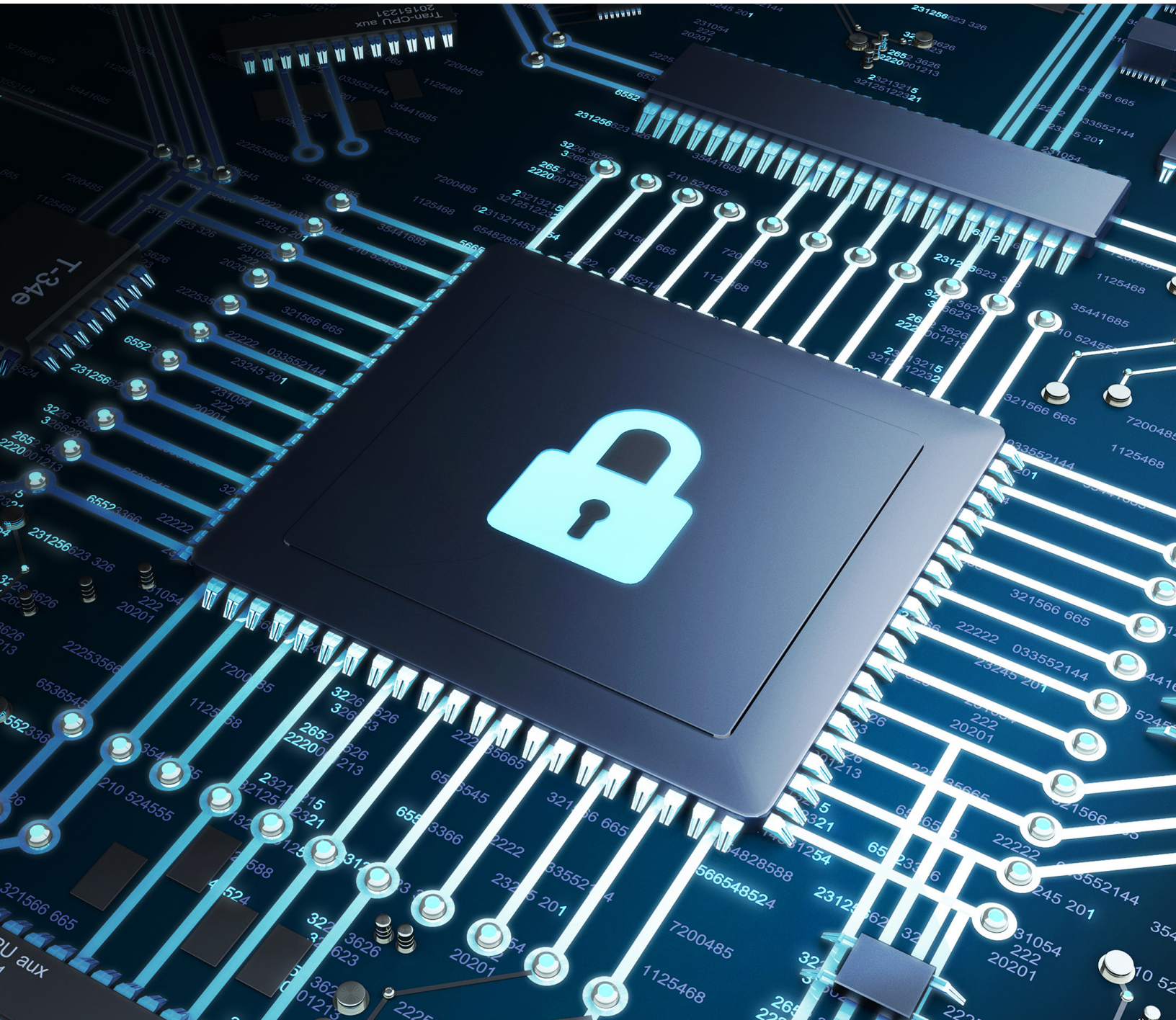
DELL Technologies

Microsoft

Livre blanc

Améliorez la sécurité des données de bout en bout avec Microsoft SQL Server, les serveurs Dell™ PowerEdge™ et Windows Server 2022



