Dell NativeEdge

Proteja: opere con confianza y seguridad de confianza cero

Índice de Contenido

Seguridad en entornos distribuidos

Para satisfacer las preferencias de los clientes y las dinámicas de mercado en constante cambio, las organizaciones están implementando nuevas aplicaciones, actualizaciones e infraestructura de computación a un volumen y una velocidad inigualables. Esta avalancha de datos, infraestructura y aplicaciones hace que sea cada vez más importante proteger los entornos distribuidos en los que residen estas nuevas tecnologías.

Conforme las empresas amplían sus operaciones, son cada vez más vulnerables a riesgos de seguridad, como la manipulación de dispositivos o el acceso no autorizado. Además, estos sistemas suelen gestionar datos personales confidenciales, lo que aumenta la responsabilidad de las empresas para proteger a sus clientes.

Para garantizar el funcionamiento de las operaciones, las empresas deben:

Garantizar
la seguridad física de la infraestructura implementada en ubicaciones distribuidas

Detectar
manipulaciones de dispositivos y corregir amenazas

Controlar
el acceso de los usuarios en todos los niveles

Ampliar
el aprovisionamiento y las actualizaciones de software en miles de dispositivos

Dell NativeEdge

Innove dondequiera que opere

Una solución de pila completa de extremo a extremo que centraliza de forma segura la implementación, la coordinación y la gestión del ciclo de vida de diversas infraestructuras y aplicaciones en el perímetro y en todos los centros de datos distribuidos.

Simplifique, optimice y proteja los entornos perimetrales y de centros de datos distribuidos con funciones como la incorporación sin intervención, la seguridad de la confianza cero y la coordinación avanzada de cargas de trabajo. NativeEdge aprovecha el tiempo de ejecución de un hipervisor y contenedor de KVM, lo que permite a las organizaciones implementar y gestionar tanto máquinas virtuales como contenedores. Se ha optimizado para coordinar cargas de trabajo e infraestructuras de IA, lo que permite una implementación y una gestión fluidas de aplicaciones basadas en IA en el perímetro y en todos los centros de datos distribuidos. NativeEdge también se puede adaptar a cualquier entorno de hardware, ya que admite una amplia gama de opciones en diversos factores de forma, desde servidores Dell PowerEdge hasta equipos de sobremesa e infraestructuras de terceros.

Dell NativeEdge se ha diseñado específicamente para abordar los exclusivos retos de los entornos distribuidos, como la complejidad operativa, la capacidad de ampliación y la seguridad. Se trata de una solución adaptada a las organizaciones modernas aprovechar el potencial de la computación en el perímetro, a la vez que reduce los costes y mejora la eficiencia.

Simplificación
Acelere los resultados y centralice las operaciones

Menos de
1 minuto
para implementar infraestructura y aplicaciones[1]

Optimización
Logre una virtualización fluida y una IA ampliable

Hasta un
68 %
de ahorro de tiempo al automatizar la coordinación de aplicaciones perimetrales[1]

Proteger
Opere con confianza y seguridad de confianza cero

Permita las operaciones perimetrales
más seguras
del mundo[2]

[1] Validación técnica de Enterprise Strategy Group por TechTarget encargada por Dell Technologies, "Dell NativeEdge - Plataforma de software de operaciones perimetrales", febrero de 2025.

[2] Datos basados en análisis internos de Dell Technologies, mayo de 2025.

Dell.com/NativeEdge

Proteja sus operaciones distribuidas en expansión reforzando de forma persistente y automática la seguridad de la infraestructura, las aplicaciones, los datos, la red y los usuarios sin ninguna intervención de TI.

Dell NativeEdge protege las operaciones distribuidas mediante:

Refuerzo de la seguridad basada en la confianza cero

Las empresas modernas son responsables de gestionar miles de aplicaciones en sitios distribuidos geográficamente y, a menudo, dependen de una combinación heterogénea de infraestructura. Esto crea una red compleja de silos tecnológicos ineficiente de gestionar, difícil de proteger y lenta de actualizar. A medida que las organizaciones continúan implementando nuevas aplicaciones, nuevos sensores y nuevos dispositivos en ubicaciones distribuidas, la superficie de ataque para posibles ciberamenazas crece.

¿Cómo pueden las empresas garantizar la seguridad continua de las operaciones de datos distribuidos?

