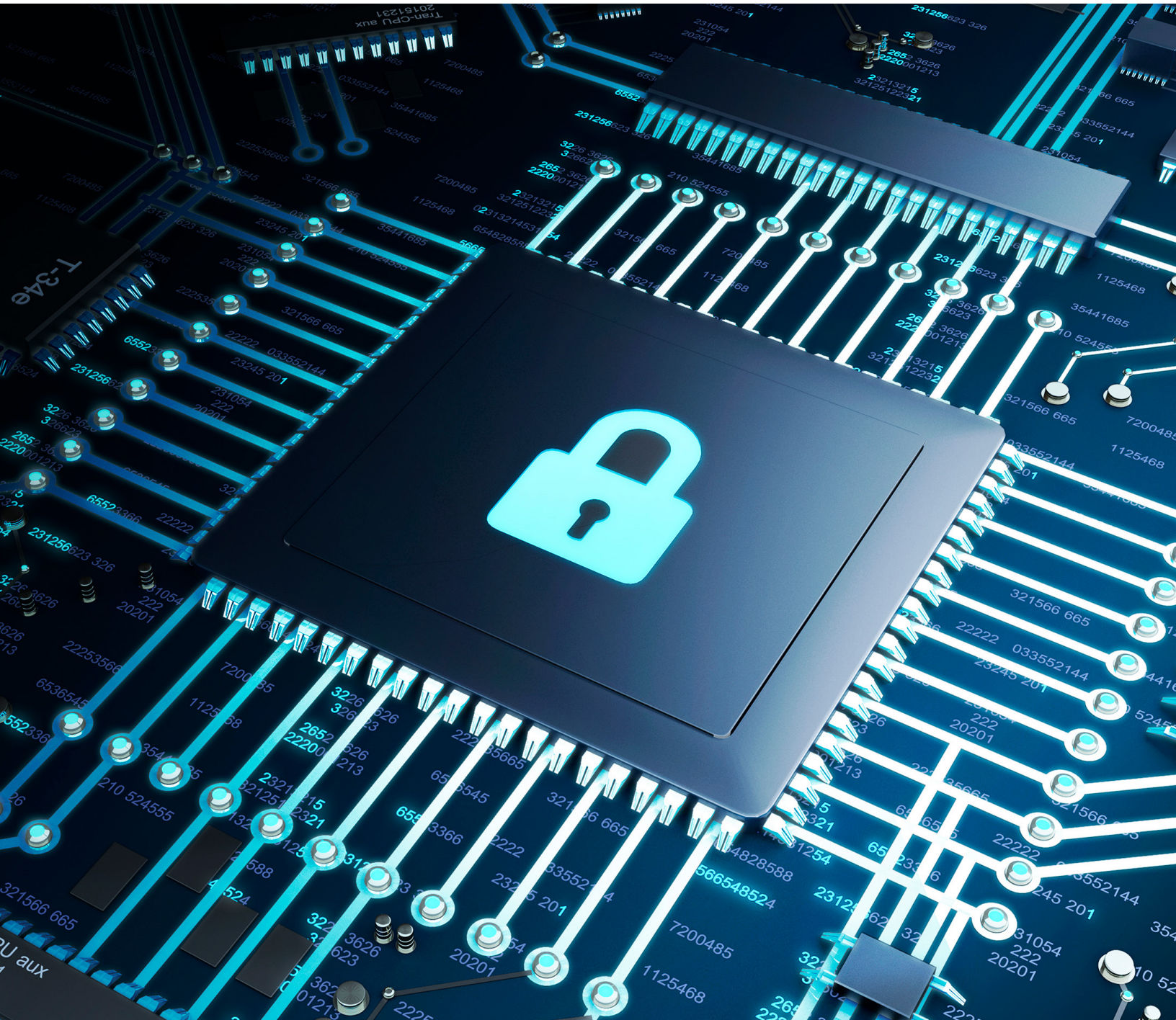
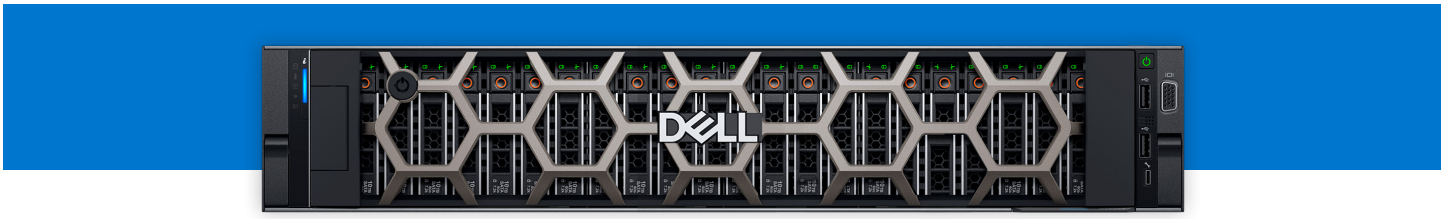
DELL Technologies

