mayor inversión.

Será la organización la que impulse la adopción de la confianza cero, no al revés

En su forma más fundamental, una arquitectura de confianza cero está diseñada para gestionar y proteger los flujos de trabajo, los roles de usuario y los privilegios relacionados, los dispositivos, los datos, las aplicaciones y las redes de una organización. La primera parte de una implementación requiere una documentación sólida en estos aspectos y, a continuación, el plano de control y la infraestructura se diseñan para aplicar las políticas que los rigen.

Si el entorno de confianza cero inhibe o altera significativamente las operaciones empresariales en detrimento de la empresa, es probable que la seguridad mejorada que se consiga no merezca la pena. Como señala Vogt, "Si [la seguridad]... se interpone en el camino de la misión central de la organización... En realidad, no somos mejores que los adversarios a los que intentamos enfrentarnos. Simplemente proporcionamos nuestra propia denegación de servicio".

Céntrese en los datos

Como indica Emmersen: "Cuando consideramos la confianza cero desde un punto de vista integral, cuando damos un paso atrás, lo importante son los datos". Proteger los datos de la organización es uno de los beneficios más valiosos del cambio a la confianza cero, y principios como la verificación y la segmentación continuas protegen los datos y las aplicaciones para evitar que las amenazas se desplacen lateralmente dentro de la red.

El registro y la supervisión continuos son componentes esenciales de la confianza cero, y esos datos y telemetría se analizan para identificar anomalías que puedan indicar un riesgo o una amenaza. Por ejemplo, un cambio en los patrones de uso de datos puede identificar una posible filtración o un ataque de ransomware.

1. De un estudio encargado por Dell a Enterprise Strategy Group, "Assessing Organizations' Security Journeys: Insights Spanning the Attack Surface, Threat Detection and Response, Attack Recovery, and Zero Trust", noviembre de 2023

DELL Technologies

Dada la enorme cantidad de datos generados por el registro de toda la actividad, las herramientas de análisis modernas deben utilizar la IA y el aprendizaje automático para ser eficaces.

El lema "Nunca confíe, siempre verifique" debe aplicarse en todo momento

Aunque gran parte del enfoque en los datos, las aplicaciones, los usuarios y los dispositivos es interno, el escrutinio inherente a una arquitectura de confianza cero debe aplicarse a lo largo de todo el ciclo de vida de TI. De lo contrario, se podrían producir vulneraciones de seguridad críticas.

La cadena de suministro es un buen ejemplo, y Vogt sugiere plantear preguntas importantes sobre el hardware y el software de otros fabricantes:

- "¿Quién más ha tenido acceso?
- ¿De qué está hecho?
- ¿Qué más hay bajo la superficie?
- ¿Cómo podemos aplicar estos principios de confianza cero [y] tener algún tipo de proceso de verificación y algún tipo de postura de privilegios mínimos a la tecnología que estamos consumiendo? ¿Incluso si es ascendente en la cadena de suministro tecnológica?"

Avanzar hacia una arquitectura de confianza cero o implementar sus principios representa la práctica recomendada actual para avanzar en la madurez de la ciberseguridad. Varias rutas representan diferentes soluciones intermedias entre el coste, el riesgo y el nivel de mejora de la seguridad. El primer paso debe ser determinar la posición única de la organización y dejar que eso guíe las decisiones tecnológicas.

Descubra cómo afrontar algunos de los principales retos de ciberseguridad actuales en **dell.com/cybersecuritymonth**

DELL Technologies