Dell NativeEdge permite operar con tranquilidad sobre una base de seguridad de confianza cero. Desde el momento en que se enciende un dispositivo, se establece una cadena de confianza basada en hardware, que utiliza funciones como UEFI Secure Boot y un módulo de plataforma de confianza virtual (vTPM) para garantizar la integridad del dispositivo. Con compatibilidad incorporada para el RGPD y otras normativas internacionales de soberanía de los datos, NativeEdge brinda tranquilidad a los entornos distribuidos. Este enfoque, combinado con capacidades como la microsegmentación de confianza cero, protege sus aplicaciones y datos para que pueda innovar de forma segura dondequiera que opere.

Seguridad basada en la confianza cero

- Confianza en los dispositivos
- Confianza en los usuarios
- Confianza en el transporte y la sesión
- Confianza en los datos
- Confianza en el software
- Visibilidad y análisis
- Automatización y coordinación

El estado de seguridad se refuerza aún más mediante la supervisión y la comprensión de todas las acciones de sus recursos, gracias a los controles empresariales relevantes, un plano de control centralizado y una infraestructura que actúa explícitamente en su beneficio. Gracias a los principios de diseño de confianza cero de NativeEdge, las empresas pueden estar seguras de que, a medida que se amplían las operaciones distribuidas, la integridad de cada recurso conectado se certifica y valida de forma continua.

Cómo garantizar la integridad del hardware a lo largo de la cadena de suministro y su ciclo de vida

Si observamos los ejemplos de un minorista o un fabricante con tiendas o fábricas ubicadas en todo el mundo, resulta cada vez más difícil gestionar y proteger la variedad de hardware con especificaciones y perfiles diferentes en función de la ubicación. Con el tiempo, estos dispositivos no se validan de forma continua, y el cumplimiento no puede verificarse a lo largo de periodos prolongados. Este riesgo aumenta exponencialmente cuando participan varias partes en la instalación de estos dispositivos.

¿Cómo puede proteger de forma uniforme la infraestructura distribuida?

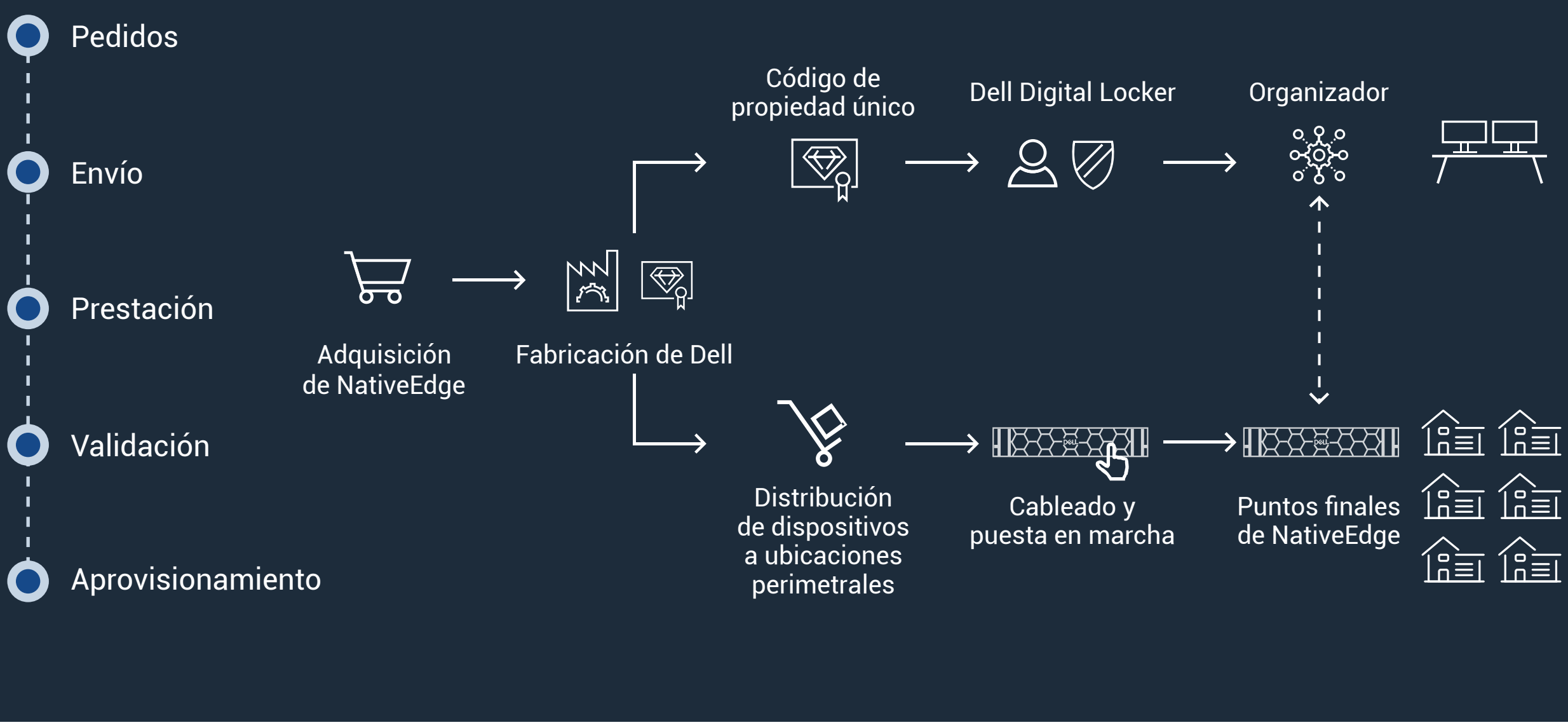
La protección de su infraestructura comienza en nuestra fábrica. Los puntos finales NativeEdge se protegen con seguridad criptográfica y verificación de componentes seguros (SCV) para garantizar la autenticidad. Esto permite un proceso de implementación seguro y sin intervención mediante la incorporación de dispositivos FIDO (FDO). Cuando un dispositivo se enciende en cualquier ubicación, su integridad se valida automáticamente, lo que establece una cadena de custodia segura sin intervención manual. Esto le permite ampliar sus operaciones con la garantía de que su infraestructura está asegurada desde el primer día.

