DELL Technologies

Confianza cero
La trayectoria para mejorar la ciberseguridad

Elija la trayectoria hacia la confianza cero de la mano de un socio experto en tecnología y seguridad.

Las organizaciones que impulsan la madurez de su ciberseguridad están creando un roadmap procesable que identifica formas de reducir la superficie de ataque, detecta las ciberamenazas y responde ante ellas, e implementa formas de recuperarse de los ciberataques, todo mediante capacidades que facilitan la confianza cero.

Para abordar las ciberamenazas cada vez más sofisticadas, Dell utiliza las capacidades de seguridad integradas en nuestras soluciones y nuestros socios para que nuestros clientes logren una confianza cero que se adapte a los objetivos empresariales de los clientes.

¿Qué es la confianza cero?

Imagine que su red es un castillo. Si el puente está bajado y alguien entra, puede deambular con libertad. Ha llegado el momento de actualizar el modelo de seguridad de defensa basado en el perímetro a la infraestructura de seguridad de confianza cero más moderna y segura.

La confianza cero no es un producto que se compra, sino una estrategia que aborda la seguridad desde la arquitectura. Nunca se fía y siempre verifica que el uso comercial sea legítimo antes de conceder acceso a los recursos a cualquier persona o cosa. Esto significa que no confía en los usuarios y los dispositivos de forma predeterminada, a pesar de que estén conectados a una red con permisos e incluso se hayan verificado previamente.

Nunca confíe, siempre verifique.

Aspectos fundamentales de un ecosistema de TI seguro.

El Departamento de Defensa de los Estados Unidos (DoD) ha adoptado e integrado en una arquitectura la infraestructura de confianza cero, tal y como la define el National Institute of Standards and Technologies (NIST).

Incluye siete pilares interrelacionados que guían a Dell Technologies en todos los dominios de seguridad. Cuando se combinan, los pilares ofrecen una arquitectura integrada de varios niveles para lograr un enfoque de seguridad integral que proteja la infraestructura y los datos de su organización.

La adopción del modelo de confianza cero ha sido un desafío debido a la complejidad de integrar diversas capacidades de seguridad y moverse por opciones fragmentadas entre varios proveedores de seguridad.

NIST

U.S. Department of Defense

DELL Technologies

Impulse la madurez de su modelo de confianza cero.

Dell tiene soluciones para ayudarle, independientemente de dónde se encuentre en su viaje.

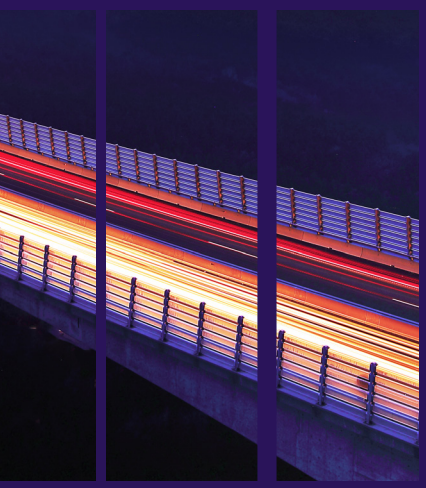
Dell Technologies ofrece opciones y flexibilidad a su organización. Si desea potenciar la madurez de su ciberseguridad, podemos proporcionarle soluciones de seguridad con capacidades de confianza cero para mejorar su capacidad de reforzar, detectar, defenderse y recuperarse ante ciberamenazas maliciosas.

Active los principios de confianza cero.

Habilite opciones y flexibilidad para mejorar la madurez en ciberseguridad.

Dell Technologies le ofrece soluciones de seguridad con capacidades de confianza cero para mejorar su capacidad de reforzar, detectar, defenderse y recuperarse ante ciberamenazas maliciosas. Así es cómo lo hacemos:

- Protecciones integradas que mejoran la automatización, la inteligencia contra amenazas, la autenticación y la visibilidad, entre otras.
- Servicios para desarrollar un roadmap, integrar tecnologías clave y llevar a cabo una gestión proactiva para respaldar la confianza cero.
- Servicios de asesoramiento profesional, gestionado y de seguridad
- Amplio ecosistema de socios



Adopción extremadamente sencilla de la confianza cero

Todo en uno con una arquitectura completamente integrada.