La vaste transition vers le télétravail qui s'est opérée dans de nombreux secteurs a amené les sociétés à s'adapter à la nouvelle normalité et à faire de la sécurité leur priorité absolue. En 2021, la plupart des dirigeants d'entreprises affirmaient que le télétravail se poursuivrait dans un futur proche.[1] Par ailleurs, les collaborateurs étant toujours plus dispersés dans le monde, les points de terminaison vulnérables se multiplient, obligeant ainsi les responsables IT au sein des entreprises à adopter une approche plus globale de la sécurité.

88 % des responsables IT interrogés s'attendent à ce que le télétravail continue de s'étendre et à ce que l'utilisation de référentiels de contenu multiples reste un problème à court terme.[1]

Les équipes IT peuvent améliorer la sécurité des données dans toute l'entreprise en adoptant au sein du datacenter une approche « whole stack », allant du matériel à l'application de base de données en passant par le système d'exploitation. La modernisation de l'infrastructure et la consolidation des données sur la dernière version de Microsoft SQL Server sur serveurs Dell™ PowerEdge™ et Windows Server 2022 offrent aux entreprises une base solide de protection des données de bout en bout face à un environnement de travail en constante évolution.

Les défis de sécurité auxquels les entreprises sont aujourd'hui confrontées

L'essor du télétravail a rendu les entreprises encore plus vulnérables aux cyberattaques :

- **Prolifération du contenu.** La prolifération du contenu est la conséquence naturelle de l'accès et de l'utilisation des données et applications d'entreprise par de nombreux collaborateurs tout au long de la journée depuis des années. Les données finissent par être stockées à différents endroits et dans une multitude de référentiels. Dès lors, la quantité de données ne cesse d'augmenter. IDC estime que les données continueront d'augmenter à un taux de croissance annuel composé (TCAC) de 24 % au cours des cinq prochaines années.[2] Plus de la moitié des responsables IT interrogés (52 %) affirment que leur entreprise dispose d'au moins 10 référentiels de mémoire fichier.[1] Tout comme le fait de posséder un grand nombre d'objets peut vite encombrer une maison et augmenter le risque de perte, le contenu enregistré ou dupliqué sur plusieurs serveurs et bases de données peut représenter un danger pour les données.

41 % des responsables IT déclarent que leur principale préoccupation concernant la prolifération du contenu est le risque accru de violations et de fuites de données.[1]

- **BYOD (Bring Your Own Device) et IT fantôme.** Les risques de sécurité accrus liés à la prolifération du contenu sont exacerbés par les politiques de BYOD (Bring Your Own Device) en vertu desquelles les organisations autorisent l'utilisation de smartphones et de tablettes personnels pour le travail. Ces appareils peuvent ne pas être mis à jour régulièrement avec les derniers correctifs de sécurité et être utilisés sur des réseaux Wi-Fi non sécurisés. L'« IT fantôme », c'est-à-dire le recours aux fonctions de sécurité autoproclamées des applications basées sur le Cloud, est un autre vecteur d'attaque potentiel pour les pirates informatiques, du fait du manque inhérent de contrôles internes et de visibilité.
- **Diversité des calendriers d'exécution des correctifs de sécurité.** De nombreuses organisations utilisent SQL Server comme plateforme de données, mais se retrouvent au fil du temps avec différentes versions du logiciel de base de données, ce qui complique la gestion des données et l'application de correctifs de sécurité. L'application de correctifs pouvant par ailleurs ralentir les systèmes et nécessiter des interruptions de service au niveau des serveurs, les équipes IT doivent définir le calendrier idéal selon lequel appliquer les correctifs à chaque version, ce qui peut retarder les mises à jour.
- **Diversité des niveaux d'accès pour les collaborateurs.** Les administrateurs IT doivent s'efforcer de maintenir les paramètres d'autorisation à mesure que des employés sont embauchés ou quittent une organisation. S'ils ne sont pas configurés correctement ou mis à jour en temps opportun, n'importe qui au sein de l'organisation peut accidentellement ou intentionnellement exposer des données de la société et de clients aux rançongiciels et pirates informatiques.