Los puntos finales NativeEdge están optimizados para ser compatibles con NativeEdge y están protegidos con seguridad criptográfica desde la fábrica de Dell.

NativeEdge aprovecha el proceso de verificación de componentes seguros (SCV) para garantizar la autenticidad e integridad de los componentes de hardware. Mediante la SCV, NativeEdge aplica la integridad de la cadena de suministro, la verificación de componentes, la validación de firmware, los procesos de arranque seguro y las firmas criptográficas para protegerse de manipulaciones o accesos no autorizados.

A medida que estos dispositivos pasan por el proceso de incorporación de dispositivos basada en FIDO, su integridad se certifica automáticamente, lo que garantiza la seguridad desde el momento de fabricación en las instalaciones de Dell hasta la recepción e instalación en el lugar de implementación. Si el hardware sufre algún tipo de manipulación, la plataforma lo aísla automáticamente, lo que protege las operaciones frente a elementos maliciosos.

Dispositivo de seguridad incorporado e infraestructura de confianza cero

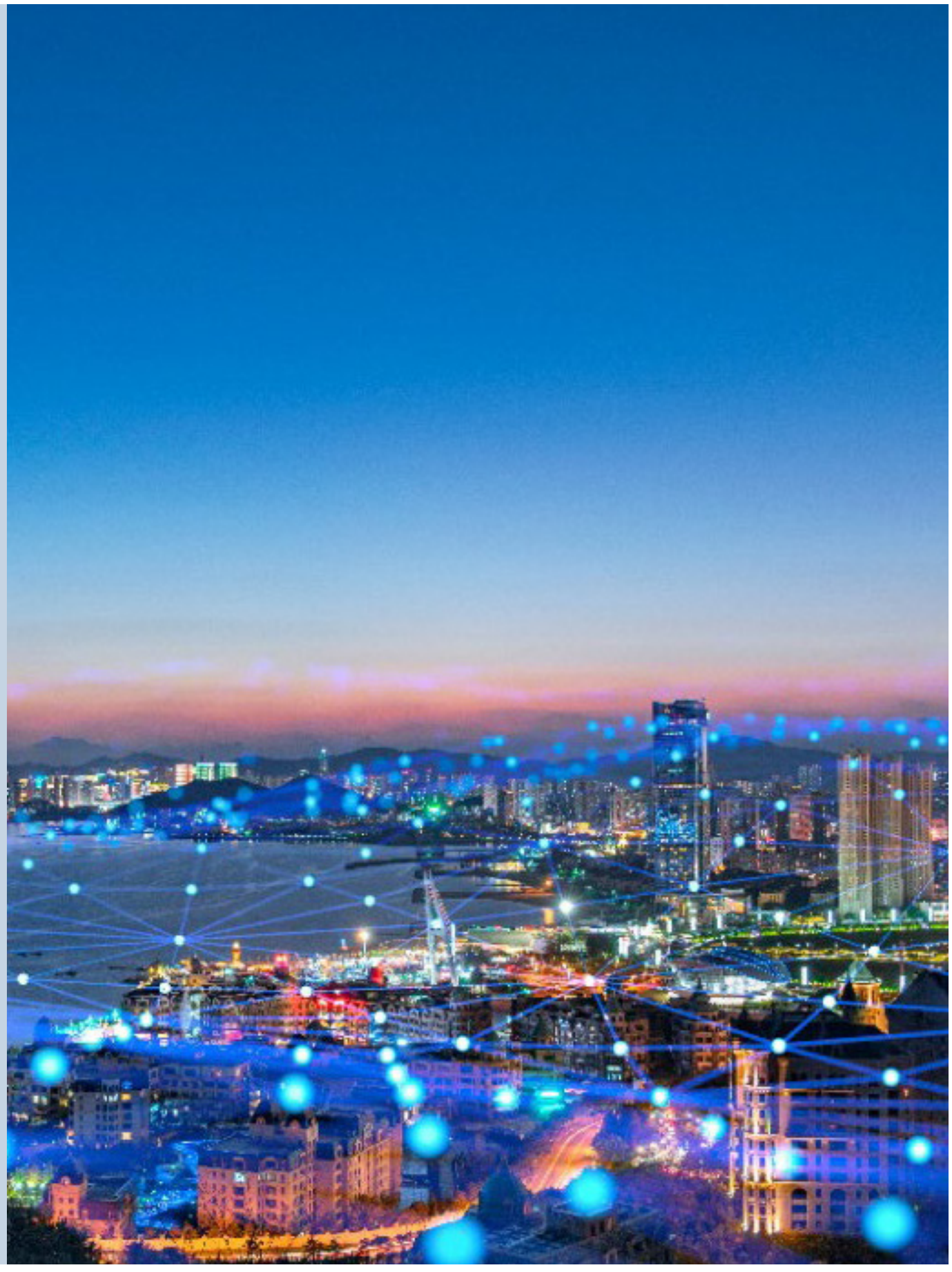


Refuerzo de los datos y las aplicaciones, del perímetro a la cloud

Considere el ejemplo de un minorista global. La naturaleza diversa y distribuida de los entornos minoristas implica que las identidades de los usuarios que acceden a aplicaciones y cargas de trabajo podrían no verificarse de forma rutinaria. Si se verifican, suele ser de manera local en ese entorno y sin visibilidad ni auditoría centralizadas.

Además, los minoristas rara vez tienen visibilidad de la cadena de suministro de software de las aplicaciones implementadas. A menudo esto queda en manos de proveedores de servicios gestionados (MSP), y puede que no existan comprobaciones automatizadas visibles que garanticen la integridad y confiabilidad de estas aplicaciones. Estas aplicaciones las suelen configurar inicialmente los mismos MSP, con la posibilidad de que la configuración se modifique con el tiempo. Por tanto, los interesados no pueden determinar si las aplicaciones cumplen con las políticas de seguridad.

En el caso de los fabricantes, el equipo de tecnología de operaciones (TO) gestiona generalmente un conjunto diverso de cargas de trabajo de aplicaciones. Algunas de estas aplicaciones interactúan con equipos como PLC y son aplicaciones patentadas sin visibilidad interna.



Las capacidades de la red de TI no se extienden a la red de TO, que está lógicamente separada. ¿Cuál es el resultado? Las cargas de trabajo de infraestructura y aplicaciones dentro de las redes de TO de los fabricantes no tienen acceso al nivel de controles de seguridad de red necesario para garantizar un entorno de TO seguro. Retos similares relacionados con la seguridad de las aplicaciones y los datos son comunes en todos los sectores.