Porque la confianza cero es un enfoque arquitectónico para la seguridad, no es un solo producto y requiere una armonización de las soluciones planificada cuidadosamente. Dell elimina la carga de integración de la confianza cero. A continuación, le explicamos cómo:

- Dell está creando la primera y única arquitectura de confianza cero completamente integrada, diseñada, probada y validada por el Departamento de Defensa de los Estados Unidos

DELL Technologies

Active los principios de confianza cero.

Logre la confianza cero de un modo que se integre en su ecosistema de seguridad concreto.

Dell ayuda a avanzar en la madurez de la ciberseguridad con el fin de respaldar las estrategias de confianza cero, lo que ayuda a reducir la superficie de ataque, mejorar la detección y acelerar la recuperación frente a ciberamenazas.

Dentro de cada uno de los pilares de confianza cero contamos con tecnologías, procesos y personas alineadas con áreas críticas en las que se necesitan políticas empresariales y de seguridad para proteger su organización. Los servicios de seguridad de Dell puede ayudarle con lo siguiente:

- Madurez de seguridad, confianza cero y evaluaciones del riesgo
- Desarrollo de estrategias y roadmaps
- Servicios gestionados de las capacidades clave de la confianza cero

DELL Technologies

Principios del modelo de confianza cero

Ofrecemos soluciones de seguridad integradas y avanzadas que suponen una ventaja en su trayectoria hacia la confianza cero.

Dell Data Protection

Vault de Cyber Recovery | PowerProtect Data Manager | CyberSense Transparent Snapshots | CloudIQ | Bloqueo del sistema | Detección de desviaciones | Gestión segura de claves empresariales | TLS 1.3 | IPv6 | Autenticación de varias fases | Inicio de sesión único | Acceso basado en funciones | CloudIQ

Servidores Dell PowerEdge

Lista de materiales de software | Verificación de componentes seguros | Raíz de confianza en chip | Bloqueo del sistema | Detección de desviaciones | Gestión segura de claves empresariales | TLS 1.3 | IPv6 | Autenticación multifactor | Inicio de sesión único | Acceso basado en funciones | CloudIQ

Plataformas de almacenamiento Dell

Aislamiento de datos | Inmutabilidad de datos | Detección de amenazas | Autenticación del control de acceso | Cifrado de datos | Refuerzo de STIG | Raíz de confianza de hardware | Arranque seguro | Firmware firmado digitalmente | Acceso basado en funciones | Instantáneas seguras

HCI y CI de Dell

Raíz de confianza de hardware | Cadena de confianza de arranque seguro | Actualizaciones firmadas digitalmente | Gestión de claves | Registro seguro | Switches virtuales distribuidos | Aislamiento de MV | Autenticación y autorización | Conectores del ecosistema | Estados validados constantemente | Integridad de los códigos de software | Matriz de compatibilidad electrónica

PC comerciales Dell

Seguridad del BIOS/firmware | Seguridad del hardware | Cadena de suministro fiable | Software de gestión de amenazas (EDR, XDR, VDR) | Software de protección de datos en la red y la cloud

Soluciones Dell para el perímetro

Atestación de HW/SW/MV | Incorporación segura | Cadena de confianza | Entrega segura de aplicaciones y SO | Gestión de derechos de datos

Switches de Dell Networking

SmartFabric | CloudIQ | SD-WAN | Segmentación VLAN | Enterprise SONiC | Listas de control de acceso | RADIUS | TACACS+ | Criptografía | Refuerzo de switches | Microsegmentación | Enrutado y reenvío virtuales

DELL Technologies

Nuestro enfoque acelerado.

El rápido y minucioso Project Fort Zero integra la confianza cero en toda su organización de forma global.

