Red Hat
Enterprise Linux

Funciones de Top Red Hat Enterprise Linux para la implementación de arquitecturas de confianza cero

Contenidos

Mantén protegida tu organización con zero trust (confianza cero)

A medida que las organizaciones amplían el uso de las nubes públicas, los dispositivos móviles y las prácticas de teletrabajo, los perímetros de red tradicionales se fragmentan e introducen nuevos retos de seguridad en los entornos de TI.

Las organizaciones se enfrentan cada vez con mayor frecuencia a participantes malintencionados que intentan aprovechar las vulnerabilidades existentes causadas por paradigmas de seguridad obsoletos como la autenticación de un solo factor, la confianza implícita, las arquitecturas basadas en el perímetro y el seguimiento inadecuado del comportamiento de los usuarios y los eventos. A medida que las amenazas para la seguridad y el impacto de las filtraciones siguen en aumento, las organizaciones reconocen la necesidad de una estrategia de seguridad más sólida y proactiva. De hecho, más del 50 % de los profesionales de la ciberseguridad consideran que la mejora de la gestión de identidades y accesos, y el acceso seguro a las aplicaciones son prioridades actuales en materia de seguridad.[1]

La confianza cero propone un cambio fundamental en la forma en que percibimos y establecemos la confianza dentro de una red, al tiempo que rechaza la suposición de que todo lo que está dentro es seguro y todo lo que está fuera no lo es. Desafía el modelo tradicional al asumir que ningún usuario ni activo puede ser intrínsecamente fiable dentro o fuera del perímetro de una red. En su lugar, los usuarios y los activos deben autenticarse y autorizarse continuamente con independencia de su ubicación o acceso a la red.

Este libro electrónico analiza las consideraciones para el establecimiento de arquitecturas de confianza cero en entornos Linux® y cómo Red Hat® Enterprise Linux puede ayudarte a proteger tu entorno de TI y tu organización.

El alto coste de un panorama de amenazas cambiante

4,45 millones USD
Coste medio de una filtración de datos en todos los sectores y regiones en 2023[2]

180 358 USD
Reducción media de los costes de filtraciones cuando se implanta una gestión eficaz de identidades y accesos[2]

82 %
Proporción de filtraciones que afectaron a datos almacenados en entornos de nube o en múltiples entornos[2]

51 %
Porcentaje de organizaciones que piensan aumentar las inversiones en seguridad como consecuencia de una filtración[2]

1 *Cybersecurity Insiders patrocinado por Fortra. "2023 Zero Trust Security Report", 2023.*

2 *Seguridad de IBM. "Cost of a Data Breach Report 2023", julio de 2023.*

¿Qué es la confianza cero?

La confianza cero es un patrón arquitectónico que aplica la seguridad a cada activo, en lugar de gestionar exclusivamente la seguridad en el perímetro de una red o mediante una solución centralizada de gestión de la seguridad. El principio fundamental del modelo de confianza cero es que no se confía implícitamente en ningún participante, sistema, red o servicio que opere dentro o fuera del perímetro de seguridad. Para que un recurso se conecte a otro, la sesión debe autenticarse y autorizarse para establecer una confianza explícita.

¿Cómo funciona la confianza cero?

La gestión de identidades y accesos es el núcleo de las arquitecturas de confianza cero. Las arquitecturas de confianza cero deben denegar el acceso a los activos de forma predeterminada. Todo sujeto que quiera interactuar con un recurso debe solicitar acceso explícito para esa interacción específica y debe evaluarse el riesgo de esa interacción antes de permitir el acceso. Por esta razón, resulta fundamental comprender la identidad y los atributos del sujeto. Se debe determinar quién solicita el acceso, a qué recursos necesita acceder, la finalidad de la transacción y cómo debe limitarse el acceso según el tiempo, el método y la función.

Una vez tomadas las decisiones de acceso, se deben almacenar, gestionar, conservar y actualizar las identidades y los atributos de identidad de forma protegida y coherente. La mayoría de las organizaciones utilizan uno o más sistemas de gestión de identidades, servidores de directorios o gestión de credenciales para administrar esta información. También deberían reevaluarse continuamente estas decisiones de acceso para garantizar su validez continuada a lo largo del tiempo.

Una arquitectura de confianza cero basada en estos principios clave puede ayudarte a proteger mejor tu entorno de TI y tu organización:

1. Nunca confíes implícitamente en los participantes.
2. Emplea una estrategia de acceso de mínimo privilegio.
3. Asume que las redes y el tráfico de red se ven comprometidos de forma predeterminada.

