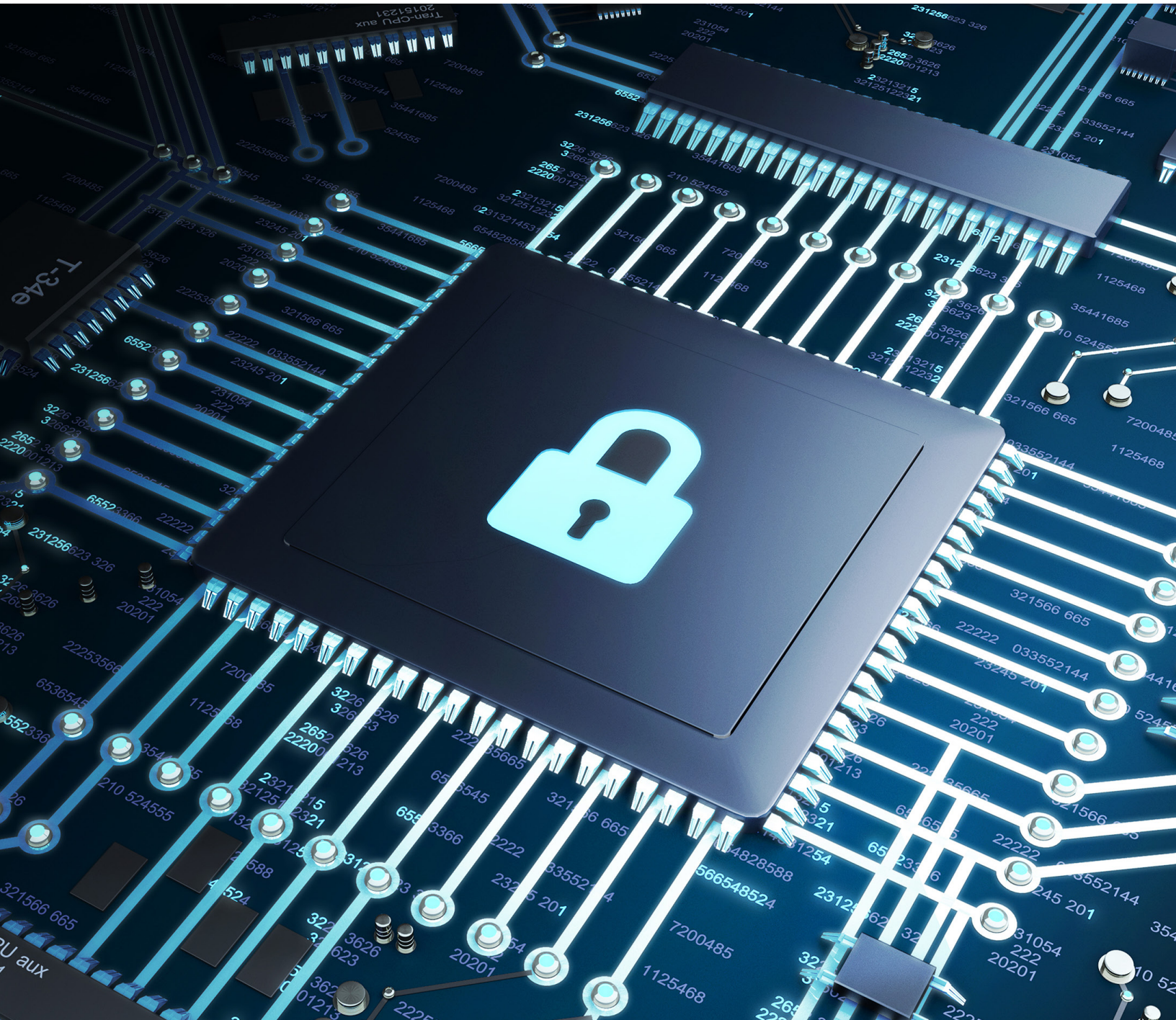
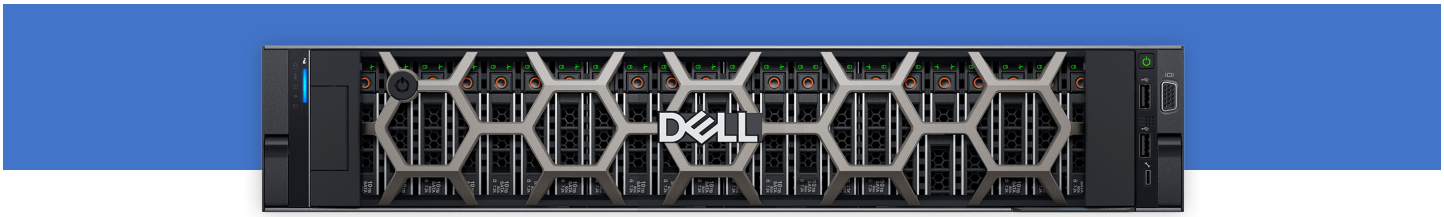
DELL Technologies