Project Fort Zero ofrece un método validado para la madurez avanzada inmediata en la confianza cero, lo que reduce las interrupciones y los costes de gestión.

El Departamento de Defensa de Estados Unidos, por nuestra experiencia y alcance dentro del sector, solicitó a Dell Technologies que les ayudara a acelerar el ritmo de adopción de la confianza cero. Para que las organizaciones del sector público y privado simplifiquen la adopción e impulsen la arquitectura de confianza cero de forma global, Dell está creando un ecosistema y liderando la integración de más de 30 empresas líderes en tecnología y seguridad. Estamos liderando el desarrollo y la ampliación global de la arquitectura de confianza cero para organizaciones privadas y públicas de todo el mundo. Esta es una prueba del compromiso de Dell con los objetivos del Departamento de Defensa de Estados Unidos para lograr la confianza cero.

En las instalaciones

En los centros de datos para organizaciones en las que el cumplimiento normativo y la seguridad de los datos son cruciales.

Remoto o regional

En ubicaciones, como puntos de venta, donde el análisis seguro y en tiempo real de los datos de los clientes puede ofrecer una ventaja competitiva.

El perímetro desmontable

En lugares como aviones o vehículos con conectividad intermitente en los que se necesita una implementación temporal para la continuidad operativa.

DELL Technologies

Le ayudaremos a acelerar la adopción de la confianza cero implementando las **152** actividades puestas en marcha por el Departamento de Defensa de Estados Unidos para lograr un nivel avanzado de confianza cero.

Facilitadores de la ejecución

Doctrina | Organización | Formación | Material | Liderazgo y formación | Personal | Instalaciones | Política

Nivel de destino de confianza cero

Confianza en los usuarios

- Inventario de usuarios
- Permiso basado en aplicaciones
- Acceso dinámico basado en reglas (parte 1)
- MFA/IDP organizacional
- Implementar el sistema y mitigar los usuarios con privilegios (parte 1)
- Gestión del ciclo de vida de la identidad de la organización
- Denegar usuario por la política predeterminada
- Autenticación única
- Implementar el sistema y mitigar los usuarios con privilegios (parte 2)
- Gestión del ciclo de vida de la identidad de la organización (parte 1)
- Implementar herramientas UEBA
- Autenticación periódica
- PKI/IDP empresarial (parte 1)

Confianza en los dispositivos

- Análisis de las brechas de la herramienta de ayuda de dispositivos
- Integrar herramientas de NextGen AV con C2C
- Dispositivo NPE/PKI bajo gestión
- Denegar dispositivo por la política predeterminada
- Implementar UEDM o herramientas equivalentes
- Gestión de dispositivos empresariales (parte 1)
- Implementar herramientas EDR e integrar con C2C
- Implementar herramientas de gestión de parches, vulnerabilidades y activos
- IDP empresarial (parte 1)
- Implementar C2C/ autorización de red basada en el cumplimiento normativo (parte 1)
- Implementar herramientas FIM y control de aplicaciones
- Soporte de IoT y BYOD limitado y gestionado
- Gestión de dispositivos empresariales (parte 2)
- Implementar herramientas XDR e integrar con C2C (parte 1)

Aplicación y carga de trabajo

- Identificación de códigos/aplicaciones
- Autorización de recursos (parte 1)
- Crear una fábrica de software de DevSecOps (parte 1)
- Código/binarios aprobados
- Programa de gestión de vulnerabilidades (parte 1)
- Autorización de recursos del SDC (parte 1)
- Autorización de recursos (parte 2)
- Crear una fábrica de software de DevSecOps (parte 2)
- Automatizar la corrección de códigos y la seguridad de aplicaciones (parte 1)
- Programa de gestión de vulnerabilidades (parte 2)
- Validación continua
- Autorización de recursos del SDC (parte 2)