Estos son los principios clave que Red Hat emplea para guiar las capacidades de confianza cero en toda la cartera de Red Hat, incluidos Red Hat Enterprise Linux, Red Hat Insights y Red Hat Identity Management.

¿Qué es un límite de confianza?

Un límite de confianza es cualquier separación lógica entre componentes en la que los sujetos que participan en una interacción cambian su estado de confianza, normalmente entre los dos estados *fiable* y *no fiable*. Por lo general, la transición de *no fiable* a *fiable* exige la autenticación de la identidad del sujeto y la autorización del derecho del sujeto, así como la necesidad de acceder a un activo específico.

Sistemas operativos: En qué se basa la confianza cero

Tu sistema operativo es la base de tu entorno de TI y de la arquitectura de confianza cero. Proporciona funciones esenciales de seguridad, controla el acceso de usuarios y aplicaciones, cifra la información confidencial y protege los secretos con objeto de establecer y mantener un entorno informático centrado en la seguridad.

Este capítulo cubre las capacidades fundamentales del sistema operativo para la adopción de la confianza cero.

Cadena de suministro del sistema operativo fiable

Los modelos de confianza cero exigen que tu sistema operativo tenga la mayor seguridad posible. Para reducir el riesgo de vulnerabilidades de seguridad en el sistema operativo, Red Hat Enterprise Linux usa una cadena de suministro de software. El análisis de código estático de todo el sistema operativo identifica errores en el estilo de programación, los métodos de referencia de la memoria y la validación del flujo de entrada, además de garantizar el cumplimiento normativo con prácticas habituales de codificación. Las exhaustivas pruebas de ingeniería de calidad (QE) minimizan los fallos de seguridad antes del envío. Los procesos de parches para la vulnerabilidad por lo general permiten el remedio frente a problemas conocidos. Las listas de materiales del software (SBOM) publicadas permiten auditar y evaluar componentes seleccionados y probados —incluidos el código fuente, software y bibliotecas de código abierto, middleware y marcos de desarrollo— que forman parte de Red Hat Enterprise Linux.

Control de acceso obligatorio

Para implementar una arquitectura de confianza cero, tu sistema operativo debe tener la capacidad de aislar y controlar el acceso a recursos con un criterio individual. Red Hat Enterprise Linux incorpora controles de acceso obligatorios (MAC) con Security-Enhanced Linux (SELinux), una tecnología que gestiona el acceso mediante políticas centralizadas de seguridad. El control granular y personalizable sobre archivos, procesos, usuarios y aplicaciones minimiza el riesgo de escalabilidad inapropiada de privilegios, mientras que el aislamiento de procesos y la separación de contenedores mitigan los ataques de escalabilidad de privilegios. Asimismo, la posibilidad de denegar todo acceso de forma predeterminada está en consonancia con la confianza cero y los principios de mínimo privilegio.

Prueba a generar perfiles de seguridad SELinux personalizados para aplicaciones en contenedores.

Accede al **laboratorio interactivo**.

Lista de permisos de aplicaciones

La lista de permisos de aplicaciones establece un índice de aplicaciones aprobadas que tienen permiso para su ejecución en un sistema por parte de un usuario específico. Esta práctica complementa los controles de acceso obligatorios, que pueden supervisar el comportamiento de las aplicaciones, pero sin saber qué aplicaciones son fiables. Red Hat Enterprise Linux proporciona capacidades incorporadas de listas de permisos de aplicaciones mediante el daemon de la política de acceso a archivos (fapolicyd) para detectar las aplicaciones no autorizadas y evitar su ejecución en sistemas o redes. Además, con políticas de listas de permisos predefinidas y personalizables, los administradores de sistemas cuentan con un mayor control sobre las aplicaciones que se ejecutan en sus servidores y redes.

Aprende a aprobar aplicaciones con fapolicyd.

Accede al **laboratorio interactivo**.

Cifrado moderno, escalable y basado en políticas

El cifrado de datos y del tráfico de la red supone una mayor protección para tu entorno de TI y tu organización. Algunas normas del sector —incluida la Norma Federal de Tratamiento de la Información (FIPS) 140 del Instituto Nacional de Normas y Tecnología (NIST) de los EE. UU.— exigen la configuración de un cifrado que cubra todo el sistema. Los controles de la criptografía personalizable y basada en políticas de Red Hat Enterprise Linux te permiten aplicar configuraciones coherentes en todos tus sistemas para que puedas satisfacer estos requisitos. Los perfiles predeterminados para las normas comunes de seguridad simplifican el cumplimiento normativo. Asimismo, la aplicación y el cumplimiento automatizados de políticas optimizan la gestión, reducen los errores y controlan el descifrado de archivos y volúmenes de software.