Dell NativeEdge ayuda a las organizaciones a proteger el pipeline de datos desde los orígenes de datos hasta las aplicaciones que se ejecutan de forma local o en la cloud. Combina medidas de seguridad avanzadas, como el cifrado, el control de acceso de usuarios, el catálogo de programas de aplicaciones, la segmentación de la red y la coordinación de la seguridad. NativeEdge también utiliza telemetría y análisis para evaluar de forma proactiva el estado de seguridad de sus ubicaciones distribuidas sin depender de expertos con capacidades de auditoría que visiten cada sitio.

Medidas de seguridad avanzadas

Las medidas de seguridad avanzadas garantizan la resiliencia de las operaciones

Control de acceso de los usuarios

NativeEdge proporciona control de acceso basado en funciones (RBAC) para analizar los niveles de acceso según las funciones y las responsabilidades de un usuario. Los usuarios de los dispositivos y las cargas de trabajo de las aplicaciones implementadas se verifican en cada sesión de acceso y se certifican de forma centralizada y visible a través de la gestión de acceso e identidades.

Segmentación de la red

La microsegmentación de la red para las aplicaciones facilita el desarrollo y la gestión de políticas dirigidas a que estas aplicaciones sean más seguras. Este enfoque mitiga los riesgos de posibles vulneraciones y el movimiento lateral de amenazas dentro de entornos virtualizados.

Catálogo de programas de aplicaciones

NativeEdge está diseñado para hacer que las aplicaciones sean más seguras. Comienza con una cadena de suministro de software segura que se basa en un Catálogo para desplegar sus aplicaciones mediante plantillas. El Catálogo es una colección de programas para implementar aplicaciones de proveedores de software independientes (ISV) o programas prevalidados de Dell desarrollados por empresas, todo ello a fin de mantener una cadena de suministro de software segura. Estos programas, basados en el estándar TOSCA y el formato YAML, automatizan la implementación de aplicaciones, así como las infraestructuras de IA en muchos dispositivos perimetrales a la vez. NativeEdge le permite establecer controles de seguridad proactivos para las aplicaciones implementadas a un nivel granular y garantiza que sus aplicaciones se implementen de forma uniforme y se alineen con sus políticas de seguridad. Por último, las cargas de trabajo de las aplicaciones se pueden ejecutar en puntos finales NativeEdge o en un entorno multicloud como máquinas virtuales y contenedores, gestionados de forma centralizada por NativeEdge.

Protección y cifrado de los datos

NativeEdge protege sus datos en todo momento y lugar (en reposo, en tránsito y en uso) frente a vulneraciones y accesos no autorizados. NativeEdge proporciona un sólido cifrado de datos en reposo (DARE), que cumple con los estándares federales de cumplimiento normativo, lo que garantiza que los datos almacenados estén cifrados y protegidos frente a robos físicos o manipulaciones. NativeEdge administra cada recurso de datos siguiendo los principios de seguridad de confianza cero, aplicando un estricto control de acceso, así como acreditando y verificando continuamente dicho control. Esto no solo protege la integridad de los datos para las aplicaciones empresariales, sino que también aumenta la confianza de todas las partes interesadas del negocio.