Microsoft

Documento técnico

Mejore la seguridad de los datos de forma integral con Microsoft SQL Server, los servidores Dell™ PowerEdge™ y Windows Server 2022





Con el gran cambio provocado por el teletrabajo en muchos sectores, las empresas se están adaptando a esta nueva normalidad y haciendo que la seguridad sea más prioritaria que nunca. En 2021, la mayoría de los líderes empresariales afirmaron que el teletrabajo continuaría en el futuro cercano.[1] Y con un mayor número de empleados repartidos por más áreas geográficas que nunca y con múltiples puntos finales vulnerables, los administradores de TI de las empresas deben adoptar un enfoque más integral de la seguridad.

El 88 % de los líderes de TI encuestados esperan que el teletrabajo continúe en alguna de sus formas, y es probable que el uso de múltiples repositorios de contenido siga siendo un problema a corto plazo.[1]

Los equipos de TI pueden mejorar la seguridad de los datos en toda la empresa adoptando un enfoque de "pila completa" en el centro de datos: desde el hardware, pasando por la aplicación de bases de datos y hasta el sistema operativo. Modernizar la infraestructura y consolidar los datos de la versión más reciente de Microsoft SQL Server en servidores Dell™ PowerEdge™ y Windows Server 2022 ofrece a las empresas una base sólida para proteger sus datos de forma integral en un panorama laboral en continuo cambio.

Retos de seguridad a los que se enfrentan las empresas hoy en día

El auge del teletrabajo ha exacerbado las formas en que las empresas ya eran vulnerables a los ciberataques:

- **Proliferación de contenidos.** La proliferación de contenidos es el resultado natural de que muchos empleados hayan accedido a los datos y aplicaciones empresariales y los hayan usado a lo largo del día durante años. Los datos terminan almacenándose en diferentes ubicaciones y en múltiples repositorios. Y el volumen de estos datos sigue creciendo. IDC estima que los datos seguirán aumentando a una tasa de crecimiento anual compuesto (TCAC) del 24 % en los próximos cinco años.[2] Más de la mitad de los líderes de TI encuestados (52 %) afirma que sus empresas tienen al menos 10 repositorios de almacenamiento de archivos.[1] Al igual que tener muchos objetos en una casa puede generar desorden y se corre el riesgo de perder las cosas, el contenido guardado o duplicado en varios servidores y bases de datos también puede poner en riesgo los datos.

El 41 % de los líderes de TI dicen que su principal preocupación con la proliferación de contenidos es el mayor riesgo de vulneraciones y filtraciones de datos.[1]