Microsoft

White paper

Ottimizzazione della sicurezza dei dati end-to-end con Microsoft SQL Server, server Dell™ PowerEdge™ e Windows Server 2022





Con l'esorbitante passaggio al lavoro da remoto in molti settori, le aziende vanno adattandosi alla nuova normalità e considerano la sicurezza una priorità più che mai. Nel 2021, la maggior parte dei leader aziendali ha affermato che il lavoro da remoto continuerà a essere un'opzione nel prossimo futuro[1]. Di conseguenza, con un numero sempre maggiore di dipendenti dislocati geograficamente in più aree e più endpoint vulnerabili, i responsabili IT aziendali devono adottare un approccio più olistico alla sicurezza.

L'88% dei leader IT intervistati prevede che una qualche forma di lavoro da remoto continuerà e l'utilizzo di più repository di contenuti probabilmente rimarrà un problema nel breve termine[1].

I team IT possono migliorare la sicurezza dei dati in tutta l'azienda adottando un approccio nel data center "sull'intero stack": dall'hardware all'applicazione del database, fino al sistema operativo. La modernizzazione dell'infrastruttura e il consolidamento dei dati nell'ultima versione di Microsoft SQL Server su server Dell™ PowerEdge™ e Windows Server 2022 offrono alle aziende una solida base per proteggere i dati end-to-end in un panorama dell'ambiente di lavoro in continua evoluzione.

Problematiche odierne delle aziende nell'ambito della sicurezza

L'aumento del lavoro da remoto ha esacerbato i modi in cui le aziende sono già vulnerabili agli attacchi informatici:

- **Proliferazione dei contenuti.** La proliferazione dei contenuti è la conseguenza naturale del fatto che molti dipendenti accedono a dati e applicazioni aziendali e ne fanno uso nell'arco della giornata da anni. I dati finiscono per essere archiviati in posizioni diverse e in più repository e continuano a crescere. IDC stima che i dati continueranno ad aumentare a un tasso di crescita annuale composto (CAGR) del 24% nei prossimi cinque anni[2]. Più della metà dei leader IT intervistati (52%) afferma che la propria azienda dispone di almeno 10 repository di file storage[1]. Proprio come avere molti oggetti all'interno di un'abitazione può causare disordine e rischio di perdita, i contenuti salvati o duplicati su più server e database possono mettere i dati a rischio.

Il 41% dei leader IT afferma che la loro principale preoccupazione per la proliferazione dei contenuti è l'aumento del rischio di violazioni e fughe di dati[1].

- **Bring Your Own Device (BYOD) e strumenti di shadow IT.** L'aumento dei rischi per la sicurezza derivante dalla proliferazione dei contenuti è esacerbato dalle policy BYOD, secondo cui le organizzazioni consentono l'uso di smartphone e tablet personali per il lavoro. Questi dispositivi potrebbero non essere aggiornati regolarmente con le patch di sicurezza più recenti e potrebbero essere utilizzati su reti Wi-Fi non protette. Lo "shadow IT", ovvero la dipendenza dalle autoproclamate funzioni di sicurezza delle app basate su cloud, è un altro potenziale vettore di attacco per gli hacker a causa della mancanza intrinseca di controlli e visibilità interni.