Confianza en los datos

- Análisis de datos
- Análisis y registro de puntos de aplicación del DLP
- Análisis y registro de puntos de aplicación del DRM
- Definir los estándares de etiquetado de datos
- Implementar herramientas de clasificación y etiquetado de datos
- Supervisión de la actividad de archivos (parte 1)
- Implementar DRM y herramientas de protección (parte 1)
- Puntos de aplicación de implementación
- Estándares de interoperabilidad
- Desarrollar una política de SDS
- Etiquetado manual de datos (parte 1)
- Supervisión de la actividad de archivos (parte 2)
- Implementar DRM y herramientas de protección (parte 2)
- Aplicación de DLP mediante análisis y etiquetas de datos (parte 1)
- Integrar el acceso DAAS con la política SDS (parte 1)
- Aplicación de DRM mediante análisis y etiquetas de datos (parte 1)
- Integrar la política y las soluciones SDS con IDP empresarial (parte 1)

Red y entorno

- Definir las políticas y reglas de acceso de control granular (parte 1)
- Definir las API de SDN
- Definir las políticas y reglas de acceso de control granular (parte 2)
- Implementar la infraestructura programable de SDN
- Macrosegmentación del centro de datos
- Implementar la microsegmentación
- Segmentar flujos en planos de datos y gestión de control
- Macrosegmentación de B/C/P/S
- Microsegmentación de dispositivos y aplicaciones
- Protección de datos en tránsito

Automatización y coordinación

- Desarrollo e inventario de políticas
- Análisis de automatización de tareas
- Análisis de automatización de respuestas
- Análisis del cumplimiento normativo de las herramientas
- Perfil de acceso de la organización
- Implementar herramientas SOAR
- Esquemas y llamadas estandarizadas de la API (parte 1)
- Enriquecimiento del flujo de trabajo (parte 1)
- Perfil de seguridad empresarial (parte 1)
- Aprovisionamiento de flujo de trabajo e integración empresarial (parte 1)
- Implementar herramientas de ML de clasificación y etiquetado de datos
- Esquemas y llamadas estandarizadas de la API (parte 2)
- Enriquecimiento del flujo de trabajo (parte 2)

Visibilidad y análisis

- Aumentar consideraciones
- Disección de registros
- Correlación de alertas e identificación de activos
- Alerta sobre amenazas (parte 1)
- Implementar herramientas de análisis
- Programa cibernético Threat Intelligence (parte 1)
- Análisis de registros
- Alerta sobre amenazas (parte 2)
- Referencias de dispositivo/usuario
- Establecer comportamiento de referencia del usuario
- Creación de perfiles y referencia (parte 1)
- Programa de inteligencia frente a ciberamenazas (parte 2)

Total de actividades objetivo: 91

Fuente: Publicación sobre la estrategia de confianza cero del Departamento de Defensa, 7 de noviembre de 2022