Aprende a usar políticas criptográficas en todo el sistema.

Accede al **laboratorio interactivo para su configuración**.

Accede al **laboratorio interactivo para su personalización**.

Protección de datos en todas las fases

Los modelos de confianza cero requieren que los datos estén asegurados en todo momento: durante su uso, en movimiento y en reposo. Red Hat Enterprise Linux es compatible con tecnologías y capacidades que proporcionan una protección ininterrumpida para tus datos. Las capacidades de Trusted Execution Environment (TEE) y el soporte de AMD Secure Encrypted Virtualization (SEV) e Intel Software Guard Extensions (SGX) sirven para salvaguardar las cargas de trabajo y los datos en uso. El establecimiento y la gestión centralizados y automatizados de las conexiones de seguridad del nivel de transporte cifrado (TLS) aumentan la seguridad de los datos en movimiento. Asimismo, Linux Unified Key Setup (LUKS) y Network Bound Disk Encryption (NBDE) proporcionan una protección de datos coherente en entornos híbridos en la nube.

Una raíz de confianza basada en hardware

La raíz de confianza basada en hardware, los testimonios remotos y las tecnologías de arranque medido te ayudan a verificar la integridad del sistema y asegurarte de que tus sistemas no se han modificado ni alterado. Red Hat Enterprise Linux proporciona capacidades fundamentales compatibles con estas tecnologías.

- Saca a la luz tus secretos criptográficos del software y llévatelos a dispositivos de hardware a prueba de alteraciones como las tarjetas inteligentes, los módulos de seguridad del hardware (HSM) y los módulos de plataformas fiables (TPM).
- Usa TPM y capacidades de arranque medido para computar y almacenar criptográficamente las mediciones de hashes de los procesos seguros de arranque y los códigos binarios del tiempo de ejecución.
- Comprueba las mediciones del arranque con agentes de testimonios remotos para determinar si los sistemas están en peligro antes de iniciar las acciones correspondientes de remedio.

Análisis del cumplimiento normativo

El incumplimiento normativo de las normas empresariales y del sector puede acarrear peligros y costes para tu organización. Red Hat Enterprise Linux incorpora herramientas de análisis del cumplimiento normativo y de vulnerabilidad como Open Security Content Automation Protocol (OpenSCAP) que ayudan a automatizar y simplificar las auditorías, encontrar y remediar los sistemas con una configuración indebida y mantener el cumplimiento normativo con el menor esfuerzo. Entre las funciones fundamentales se incluyen las siguientes:

- Perfiles de cumplimiento normativo predefinidos y personalizables.
- Capacidades de generación de informes y de referencias.
- Integración con Red Hat Satellite y Red Hat Insights para la gestión a gran escala.
- Referencias incorporadas de seguridad para la Norma de Seguridad de Datos del Sector de Tarjetas de Pago (PCI-DSS), Perfil de Protección Mejorada de Sistemas Operativos (OSPP), Centro Australiano de Ciberseguridad (ACSC) o Essential Eight, Referencia del Centro de Seguridad de Internet (CIS), Ley de Portabilidad y Responsabilidad de los Seguros Médicos (HIPAA) y Guías de Implementación Técnica de Seguridad de la Agencia de Sistemas de Información para la Defensa (DISA STIG).

Prueba el análisis del cumplimiento normativo de la seguridad y de la vulnerabilidad mediante OpenSCAP.

Accede al **laboratorio interactivo**.

Aprende a remediar las vulnerabilidades con Red Hat Insights.

Accede al **laboratorio interactivo**.

Gestión automatizada de configuraciones

La automatización resulta crítica para mantener configuraciones coherentes de seguridad y satisfacer los requisitos de gobernanza y cumplimiento normativo a gran escala. Las funciones del sistema Red Hat Enterprise Linux te permiten automatizar la configuración y gestión de la seguridad en entornos híbridos en la nube y reducir la experiencia precisa para implementar una arquitectura de confianza cero. Este contenido predefinido de automatización basado en Red Hat Ansible® Automation Platform simplifica la configuración de funciones centradas en la seguridad como SELinux, NBDE, Secure Shell (SSH), políticas criptográficas y gestión de identidades y certificados.

Prueba las funciones del sistema de Try Red Hat Enterprise Linux

Accede al **laboratorio interactivo**.

Administración de identidades: Control de acceso para recursos de TI

Las soluciones de gestión de identidades (IdM) garantizan que los usuarios autorizados –y solo los usuarios autorizados– puedan acceder a los recursos que precisan. Al abarcar las políticas y tecnologías en toda la organización, estas soluciones con toda propiedad identifican, autentican y autorizan el acceso a activos mediante identidades, atributos, credenciales y certificados.