- **Pianificazioni diverse delle patch di sicurezza.** Molte organizzazioni utilizzano SQL Server come piattaforma dati, ma con il passare del tempo si ritrovano con versioni diverse del software di database, situazione che complica la gestione dei dati e l'applicazione di patch di sicurezza. Inoltre poiché l'applicazione di patch può rallentare i sistemi e richiedere downtime dei server, i team IT devono determinare l'intervallo di tempo ideale per applicare patch a ciascuna versione, con possibili ritardi negli aggiornamenti.

- **Diversi livelli di accesso dei dipendenti.** Gli amministratori IT devono cercare di gestire le impostazioni delle autorizzazioni quando i dipendenti vengono assunti o lasciano un'organizzazione. Se queste impostazioni non vengono configurate in modo appropriato o aggiornate in modo tempestivo, qualcuno nell'organizzazione può accidentalmente o intenzionalmente esporre i dati aziendali e dei clienti a ransomware e hacker.

Modernizzare la gestione dei dati su una base sicura

L'esecuzione di SQL Server sui server Dell PowerEdge e su Windows Server 2022 aiuta gli amministratori IT a superare queste problematiche e a proteggere i carichi di lavoro business-critical nell'infrastruttura moderna a livello di hardware, sistema operativo (OS) e software.

> Il 65% dei CIO e degli altri leader IT sospetta che file e documenti con informazioni sensibili vengano salvati localmente sui dispositivi personali dei dipendenti[1].

Server Dell PowerEdge

I server Dell PowerEdge aiutano le aziende a difendersi dai rischi intrinseci dell'ambiente odierno con un'infrastruttura abilitata per la sicurezza che supporta una gamma completa di carichi di lavoro e obiettivi moderni. I server PowerEdge sono progettati per accelerare il deployment e migliorare le prestazioni delle applicazioni del database, dell'High Performance Computing (HPC), degli ambienti di virtualizzazione e dell'edge computing. Inoltre, gli strumenti Dell™ OpenManage™ aiutano gli amministratori IT a gestire cluster di grandi dimensioni in modo semplice ed efficace.

I server PowerEdge sono creati su una Root of Trust basata su processore immutabile e abilitano funzioni di sicurezza come la verifica di avvio end-to-end, tra cui personalizzazione di UEFI (Unified Extensible Firmware Interface) Secure Boot, BIOS attendibile, catena di attendibilità del firmware e bootloader del sistema operativo verificato. Il firmware è protetto in conformità con le linee guida NIST (ciò vale anche per gli aggiornamenti firmware firmati) e la gestione dei certificati è semplificata tramite il rinnovo automatico.

I server PowerEdge forniscono inoltre la protezione dei dati inattivi grazie all'utilizzo di Secure Enterprise Key Manager (SEKM) e della protezione dei dati in uso con tecnologie di confidential computing della CPU. Per ridurre le minacce come componenti contraffatti, malware e manomissione del firmware, Dell Technologies adotta un approccio completo alla sicurezza della supply chain con strumenti volti a evitare la contraffazione: una catena di custodia della produzione, la firma del codice, sistemi antintrusione per lo chassis e packaging antimanomissione. Inoltre, la funzione Secured Component Verification (SCV) estende la sicurezza della supply chain verificando l'integrità dei componenti server.

Dell Technologies, uno dei maggiori partner di Microsoft, collabora con quest'ultima da quasi quarant'anni per sviluppare soluzioni hardware e software leader del settore e abilitate per la sicurezza. Grazie a questa collaborazione, i software Microsoft, come Windows Server e SQL Server, vengono eseguiti in modo ottimale sui server Dell PowerEdge.