- **Programa "traiga su propio dispositivo" (BYOD) y TI oculta.** El aumento de los riesgos de seguridad derivados de la proliferación de contenidos se ve acrecentado por las políticas BYOD, en las que las organizaciones permiten el uso de teléfonos inteligentes y tabletas personales para trabajar. Puede que estos dispositivos no se actualicen regularmente con los parches de seguridad más recientes y que se utilicen en redes Wi-Fi no seguras. La "TI oculta", o la dependencia de las autoproclamadas características de seguridad de las aplicaciones basadas en la cloud, es otro potencial vector de ataque para los piratas informáticos debido a la falta inherente de controles internos y visibilidad.
- **Diferentes programas de aplicación de parches de seguridad.** Muchas organizaciones utilizan SQL Server como plataforma de datos, pero con el tiempo acaban teniendo diferentes versiones del software de la base de datos, lo que complica la administración de los datos y de los parches de seguridad. Dado que la aplicación de parches puede ralentizar los sistemas y requerir un tiempo de inactividad de los servidores, los equipos de TI deben determinar el plazo ideal para aplicar parches a cada versión, lo que puede retrasar las actualizaciones.
- **Diferentes niveles de acceso para los empleados.** Los administradores de TI deben intentar mantener la configuración de permisos cuando se contrata a empleados o estos se van de una organización. Si no se configura correctamente o si no se actualiza de manera oportuna, alguien de la organización puede exponer de manera accidental o intencionada los datos de la empresa y sus clientes a ransomware y piratas informáticos.

Modernice la gestión de datos sobre una base segura

La ejecución de SQL Server en servidores Dell PowerEdge y Windows Server 2022 ayuda a los administradores de TI a superar estos retos y a proteger las cargas de trabajo críticas para la empresa en infraestructuras modernas en los niveles de hardware, sistema operativo (SO) y software.

El 65 % de los directores de TI y otros líderes de TI sospechan que los archivos y documentos con información confidencial se guardan localmente en los dispositivos personales de los empleados.[1]

Servidores Dell PowerEdge

Los servidores Dell PowerEdge ayudan a las empresas a defenderse de los riesgos inherentes al entorno actual con una infraestructura habilitada para la seguridad que admite una amplia gama de cargas de trabajo y objetivos actuales. Los servidores PowerEdge se han diseñado para acelerar la implementación y mejorar el rendimiento de las aplicaciones de bases de datos, la informática de alto rendimiento (HPC), los entornos de virtualización y la computación en el perímetro. Además, las herramientas de Dell™ OpenManage™ ayudan a los administradores de TI a gestionar grandes clústeres con facilidad y eficacia.

Los servidores PowerEdge se fabrican sobre una raíz de confianza inmutable basada en chip de silicio, y ofrecen funciones de seguridad como la verificación de arranque integral, lo que incluye la personalización del arranque seguro de UEFI, el BIOS de confianza, la cadena de confianza del firmware y el cargador de arranque del SO verificado. El firmware está protegido mediante las directrices del Instituto Nacional de Estándares y Tecnología (NIST), que incluyen las actualizaciones de firmware firmadas, y la gestión de certificados se simplifica gracias a la renovación automática.

Los servidores PowerEdge también ofrecen protección de datos en reposo mediante Secure Enterprise Key Manager (SEKM) y la protección de los datos en uso con tecnologías de CPU confidenciales para computación. Para mitigar amenazas como componentes falsificados, malware y manipulación de firmware, Dell emplea un enfoque integral de la seguridad de la cadena de suministro que incluye herramientas para la prevención de la falsificación, una cadena de custodia de fabricación, una firma de códigos y embalajes a prueba de intrusiones en el chasis y manipulaciones. Además, la verificación de componentes seguros (SCV) aumenta la seguridad de la cadena de suministro mediante la verificación de la integridad de los componentes del servidor.

Dell Technologies, uno de los socios más importantes de Microsoft, ha trabajado estrechamente con esta organización durante casi cuatro décadas para desarrollar soluciones de hardware y software basadas en la seguridad que lideran el sector. Gracias a esta colaboración, el software de Microsoft, como Windows Server y SQL Server, se ejecuta de forma óptima en los servidores Dell PowerEdge.

Windows Server 2022

Windows Server 2022 cuenta con un servidor con núcleo protegido basado en Windows que utiliza funcionalidades de hardware, firmware y sistema operativo para protegerse contra las amenazas actuales y futuras. Los servidores con núcleo protegido utilizan la compatibilidad del procesador con la tecnología de raíz de confianza dinámica para mediciones (DRTM) para aislar el firmware, de modo que cualquier vulneración tenga menos posibilidades de afectar al código del firmware. Además, la seguridad basada en virtualización (VBS) aísla las partes críticas del sistema operativo (como el kernel) del resto del sistema para proteger las aplicaciones y los datos, al tiempo que ayuda a garantizar que los servidores permanezcan dedicados a ejecutar las cargas de trabajo críticas.