Este capítulo cubre las capacidades fundamentales de la gestión de identidades para la adopción de la confianza cero.

Almacén de identidades

El controlador de dominios te permite gestionar identidades, accesos y políticas para usuarios, servicios y hosts. Incluido en Red Hat Enterprise Linux, Red Hat Identity Management es un almacén centralizado de identidades y un controlador de dominios que ayuda a reducir la carga administrativa, simplificar la gestión de la seguridad y garantizar la coherencia en todo tu entorno. Gracias a él, puedes almacenar todas las identidades en un solo lugar, consolidar operaciones y aplicar políticas de modo uniforme en todos los recursos y entornos. El registro simplificado de dominios te permite crear unos límites de seguridad fiables, mientras que la autenticación optimizada mejora la experiencia global de los usuarios finales.

Inicio de sesión único

En las arquitecturas de cero confianza, cada servicio, dispositivo y servidor exige una autenticación de acceso independiente. Los sistemas con inicio de sesión único (SSO) simplifican el acceso mediante el uso de un servicio central de identidades que permite a los servidores comprobar los usuarios verificados. Red Hat Enterprise Linux es compatible con OAuth 2.0 y Red Hat Identity Management, lo que les permite a los usuarios autenticarse una sola vez y acceder a numerosos servicios y así disponer de una experiencia optimizada. La integración con diversos servicios –entre los que se incluyen la tecnología de inicio de sesión único de Red Hat, Microsoft AzureAD y GitHub– te permite seguir usando tus servicios de identidades existentes, además de ofrecer la flexibilidad precisa de cara al futuro.

Integración con otros sistemas de gestión de identidades

La mayoría de las organizaciones ya usan uno o más sistemas de gestión de identidades para sus entornos Linux y Windows. La integración de estos sistemas en una sola solución global puede ayudarte a centralizar las operaciones, garantizar la coherencia en toda tu organización y mejorar la eficacia administrativa. Red Hat Identity Management se integra de forma original con Microsoft Active Directory, por lo que puedes gestionar identidades en todos tus entornos mixtos, al tiempo que aplicas políticas personalizadas de control de accesos a tu dominio de Red Hat Enterprise Linux.

Gestión de políticas

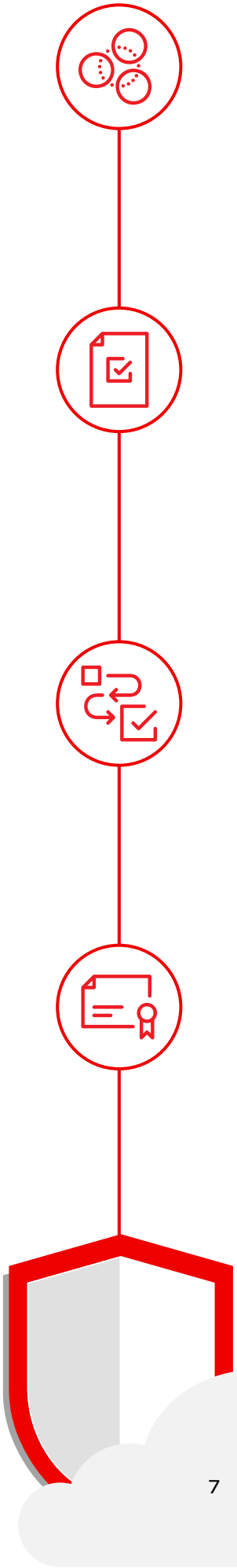
Un enfoque basado en políticas que cubra la gestión de identidades puede servirte para mejorar la coherencia, la eficacia y la seguridad. Red Hat Identity Management te permite establecer y aplicar controles basados en políticas desde una interfaz centralizada para así garantizar que las identidades, los accesos y los recursos se pueden configurar con propiedad. Las políticas personalizables de identidades y accesos ayudan a limitar la escalabilidad de privilegios en todo tu entorno. Asimismo, los controles de acceso basados en funciones (RBAC) te permiten delegar las capacidades administrativas de los servidores de gestión de identidades —incluidos la gestión de autenticaciones y autorizaciones, y la grabación, auditoría y registro de sesiones— en tu equipo.