DELL Technologies

Confianza cero avanzada

Confianza en los usuarios	Confianza en los dispositivos	Aplicación y carga de trabajo	Confianza en los datos	Red y entorno	Automatización y coordinación	Visibilidad y análisis
Acceso dinámico basado en reglas (parte 2)	IDP empresarial (parte 2)	Enriquecer atributos para la autorización de recursos (parte 1)	Etiquetado manual de datos (parte 2)	Optimización y detección de recursos de red	Perfil de seguridad empresarial (parte 2)	Alerta sobre amenazas (parte 3)
Permisos y roles empresariales (parte 1)	Implementar C2C/ autorización de red basada en el cumplimiento normativo (parte 2)	Enriquecer atributos para la autorización de recursos (parte 2)	Supervisión de la actividad de las bases de datos	Decisiones de acceso en tiempo real	Aprovisionamiento de flujo de trabajo e integración empresarial (parte 2)	Creación de perfiles y referencia (parte 2)
MFA flexible alternativa (parte 1)	Supervisión de la actividad de entidades (parte 1)	Autorización para operar (ATO) continua (parte 1)	Soporte y etiquetado automatizado de datos (parte 1)	Microsegmentación del proceso	Implementar la herramienta de automatización con IA	Soporte de referencia UEBA (parte 1)
Análisis JIT/JEA y aprobaciones en tiempo real (parte 1)	Integrar por completo la seguridad de los dispositivos con C2C	Automatizar la corrección de códigos y la seguridad de aplicaciones (parte 2)	Aplicación de DRM mediante análisis y etiquetas de datos (parte 2)		Enriquecimiento del flujo de trabajo (parte 3)	Soporte de referencia UEBA (parte 2)
Gestión del ciclo de vida de la identidad de la organización (parte 2)	PKI empresarial (parte 1)	Microsegmentos de API REST	Aplicación de DLP mediante análisis y etiquetas de datos (parte 2)		IA impulsada por análisis decide las modificaciones de automatización y orquestación	Acceso a la red habilitado por la IA
Supervisión de la actividad de usuarios (parte 1)	Soporte de IoT y BYOD completo y gestionado (parte1)	Autorización para operar (ATO) continua (parte 2)	Integrar el acceso DAAS con la política SDS (parte 2)		Implementar guías	Control de acceso dinámico habilitado por la IA
Autenticación continua (parte 1)	Implementar herramientas XDR e integrar con C2C (parte 2)		Integrar la política y las soluciones SDS con IDP empresarial (parte 2)		Flujos de trabajo automatizados	
Autenticación continua (parte 2)	Supervisión de la actividad de entidades (parte 2)		Integrar la herramienta SOS e integrar con la herramienta DRM (parte 1)			
PKI/IDP empresarial (parte 3)	PKI empresarial (parte 2)		Soporte y etiquetado automatizado de datos (parte 2)			
Permisos y roles de empresarios (parte 2)	Soporte de IoT y BYOD completo y gestionado (parte 2)		Monitorización integral de la actividad de los datos			
MFA flexible alternativa (parte 2)			Aplicación de DRM mediante análisis y etiquetas de datos (parte 3)			
Análisis JIT/JEA y aprobaciones en tiempo real (parte 2)			Aplicación de DLP mediante análisis y etiquetas de datos (parte 3)			
Gestión del ciclo de vida de la identidad de la organización (parte 3)			Integrar el acceso DAAS con la política SDS (parte 3)			
Supervisión de la actividad de usuarios (parte 2)			Integrar la herramienta SDS e integrar con la herramienta DRM (parte 2)			
PKI/IDP empresarial (parte 2)						

Total de actividades avanzadas: 61

Dell Technologies puede simplificar la complejidad de lograr la madurez de la confianza cero rápidamente.

Fuente: Publicación sobre la estrategia de confianza cero del Departamento de Defensa, 7 de noviembre de 2022

DELL Technologies

Satisfacer las necesidades de todas las organizaciones

Impulse la madurez de su modelo de confianza cero.

La confianza cero es un marco definido y un conjunto de principios que guían la forma de abordar la seguridad y se puede implementar mediante diversas capacidades. Ya sea que su objetivo sea la confianza cero en su totalidad o que se centre en mejoras específicas que se ajusten a los principios de confianza cero, Dell es un socio de seguridad con experiencia que le ayudará a impulsar su trayectoria hacia la seguridad.

- Químico
- Tecnología informática
- Comunicaciones
- Servicios de emergencias
- Alimentación y agricultura
- Defensa
- Salud pública y servicios de salud
- Fabricación
- Servicios financieros
- Reactores nucleares
- Comercial
- Administración pública
- Energía
- Transporte
- Agua y aguas residuales
- Presas

DELL Technologies

DELL Technologies

Un socio experto en tecnología y seguridad para la trayectoria de su organización hacia la confianza cero.

Mejore la ciberseguridad a largo plazo mediante la implementación de la confianza cero.

Ofertas de servicios de seguridad de Dell:

Evaluación experta de la madurez de la seguridad y el riesgo general.

Desarrollo de un roadmap hacia la confianza cero.

Gestión continua de las actividades de seguridad.

DELL Technologies

Dell.com/SecuritySolutions

Solicite una llamada

Chatear con un asesor de seguridad

Llame al 1-800-433-2393