Coordinación de la seguridad

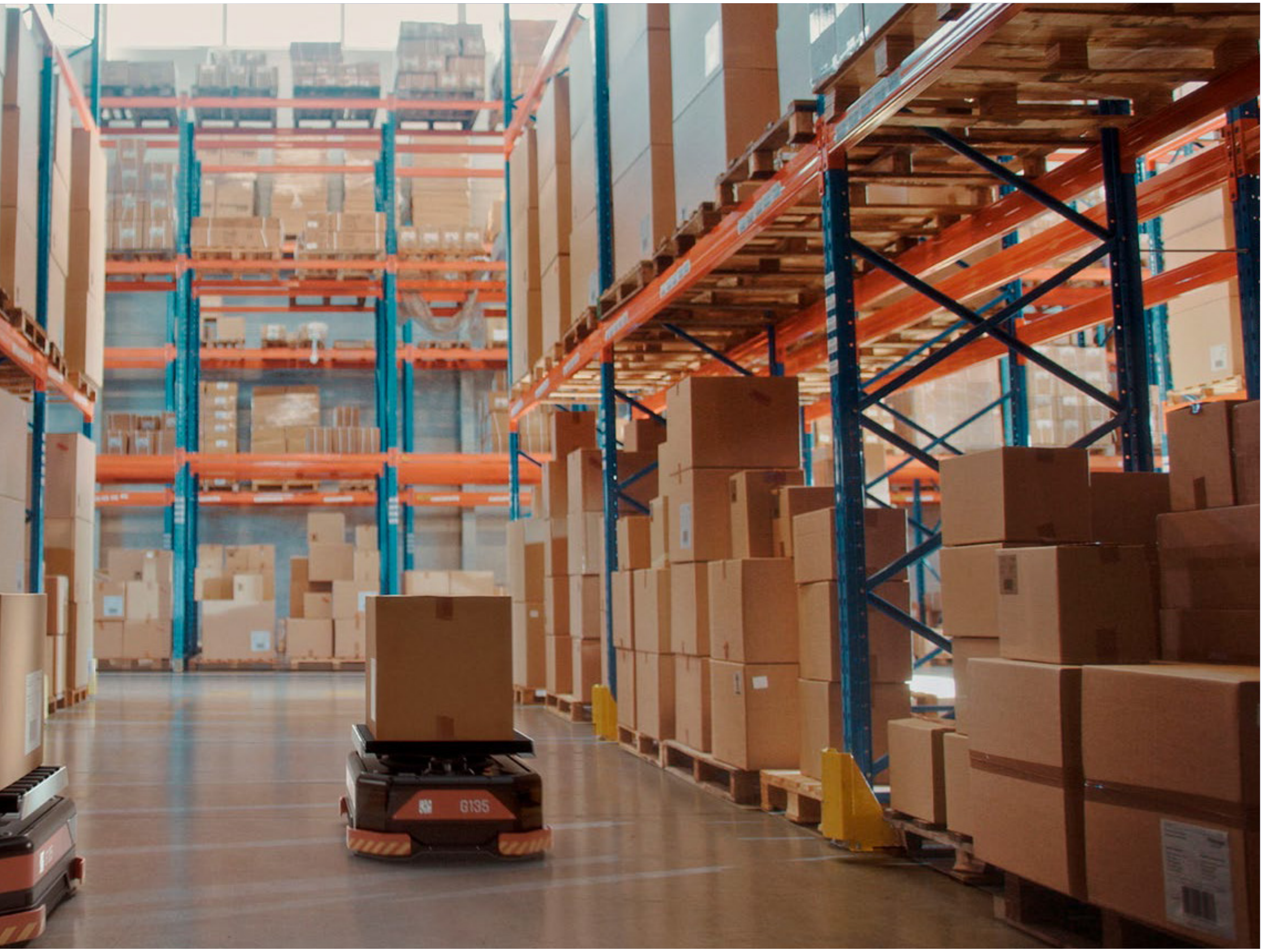
Las acciones o los eventos no autorizados suelen pasar desapercibidos y, a menudo, nunca se solucionan. Esto añade riesgos debido a los procesos manuales y, a menudo, queda en segundo plano frente a tareas empresariales de alta prioridad. Además, existen variaciones en la integración de TI en torno a la gestión de acceso e identidades (IAM), el control de acceso basado en funciones (RBAC) y el plano de control.

Esto da lugar a una coordinación de seguridad desconectada que a menudo se gestiona en cada sitio de forma individual. En muchos casos de TO, estos dispositivos están en un entorno M2M (máquina a máquina), sin reconocimiento de usuarios. La coordinación centralizada es crucial para estos entornos.

NativeEdge garantiza una coordinación de seguridad uniforme en todo el perímetro. En función del conjunto de acciones y eventos que ocurren en el entorno perimetral, proporciona una vista unificada de su estado de seguridad, lo que permite la autenticación centralizada y la aplicación uniforme de políticas en todos los sitios. Utiliza las funciones IAM y RBAC que permiten una gestión segura de la plataforma utilizando el principio de privilegio mínimo, lo que proporciona la granularidad que las empresas necesitan. NativeEdge también simplifica el cumplimiento de regulaciones como RGPD, PCI y HIPAA mediante la automatización del registro y la gestión de configuraciones, ayudándole a operar con confianza en cualquier entorno y a incorporar reglas de gobernanza, riesgo y cumplimiento normativo (GRC) y operaciones de seguridad (SecOps).