Esta funcionalidad de núcleo protegido ayuda a defenderse proactivamente y a interrumpir muchas de las rutas que utilizan los atacantes para explotar los sistemas. Varias tecnologías de seguridad de Microsoft son estándar o compatibles con los servidores con núcleo protegido, lo que incluye integridad del código protegida por hipervisor de VBS, Trusted Platform Module (TPM) 2.0, cifrado de unidad BitLocker y arranque seguro de UEFI.

Para obtener más información sobre las funcionalidades de protección avanzadas de Windows Server 2022 en servidores Dell PowerEdge, consulte el documento técnico "Obtenga una protección de seguridad avanzada con las funcionalidades combinadas de Windows Server 2022 y los servidores Dell EMC PowerEdge de última generación".

Proteger los datos en el nivel de la aplicación de bases de datos

SQL Server se ha diseñado pensando en la seguridad. Sin embargo, como se ha mencionado anteriormente, muchas empresas ejecutan varias versiones de SQL Server y los departamentos de TI buscan una estrategia de bases de datos más sencilla y consolidada.

Además, la asistencia extendida de SQL Server 2012 finaliza en julio de 2022, lo que hace que la consolidación de bases de datos en la última versión de SQL Server sea un problema aún más urgente. Si bien las versiones anteriores de la base de datos de SQL Server seguirán funcionando, no habrá una solución del fabricante en caso de problemas. Tampoco se proporcionarán parches ni actualizaciones de seguridad, lo que podría hacer que los sistemas sean vulnerables a los ataques maliciosos.

Para muchas empresas, el camino más sencillo y práctico hacia la consolidación es actualizar a la versión más reciente de SQL Server y ejecutar las versiones anteriores en modo de compatibilidad. De este modo, los administradores de bases de datos pueden realizar una copia de seguridad de una base de datos de SQL Server heredada y, a continuación, cargarla y ejecutarla en SQL Server 2019/2022 en modo de compatibilidad. Este enfoque puede ser una forma rápida y sencilla de actualizar si no es necesario realizar pruebas de regresión completas. SQL Server 2019 (con un nivel de compatibilidad de 150) admite versiones anteriores a SQL Server 2008 R2 (con un nivel de compatibilidad de 100).

Procedimientos recomendados de seguridad

Para proteger aún más los datos, es posible que los equipos de TI quieran asegurarse de que siguen los procedimientos recomendados de seguridad para SQL Server (para obtener más información sobre estos procedimientos recomendados y sobre cómo implementarlos, consulte la entrada del blog de Microsoft, "Protección de SQL Server"). Estas prácticas recomendadas de seguridad se aplican a todos los niveles de la infraestructura del centro de datos, incluidos el hardware y el sistema operativo, e incluyen:

- **Mejore la seguridad física.** La seguridad física limita estrictamente el acceso a los componentes físicos del hardware y del servidor. Esto significa utilizar salas cerradas con acceso restringido para los servidores y dispositivos de red. El acceso a los soportes de copia de seguridad está limitado por el hecho de que se almacenan en una ubicación segura fuera de las instalaciones. Se recomienda adoptar un enfoque por capas: impedir el acceso o solicitar una tarjeta de acceso/aprobación en el perímetro del centro, en el perímetro del edificio, en el interior del edificio y en la planta del centro de datos.
- **Mantenga el sistema operativo actualizado.** Los service packs y las actualizaciones del sistema operativo incluyen importantes mejoras de seguridad. Las actualizaciones y mejoras del sistema operativo se pueden aplicar después de probarlas con aplicaciones de bases de datos.
- **Utilice firewalls.** Los firewalls aumentan la seguridad en el sistema operativo al proporcionar un cuello de botella en el que se pueden centrar las medidas de seguridad.
- **Reduzca la superficie.** Limite las áreas susceptibles a las vulneraciones desactivando o inhabilitando las funciones y los componentes que no se estén utilizando. La superficie de SQL Server se puede reducir mediante la ejecución de los servicios necesarios que tengan "privilegios mínimos" y que concedan derechos a los servicios y usuarios en el nivel adecuado.
- **Implemente el control de acceso basado en funciones (RBAC) en los "elementos susceptibles de protección".**[3] Los elementos que pueden protegerse incluyen componentes como el servidor, la base de datos y los objetos que contiene la base de datos. Estos elementos son los recursos para los que regula el acceso el sistema de autorización del motor de base de datos de SQL Server.
- **Cifre los datos en todos los niveles.** Esto incluye el cifrado de datos de almacenamiento y de aplicaciones.
- **Cree y utilice certificados.** Los certificados son claves de software que permiten que dos servidores se comuniquen de forma segura. En SQL Server, los certificados mejoran la seguridad de los objetos y las conexiones.
- **Restrinja el acceso a los archivos del sistema operativo que SQL Server utiliza.**
- **Utilice contraseñas seguras en toda la organización.** Se trata de una práctica de seguridad sencilla, pero no se le suele dar la prioridad que le corresponde.
- **Realice auditorías.** Asegúrese de que la recuperación después de una copia de seguridad funcione según lo esperado y que el acceso se aplique correctamente.
- **Use Microsoft Defender para las bases de datos de SQL Server.** Las bases de datos de Microsoft Defender para SQL Server examinan las bases de datos en busca de vulnerabilidades. Esto permite detectar anomalías que indican intentos inusuales y potencialmente dañinos de acceder a las bases de datos o explotarlas. Estas anomalías incluyen actividades sospechosas en bases de datos, vulnerabilidades potenciales, ataques de inyección SQL y patrones anómalos de consulta y acceso a la base de datos.

Por último, cada nueva versión de SQL Server incluye nuevas características de seguridad que mejoran la protección de datos. La nueva función de libro mayor, anunciada para SQL Server 2022, ayuda a proteger la integridad de los datos mediante la creación de un registro inmutable de las modificaciones de datos a lo largo del tiempo. Esto puede ayudar a proteger los datos contra la manipulación por parte de actores maliciosos, y supone una ventaja en situaciones como auditorías internas y externas.

Libro mayor de SQL Server

- Utiliza un registro inmutable para proteger los datos frente a manipulaciones de actores maliciosos
- Establece la confianza digital en un sistema centralizado gracias a la tecnología de blockchain
- Permite confirmar a otras partes que la integridad de los datos no se ha vulnerado

Consolide y proteja desde el hardware hasta la base de datos

La importancia de la TI no hará más que crecer junto con el volumen de los datos en las empresas digitales. Y dado que esa gran cantidad de datos va acompañada de ciberataques cada vez más inteligentes y frecuentes, los equipos de TI deben adoptar una estrategia de seguridad de los datos que ayude a proteger la infraestructura en todos los niveles. La actualización a la última versión de SQL Server y el SO Windows Server en servidores Dell PowerEdge puede ayudar a las empresas a proteger los datos confidenciales propios y de sus clientes.

Adopte un enfoque que priorice la seguridad en su infraestructura. Obtenga más información sobre cómo pueden ayudarle las soluciones de Dell y Microsoft: www.dell.com/en-us/dt/solutions/microsoft-data-platform/index.htm.

Consulte "Obtenga una protección de seguridad avanzada con las funcionalidades combinadas de Windows Server 2022 y los servidores Dell EMC PowerEdge de última generación".

[1] Egnyte. "2021 Data Governance Trends: Predictions, pitfalls and technologies for the future of digital work". 2021. www.egnyte.com/sites/default/files/2021-09/2021DataGovernanceTrendsReport.pdf.
[2] IDC. "Data Creation and Replication Will Grow at a Faster Rate than Installed Storage Capacity, According to the IDC Global DataSphere and StorageSphere Forecasts". Marzo de 2021.
[3] Para obtener más información sobre los elementos susceptibles de protección, consulte https://docs.microsoft.com/en-us/sql/relational-databases/security/securables.

DELL Technologies

Microsoft

Modernícese con Windows Server 2022.
El sistema operativo preparado para la cloud que potencia las inversiones en las instalaciones con capacidades híbridas.