Windows Server 2022

Windows Server 2022 include un server con core protetto basato su Windows che utilizza funzionalità hardware, firmware e del sistema operativo per la protezione dalle minacce attuali e future. I server con core protetto utilizzano il supporto del processore per la tecnologia DRTM (Dynamic Root of Trust for Measurement) al fine di isolare il firmware, in modo che qualsiasi violazione abbia meno possibilità di influenzare il codice del firmware. Inoltre, la sicurezza basata sulla virtualizzazione (VBS) isola dal resto le parti critiche del sistema operativo, come il kernel, per proteggere applicazioni e dati, contribuendo al contempo a garantire che i server rimangano dedicati all'esecuzione di carichi di lavoro critici.

La funzione core protetto aiuta a difendersi e a bloccare in modo proattivo molti percorsi che i malintenzionati potrebbero utilizzare per l'exploit dei sistemi. I server con core protetto offrono in modo standard o supportano molteplici tecnologie di sicurezza Microsoft, tra cui l'integrità del codice con protezione dell'hypervisor in VBS, Trusted Platform Module (TPM) 2.0, crittografia dell'unità BitLocker e UEFI Secure Boot.

Per ulteriori informazioni sulle funzionalità di protezione avanzate di Windows Server 2022 sui server Dell PowerEdge, leggere il white paper "Protezione avanzata con le funzionalità combinate di Windows Server 2022 e i server Dell EMC PowerEdge di nuova generazione".

Proteggere i dati a livello di applicazione del database

Alla base della progettazione di SQL Server vi è la sicurezza. Tuttavia, come accennato in precedenza, molte aziende eseguono diverse versioni di SQL Server e i dipartimenti IT sono alla ricerca di una strategia per i database più semplice e consolidata.

Inoltre, il supporto esteso di SQL Server 2012 termina a luglio 2022, fattore che rende il consolidamento del database alla versione più recente di SQL Server un problema più urgente. Anche se le versioni precedenti del database SQL Server continueranno a funzionare, in caso di problemi non sarà disponibile una correzione supportata dal produttore. Inoltre, non verranno fornite patch o aggiornamenti di sicurezza, condizione che potrebbe rendere i sistemi vulnerabili ad attacchi malevoli.

Il percorso più semplice e pratico verso il consolidamento per molte aziende è l'aggiornamento alla versione più recente di SQL Server e l'esecuzione di versioni precedenti in modalità compatibilità. Gli amministratori di database possono semplicemente eseguire il backup di un database SQL Server legacy, quindi caricarlo e avviarlo in SQL Server 2019/2022 in modalità di compatibilità. Questo approccio può rappresentare un modo rapido e semplice per eseguire l'aggiornamento se non è necessario il test di regressione completo. SQL Server 2019 (con un livello di compatibilità di 150) può supportare le versioni di SQL Server 2008 R2 (livello di compatibilità 100).

Best practice per la sicurezza

Per proteggere ulteriormente i dati, i team IT potrebbero voler essere certi di seguire le best practice di sicurezza per SQL Server (per ulteriori informazioni su queste best practice e sui modi per implementarle, leggere il post del blog Microsoft "Proteggere SQL Server"). Queste best practice per la sicurezza si applicano a tutti i livelli dell'infrastruttura del data center, tra cui hardware e sistema operativo, e includono quanto segue:

- **Ulteriore sicurezza fisica.** La sicurezza fisica limita rigorosamente l'accesso al server fisico e ai componenti hardware. Ciò significa utilizzare stanze chiuse a chiave con accesso limitato ai server e ai dispositivi di rete. L'accesso ai supporti di backup è limitato mediante l'archiviazione in una posizione off-site sicura. È consigliabile adottare un approccio multilayer: impedire l'accesso o richiedere una chiave magnetica/l'approvazione al perimetro della struttura, al perimetro dell'edificio, all'interno dell'edificio e nel data center.
- **Mantenere aggiornato il sistema operativo.** I service pack e gli aggiornamenti del sistema operativo includono importanti miglioramenti della sicurezza. Gli aggiornamenti e gli upgrade al sistema operativo possono essere applicati dopo essere stati testati con le applicazioni del database.
- **Utilizzare i firewall.** I firewall aumentano la sicurezza a livello di sistema operativo fornendo una strozzatura in cui è possibile concentrare le misure di sicurezza.
- **Ridurre la superficie.** È possibile limitare le aree vulnerabili alle violazioni disattivando o disabilitando funzioni e componenti non in uso. La superficie di attacco di SQL Server può essere ridotta eseguendo i servizi necessari che hanno "privilegi minimi" e che concedono ai servizi e agli utenti diritti al livello appropriato.
- **Implementare il controllo degli accessi basato sui ruoli (RBAC) per le entità a protezione diretta[3].** Le entità a protezione diretta includono componenti quali il server, il database e gli oggetti contenuti nel database. Le entità a protezione diretta sono le risorse a cui il sistema di autorizzazione del motore di database di SQL Server regola l'accesso.
- **Crittografare i dati a tutti i livelli.** Si fa riferimento alla crittografia dei dati delle applicazioni e dello storage.
- **Creare e usare i certificati.** I certificati sono chiavi software che consentono a due server di comunicare in modo sicuro. In SQL Server, i certificati migliorano la sicurezza di oggetti e connessioni.
- **Limitare l'accesso ai file del sistema operativo utilizzati da SQL Server.**
- **Utilizzare password complesse in tutta l'organizzazione.** Si tratta di una pratica di sicurezza semplice ma spesso sottovalutata.
- **Condurre audit.** Assicurarsi che il ripristino dopo il backup funzioni come previsto e che l'accesso venga applicato in modo appropriato.
- **Usare Microsoft Defender per database SQL Server.** Microsoft Defender per i database SQL Server analizza i database alla ricerca di vulnerabilità. Rileva le anomalie che indicano tentativi insoliti e potenzialmente dannosi di accedere o sfruttare i database. Queste anomalie includono attività sospette del database, potenziali vulnerabilità, attacchi SQL injection e accesso anomalo al database e modelli di query.

Infine, ogni nuova versione di SQL Server include nuove funzioni di protezione che migliorano la protezione dei dati. La nuova funzione di contabilità generale, annunciata per SQL Server 2022, aiuta a proteggere l'integrità dei dati creando un track record immutabile delle modifiche apportate nel tempo ai dati. In questo modo è possibile proteggere i dati da manomissioni da parte di utenti malintenzionati ed è utile per scenari come i controlli interni ed esterni.

Libro mastro di SQL Server

- Utilizza un registro mastro immutabile per proteggere i dati da manomissioni da parte di malintenzionati.
- Definisce la fiducia digitale in un sistema centralizzato utilizzando la tecnologia blockchain
- Attesta ad altre parti che l'integrità dei dati non è stata compromessa.

Consolidare e proteggere dall'hardware al database

Il ruolo dell'IT è destinato a essere sempre più prominente all'aumentare dei dati nell'azienda digitale. Poiché questa ricchezza di dati è accompagnata da attacchi informatici più intelligenti e più frequenti, i team IT devono adottare una strategia di sicurezza dei dati che aiuti a proteggere l'infrastruttura a tutti i livelli. L'aggiornamento alla versione più recente di SQL Server e Windows Server sui server Dell PowerEdge può aiutare le aziende a proteggere i dati sensibili aziendali e dei clienti.

Un approccio che metta la sicurezza al primo posto nell'infrastruttura è ciò che serve. Per conoscere come le soluzioni Dell e Microsoft possono essere d'aiuto accedere alla pagina: www.dell.com/en-us/dt/solutions/microsoft-data-platform/index.htm.

Leggere "Protezione avanzata con le funzionalità combinate di Windows Server 2022 e i server Dell EMC PowerEdge di nuova generazione".

[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 2021.
[3] Per maggiori informazioni sulle entità a protezione diretta, leggere https://docs.microsoft.com/en-us/sql/relational-databases/security/securables.

DELL Technologies

Microsoft

Modernizzazione con Windows Server 2022.
Il sistema operativo predisposto per il cloud che incrementa gli investimenti on-premise con funzionalità ibride.