Moderniser la gestion des données sur une base sécurisée

L'exécution de SQL Server sur des serveurs Dell PowerEdge et Windows Server 2022 permet aux administrateurs IT de relever ces défis et de sécuriser les charges applicatives stratégiques sur l'infrastructure moderne au niveau du matériel, du système d'exploitation (OS) et des logiciels.

> 65 % des DSI et autres responsables IT soupçonnent les collaborateurs d'enregistrer en local des fichiers et documents contenant des données sensibles sur leurs appareils personnels.[1]

Serveurs Dell PowerEdge

Les serveurs Dell PowerEdge aident les entreprises à se défendre contre les risques inhérents à l'environnement d'aujourd'hui grâce à une infrastructure sécurisée qui prend en charge un large éventail de charges applicatives et d'objectifs modernes. Les serveurs PowerEdge sont conçus pour accélérer le déploiement et améliorer les performances des applications de base de données, du calcul haute performance (HPC), des environnements de virtualisation et du calcul en périphérie. De plus, les outils Dell™ OpenManage™ aident les administrateurs IT à gérer de vastes clusters aisément et efficacement.

Les serveurs PowerEdge reposent sur une fonctionnalité immuable Silicon Root of Trust et permettent le recours à des fonctions de sécurité telles que la vérification au démarrage de bout en bout, notamment la personnalisation UEFI (Unified Extensible Firmware Interface) Secure Boot, le BIOS fiable, la chaîne d'approbation du firmware et le chargeur de démarrage vérifié du système d'exploitation. Le firmware est protégé conformément aux instructions du NIST (National Institute of Standards and Technology), notamment pour les mises à jour de firmware signés, et la gestion des certificats est simplifiée via un renouvellement automatique.

Les serveurs PowerEdge offrent également une protection des données au repos à l'aide de la solution Secure Enterprise Key Manager (SEKM) et une protection des données en cours d'utilisation avec des technologies de processeurs de calcul confidentielles. Pour atténuer les menaces telles que les contrefaçons de composants, les logiciels malveillants et les altérations du firmware, Dell Technologies adopte une approche globale de la sécurité de la chaîne logistique avec des outils conçus pour éviter les contrefaçons et prévoyant chaîne de responsabilité de la fabrication, signature du code, protection contre les intrusions dans le boîtier et emballage inviolable. De plus, la vérification sécurisée des composants (Secure Component Verification – SCV) étend la sécurité de la chaîne logistique en vérifiant l'intégrité des composants du serveur.

L'un des principaux partenaires de Microsoft, Dell Technologies travaille en étroite collaboration avec la société depuis près de quarante ans pour développer des solutions matérielles et logicielles sécurisées leaders sur le marché. Grâce à cette collaboration, les logiciels Microsoft (Windows Server et SQL Server, par exemple) fonctionnent de manière optimale sur les serveurs Dell PowerEdge.

Windows Server 2022

Windows Server 2022 est doté d'un serveur Secured-core basé sur Windows qui utilise le matériel, le firmware et les fonctionnalités du système d'exploitation pour se protéger contre les menaces actuelles et futures. Les serveurs Secured-core utilisent la prise en charge du processeur pour la technologie DRTM (Dynamic Root of Trust for Measurement) afin d'isoler le firmware et de réduire ainsi les risques de violation du code du firmware. En outre, la sécurité basée sur la virtualisation (VBS) isole les composants critiques du système d'exploitation (le noyau, par exemple) du reste du système pour protéger les applications et les données tout en permettant de s'assurer que les serveurs restent dédiés à l'exécution des charges applicatives stratégiques.