Autenticación multifactorial

La autenticación multifactorial (MFA) añade una capa extra de seguridad al requerir varias comprobaciones para verificar una identidad antes de conceder el acceso. Red Hat Identity Management incluye la MFA mediante dispositivos criptográficos como tokens de hardware y tarjetas inteligentes. También puedes seleccionar y configurar diversos tipos de autenticación —entre los que se incluyen contraseñas, certificados, servicio de usuario de marcación de autenticación remota (RADIUS), contraseñas de un solo uso (OTP) y criptografía de claves públicas para la autenticación inicial (PKINIT)—, así como establecer métodos de autenticación predeterminados para todos los usuarios.

Gestión de certificados

Los certificados digitales contienen la información necesaria para autenticar la identidad de usuarios, aplicaciones, sitios web y otros sujetos. Estos deberían crearse, monitorizarse, renovarse y retirarse con arreglo a los principios de mínimo privilegio. Red Hat Identity Management es compatible con la gestión de ciclos de vida útil completos para los certificados de usuarios, hosts y servicios. También puedes implementar Red Hat Certificate System, una autoridad de certificados que admite actividades de gestión avanzada como la disponibilidad de tarjetas inteligentes, tipos de certificados personalizados y almacenamiento secreto protegido. La compatibilidad con protocolos y normas comunes —incluidos X.509, Automatic Certificate Management Environment (ACME), Simple Certificate Enrollment Protocol (SCEP) y Secure Sockets Layer (SSL), y TLS— te permite crear certificados aptos para tu ecosistema de TI. El seguimiento automático de las fechas de caducidad de los certificados garantiza unas renovaciones puntuales. Asimismo, la autenticación de infraestructura de claves públicas (PKI) comprueba que las identidades sean fiables.

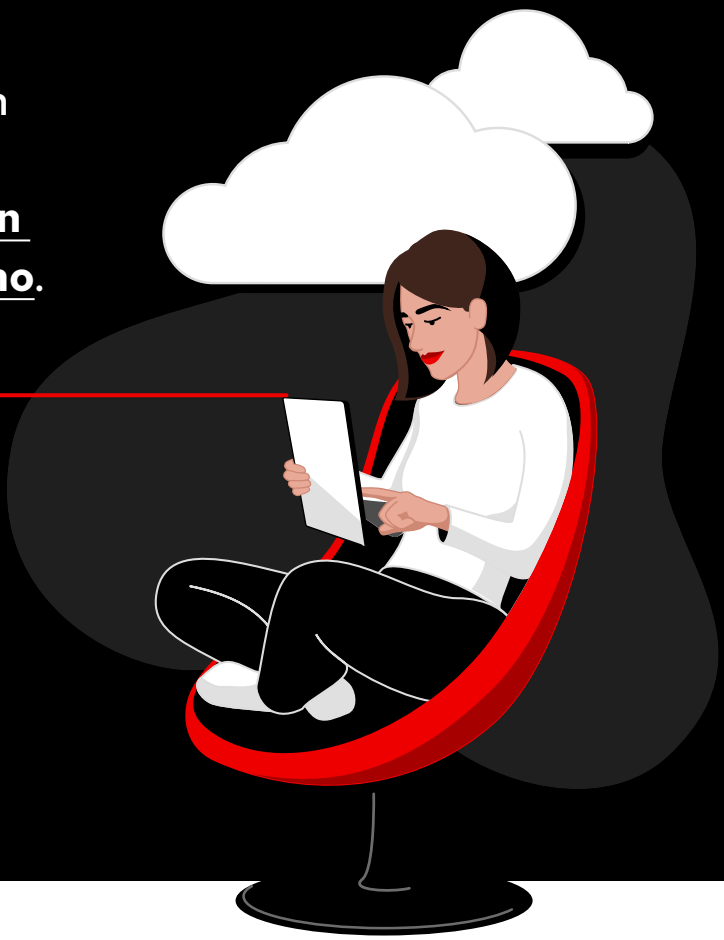


Comienza ahora mismo con confianza cero

La adopción de una arquitectura de confianza cero puede ayudarte a proteger tus activos de TI y empresariales en un mundo sometido a rápidos cambios.

Red Hat proporciona una base fiable, integrada y centrada en la seguridad para las arquitecturas de confianza cero. De hecho, ya puedes usar muchos de los componentes precisos para implementar un modelo de confianza cero. Red Hat Enterprise Linux ofrece tecnologías de seguridad, controles, certificaciones y soporte para el diseño, creación y gestión de arquitecturas de confianza cero. Además, con Red Hat Identity Management, puedes centralizar la gestión de identidades, respetar los controles de seguridad y cumplir con las normas de seguridad en todo tu entorno.

Pruébalo hoy mismo con nuestros **laboratorios interactivos basados en la web y sin coste alguno**.



568051_0124_KVM

Red Hat