Engineer

Confianza cero

modelo que no da confianza solo por la ubicación en la red

Qué es

La confianza cero es un modelo de seguridad en el que nada recibe confianza por el lugar que ocupa en la red. NIST SP 800-207, la publicación federal estadounidense que expuso el modelo en 2020, lo define como un paradigma centrado en proteger recursos, con la premisa de que la confianza nunca se concede de forma implícita y debe evaluarse continuamente. Estar en la red de la oficina, conectado a la VPN o en el mismo centro de datos no da por sí solo ningún derecho a una petición. Cada solicitud de un recurso se decide por sus circunstancias: quién pide, desde qué dispositivo, qué pide y bajo qué condiciones. En inglés, zero-trust con guion modifica un nombre, como en zero-trust design. El plan que pone el modelo en práctica se llama arquitectura de confianza cero, o ZTA por sus siglas inglesas.

NIST nombra a las partes con precisión. Un sujeto es quien o lo que hace una petición: un usuario, un servicio o un dispositivo. Un recurso es cualquier cosa que merezca protección; la publicación incluye impresoras y capacidad de cómputo junto con los datos. Entre ambos hay tres componentes lógicos. El motor de políticas decide si se concede la solicitud y registra la decisión. El administrador de políticas la ejecuta, abre o cierra el camino entre sujeto y recurso y emite las credenciales o tokens para esa sesión concreta. El punto de aplicación de políticas está en el propio camino: deja pasar la sesión, la vigila y la termina cuando se le ordena.

La publicación explica el cambio con un aeropuerto. Los pasajeros pasan un único control y, al otro lado, viajeros, tripulaciones y personal del aeropuerto se mueven por la terminal y reciben todos un trato de confianza. Esa terminal es lo que NIST llama una zona de confianza implícita: un área donde se confía en cada persona hasta el nivel del último control que ha superado. Una red de oficina plana funciona igual. La confianza cero reduce esa zona todo lo posible al acercar la decisión y su aplicación al recurso.

Utilice el concepto en una decisión

Aplique «¿Qué es la confianza cero?» a una decisión real. Podemos ayudarle a relacionar el concepto con el sistema que está construyendo o comprando. Cuentas, contraseñas y permisos organizados para que cada persona tenga exactamente el acceso que necesita y lo pierda el mismo día que deja la empresa.

Explore nuestros servicios Póngase en contacto →

Compruebe los supuestos detrás del término

Utilice la explicación y los trabajos enlazados para formular preguntas sobre su proyecto. Podemos examinar los supuestos con usted antes de elegir una herramienta. 1.000 reglas RBAC para servidores Linux — 1,000 reglas de acceso escritas para cerrar una brecha de seguridad

1.000 reglas RBAC para servidores Linux Póngase en contacto →

Por qué importa

El modelo anterior traza una frontera alrededor de la organización y confía en lo que queda dentro. La objeción de NIST es clara: cuando los atacantes atraviesan el perímetro, el movimiento lateral no encuentra obstáculos, y el movimiento lateral no autorizado ha sido uno de los mayores retos de las agencias para las que se escribió la publicación. Además, la frontera ha dejado de ajustarse al trabajo. El personal inicia sesión desde redes domésticas y de hoteles, se admiten dispositivos personales en algunos sistemas y gran parte de lo que utiliza se ejecuta en la nube de otro. De ahí las premisas de NIST: la red privada no es una zona de confianza implícita, un atacante puede estar ya dentro y el personal remoto debería tratar como hostil la red local desde la que se conecta.

Lo que gana un equipo es la contención. Según el tercero de los siete principios de NIST, el acceso se concede por sesión con los mínimos privilegios necesarios para la tarea, y autenticarse ante un recurso no concede nada sobre otro. Una contraseña robada o un portátil comprometido alcanzan entonces lo que esa cuenta y ese dispositivo tienen permitido en ese momento y a través de un punto de aplicación, en vez de toda la red interna. Las decisiones también dejan rastro. El motor de políticas registra cada concesión y cada rechazo, por lo que la pregunta de quién podía llegar a un sistema y por qué se responde con registros en lugar de con recuerdos.