La fonctionnalité Secured-core permet une défense proactive en perturbant la plupart des voies empruntées par les pirates informatiques pour exploiter les systèmes. Plusieurs technologies de sécurité Microsoft sont standard ou prises en charge sur les serveurs Secured-core, y compris l'intégrité du code protégé par hyperviseur dans VBS, le module TPM (Trusted Platform Module) 2.0, BitLocker Drive Encryption et UEFI Secure Boot.

Pour plus d'informations sur les fonctionnalités de protection avancée de Windows Server 2022 sur les serveurs Dell PowerEdge, lisez le livre blanc « Gain Advanced Security Protection with the Combined Capabilities of Windows Server 2022 and Next-Generation Dell EMC PowerEdge Servers ».

Protéger les données au niveau des applications de base de données

SQL Server est conçu dans une optique de sécurité. Toutefois, comme mentionné précédemment, de nombreuses entreprises exécutent plusieurs versions de SQL Server et les services IT s'efforcent de trouver une stratégie de base de données plus simple et consolidée.

En outre, le support étendu de SQL Server 2012 prenant fin en juillet 2022, la question de la consolidation des bases de données sur la dernière version de SQL Server devient d'autant plus urgente. Même si les anciennes versions de base de données SQL Server continueront de fonctionner, aucun correctif pris en charge par le fabricant ne sera disponible en cas de problème. De même, aucun correctif ni mise à jour de sécurité ne sera fourni, ce qui pourrait rendre les systèmes vulnérables aux attaques malveillantes.

Pour de nombreuses entreprises, le chemin le plus simple et le plus pratique vers la consolidation consiste à procéder à une mise à niveau vers la dernière version de SQL Server et à exécuter des versions antérieures en mode de compatibilité. Les administrateurs de base de données peuvent simplement sauvegarder une base de données SQL Server existante, puis la charger et la lancer dans SQL Server 2019/2022 en mode de compatibilité. Cette approche peut être un moyen simple et rapide de procéder à une mise à niveau si des tests de régression complets ne sont pas nécessaires. SQL Server 2019 (avec un niveau de compatibilité de 150) peut prendre en charge des versions antérieures à SQL Server 2008 R2 (niveau de compatibilité de 100).

Pratiques d'excellence en matière de sécurité

Afin de mieux protéger les données, il peut être judicieux que les équipes IT veillent à suivre les pratiques d'excellence en matière de sécurité pour SQL Server (pour plus d'informations sur ces pratiques d'excellence et les moyens de les mettre en œuvre, lisez l'article « Securing SQL Server ») sur le blog Microsoft. Ces pratiques d'excellence en matière de sécurité s'appliquent à tous les niveaux de l'infrastructure du datacenter, y compris au matériel et au système d'exploitation, et comprennent les approches suivantes :