Telemetría y análisis

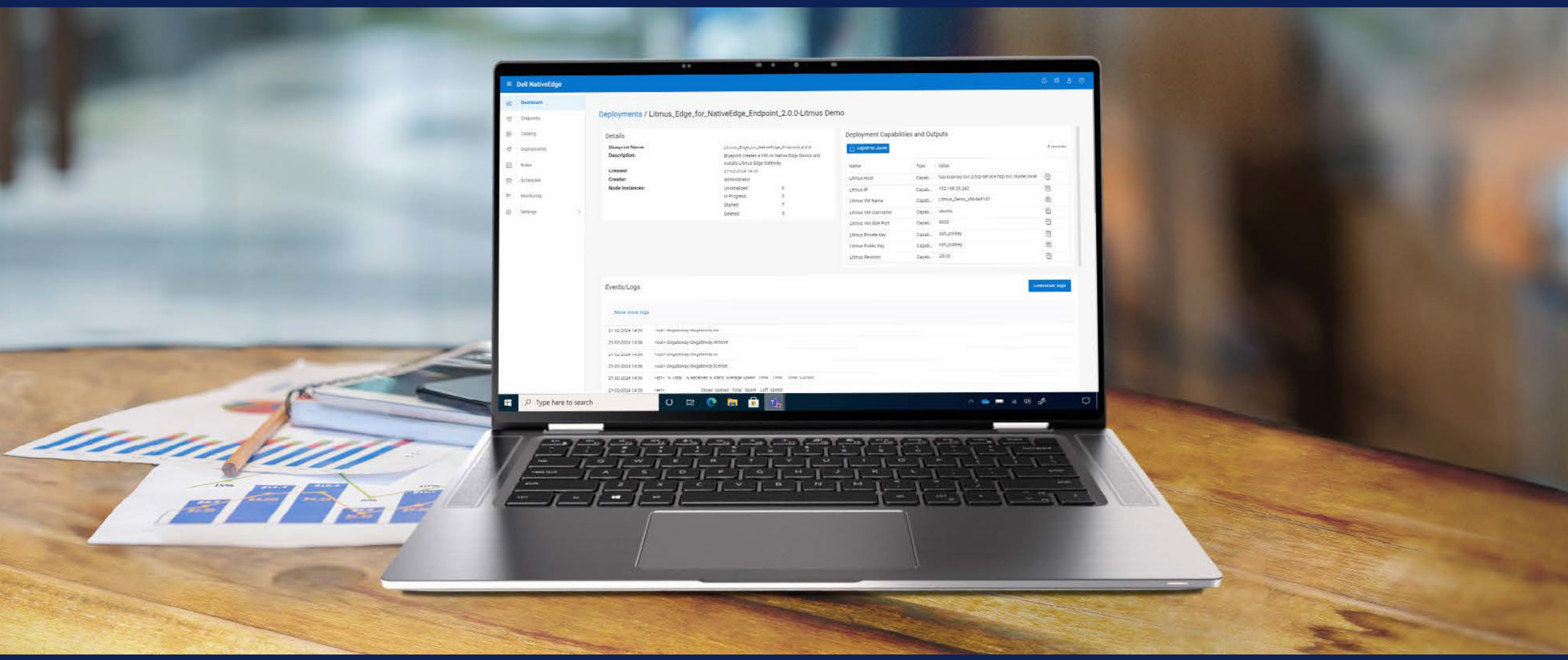
NativeEdge realiza evaluaciones de seguridad de forma continua según los estándares de cumplimiento definidos, basándose en la telemetría del hardware y el entorno operativo. Se utilizan para determinar la detección de desviaciones en la configuración, configuraciones incorrectas y la necesidad de actualizaciones de seguridad.



Proteja su área de perímetro

Dell NativeEdge protege su entorno perimetral con principios de seguridad de confianza cero, incluida la incorporación segura de dispositivos basada en FIDO, junto con un sistema operativo NativeEdge reforzado y seguro. Con Dell NativeEdge, puede estar seguro de que la infraestructura, los usuarios, la red, las aplicaciones y los datos se certifican y validan de forma continua en toda las ubicaciones distribuidas.

Innove dondequiera que opere



DELL Technologies

Más información en **Dell.com/NativeEdge**