Cómo se aplica en la práctica

Pensemos en un sistema de compras, el tipo de aplicación que NIST propone para una primera migración porque lo utiliza un grupo definido de empleados, a diferencia del correo, del que depende toda la organización. Una persona del equipo de compras lo abre desde un portátil de la empresa. La petición llega al punto de aplicación situado delante de la aplicación, que pregunta al motor de políticas. El algoritmo de confianza del motor sopesa los datos que enumera

NIST: la propia petición, incluidas la versión del sistema operativo del dispositivo y su nivel de parches; la base de datos de sujetos; la de activos; los requisitos del propio recurso, que pueden indicar un nivel de garantía de autenticación o rechazar direcciones del extranjero; y la inteligencia de amenazas. Un registro ilustrativo de la decisión, con nombres de campos inventados por nosotros y ajenos a cualquier producto, podría ser el siguiente:

```
solicitud buyer-17 en laptop-0417 -> aplicación de compras, lectura y escritura
sujeto    equipo de compras; sesión iniciada con clave resistente al phishing
activo    gestionado por la empresa; parches de OS al día; disco cifrado
recurso   exige AAL2 o superior, equipo gestionado e IP de origen nacional
amenaza   dirección de origen ausente de las fuentes de amenazas consultadas
decisión  autorizar leer y escribir solo esta sesión; registrar como aprobado
```

La concesión cubre esta sesión y esta aplicación concretas. Cuando la misma persona, en el mismo portátil, abre los contratos de proveedores guardados en un almacén de documentos, el motor toma una nueva decisión de acceso: autenticarse ante el primer recurso no concede automáticamente acceso al segundo. También cuenta el contexto. Un ejemplo de NIST es un contable que normalmente trabaja en horario de oficina y, de pronto, pide acceso al sistema financiero en plena noche desde un lugar que el motor no reconoce. Un algoritmo de confianza contextual puede generar una alerta y exigir primero que el sujeto cumpla un nivel de confianza más estricto. Otro es un empleado de recursos humanos que lee entre 20 y 30 expedientes de personal un día normal y después solicita más de 100.

Para los servicios en la nube, NIST señala que los clientes pueden acudir directamente al servicio, con los puntos de aplicación de la organización comprobando la política en el camino, en lugar de entrar primero por una VPN en la red interna. Todas esas decisiones dependen de saber quién debe llegar a qué. NIST pide inventariar activos, sujetos, flujos de datos y procesos de trabajo antes de construir nada. Esa preparación es el tipo de consolidación que describe nuestro caso sobre gestión del acceso en M365 y SSO: identidades y accesos reunidos en M365, 1Password, Red Hat SSO y OKTA SSO, mínimo privilegio aplicado e incorporación y salida de personal normalizadas para conceder y revocar el acceso con rapidez.

Dónde surgen los problemas

Comprarlo como un producto. NIST indica que la confianza cero es un conjunto de principios orientadores, en lugar de una arquitectura única, y que no existe un único conjunto de herramientas o servicios para una empresa de confianza cero. Una nueva pasarela de acceso remoto con esa etiqueta cambia poco si cada sujeto que admite sigue llegando a toda la red situada detrás. Trate el cambio, en palabras de NIST, como «un recorrido en lugar de una sustitución completa», un proceso de negocio cada vez. Juzgue cada producto por los principios que pretende cumplir, incluido si sus formatos de datos permitirían cambiarlo después por otro proveedor.

Escribir la política antes del inventario. El motor de políticas solo puede decidir a partir de lo que sabe sobre sujetos, activos y procesos. Si esa información está incompleta, advierte NIST, el resultado habitual es un proceso de negocio detenido porque el motor rechaza peticiones por falta de datos. La TI en la sombra, los sistemas creados fuera de la gestión del departamento de TI, agrava el problema. Primero identifique y catalogue activos, sujetos, flujos de datos y procesos, incluida esa TI en la sombra. Solo después escriba los criterios para un proceso candidato.