- **Améliorer la sécurité physique.** La sécurité physique limite strictement l'accès au serveur physique et aux composants matériels. Cela implique d'utiliser des pièces verrouillées offrant un accès restreint aux serveurs et aux appareils réseau. L'accès aux supports de sauvegarde est limité, ceux-ci étant stockés hors site dans des locaux sécurisés. Il est recommandé d'adopter une approche à plusieurs niveaux, en empêchant l'accès ou en exigeant une carte-clé ou une approbation pour tout accès au périmètre du site, au périmètre du bâtiment, à l'intérieur du bâtiment et au sein du datacenter lui-même.
- **Maintenir le système d'exploitation à jour.** Les correctifs et mises à niveau du système d'exploitation incluent d'importantes améliorations en matière de sécurité. Les mises à jour et mises à niveau du système d'exploitation peuvent être appliquées après avoir été testées avec des applications de base de données.
- **Utiliser des pare-feu.** Les pare-feu augmentent la sécurité au niveau du système d'exploitation en fournissant un passage obligé permettant le ciblage des mesures de sécurité.
- **Réduire la surface.** Limitez les zones vulnérables aux violations en désactivant les fonctionnalités et les composants qui ne sont pas utilisés. La surface d'exposition de SQL Server peut être réduite en exécutant les services requis qui ont le « privilège minimum » et accordent des droits aux services et aux utilisateurs au niveau approprié.
- **Implémenter un contrôle d'accès basé sur les rôles (RBAC) pour les « éléments sécurisables ».**[3] Les éléments sécurisables sont des composants tels que le serveur, la base de données et les objets qu'elle contient. Les éléments sécurisables sont les ressources dont l'accès est régulé par le système d'autorisation SQL Server Database Engine.
- **Chiffrer les données à tous les niveaux.** Cela inclut le chiffrement des données d'application et de stockage.
- **Créer et utiliser des certificats.** Les certificats sont des clés logicielles qui permettent à deux serveurs de communiquer en toute sécurité. Dans SQL Server, les certificats améliorent la sécurité des objets et des connexions.
- **Limiter l'accès aux fichiers du système d'exploitation utilisés par SQL Server.**
- **Utiliser des mots de passe forts à l'échelle de l'organisation.** Il s'agit d'une pratique de sécurité simple, mais souvent sous-estimée.
- **Effectuer des audits.** Assurez-vous que la récupération après sauvegarde fonctionne comme prévu et que l'accès est appliqué de manière appropriée.
- **Utiliser Microsoft Defender pour les bases de données SQL Server.** Microsoft Defender pour les bases de données SQL Server analyse les bases de données pour détecter d'éventuelles failles de sécurité. Il détecte les anomalies qui sont le signe de tentatives inhabituelles et potentiellement dangereuses d'accès ou d'exploitation des bases de données. Ces anomalies comprennent les activités de base de données suspectes, les failles de sécurité potentielles, les attaques par injection SQL et les modèles anormaux d'accès et de requêtes aux bases de données.

Enfin, chaque nouvelle version de SQL Server inclut de nouvelles fonctionnalités de sécurité qui améliorent la protection des données. La nouvelle fonctionnalité de registre, annoncée pour SQL Server 2022, permet de protéger l'intégrité des données en créant un historique immuable des modifications apportées aux données au fil du temps. Cela peut aider à protéger les données contre toute falsification par des acteurs malveillants, et s'avère également bénéfique pour des scénarios tels que les audits internes et externes.

Registre SQL Server

- Utilise un registre immuable pour protéger les données contre toute falsification par des acteurs malveillants
- Établit une relation de confiance numérique dans un système centralisé à l'aide de la technologie de blockchain
- Atteste à d'autres parties que l'intégrité des données n'a pas été compromise

Consolidation et protection du matériel à la base de données

Le rôle de l'IT ne fera qu'augmenter à mesure qu'augmentera la quantité de données à l'ère de l'entreprise numérique. Et comme cette multitude de données s'accompagne de cyberattaques toujours plus intelligentes et plus fréquentes, les équipes IT doivent adopter une stratégie de sécurité des données capable de contribuer à protéger l'infrastructure à tous les niveaux. La mise à niveau vers la dernière version de SQL Server et Windows Server sur les serveurs Dell PowerEdge peut aider les entreprises à protéger leurs données sensibles et celles de leurs clients.

Adoptez une approche axée sur la sécurité pour votre infrastructure. Découvrez en quoi les solutions Dell et Microsoft peuvent vous aider : www.dell.com/en-us/dt/solutions/microsoft-data-platform/index.htm.

Lisez l'article « Gain Advanced Security Protection with the Combined Capabilities of Windows Server 2022 and Next-Generation Dell EMC PowerEdge Servers. »

[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. » Mars 2021.
[3] Pour plus d'informations sur les éléments sécurisables, lisez https://docs.microsoft.com/en-us/sql/relational-databases/security/securables.

DELL Technologies

Microsoft

Modernisez-vous avec Windows Server 2022.
Le système d'exploitation prêt pour le Cloud qui optimise les investissements sur site avec des fonctionnalités hybrides.