Los administradores conservan acceso general. En muchos diseños antiguos, los desarrolladores y administradores de sistemas pueden llegar a todos los recursos. NIST señala esas cuentas para examinarlas con especial atención. Someter al resto a decisiones de acceso por sesión mientras las cuentas de administrador conservan su alcance permanente deja las credenciales más valiosas como el camino más corto hacia dentro. Haga pasar también las cuentas privilegiadas por el mismo motor, deles el acceso que necesita su tarea actual y use registros y auditorías para conocer sus patrones habituales y detectar las desviaciones.

El motor de políticas se convierte en el nuevo perímetro. Ningún recurso se comunica con otro sin la aprobación del motor y del administrador. Quien tenga acceso a las reglas del motor puede hacer cambios no autorizados o cometer errores, y un atacante que interrumpa los puntos de aplicación o el administrador puede detener el negocio. Registre y audite cada cambio de configuración, ejecute la aplicación de políticas en un entorno de nube bien protegido o replíquela en varios lugares, y aplique las restricciones de acceso más estrictas a los datos de tráfico almacenados y a la política: solo desde cuentas de administrador dedicadas.

Aplicarlo todo desde el primer día. Pocas políticas aciertan a la primera. NIST prevé una fase de ajuste en la que se rechazan peticiones que deberían prosperar. Pasar directamente a la aplicación estricta deja a empleados sin acceso al trabajo que necesitan hacer por cada carencia de la política. Ejecute durante un tiempo el nuevo proceso en modo de solo informes. Conceda la mayoría de las peticiones, compare los registros con la política prevista y aplique únicamente lo básico, como rechazar las peticiones que fallen la MFA o procedan de direcciones conocidas como hostiles. Endurezca la política cuando comprenda el patrón normal.

Tratar la MFA como la meta. La MFA reduce el riesgo de una contraseña robada, pero NIST señala que un atacante con credenciales válidas o una persona de dentro con malas intenciones aún puede llegar a todo lo que permita la cuenta. Mantenga limitado el alcance de cada cuenta y use un algoritmo de confianza contextual que sopese hora, lugar y volumen, para que unas credenciales válidas usadas de forma inusual también generen una alerta.

Lecturas adicionales

- NIST SP 800-207, Zero Trust Architecture — publicación de agosto de 2020: definición, siete principios, componentes lógicos, amenazas y hoja de ruta para la migración.
- NIST SP 1800-35, Implementing a Zero Trust Architecture — guía práctica de NIST publicada en junio de 2025, con 19 implementaciones de ejemplo construidas con 24 colaboradores.
- NIST SP 800-207A — publicación de septiembre de 2023: control de acceso a aplicaciones nativas de nube entre varias nubes mediante pasarelas API, proxies auxiliares y identidades de servicio, en lugar de direcciones de red.
- NIST SP 800-63B-4 — niveles de garantía de autenticación que pueden exigir los recursos; entre ellos, AAL3 requiere resistencia al phishing.

Glosario

Elija según sus restricciones reales

Describa la ruta de despliegue, los riesgos operativos y quiénes se encargan de las guardias. Podemos definir el alcance de un cambio con comprobaciones, una vía de recuperación y responsabilidades claras.

Vea cuánto cuesta Póngase en contacto →

Haga práctica la terminología

Pregunte cómo se aplica «¿Qué es la confianza cero?» a su organización. Basta un ejemplo concreto de su sistema actual para iniciar la conversación.

Explore nuestros servicios

welcome@engineer.company +45 50 10 61 84 Copenhague, Dinamarca

Llévese esta página

Tarjeta de contacto

Creado con esmero y cariño por D.

CVR 45969703 · Tagensvej 105C, 3. th, 2200 København N

Derechos de autor © 2025 – actualidad · Engineer ApS · Todos los derechos reservados.

Impreso desde https://engineer.company/es/glossary/zero-trust/