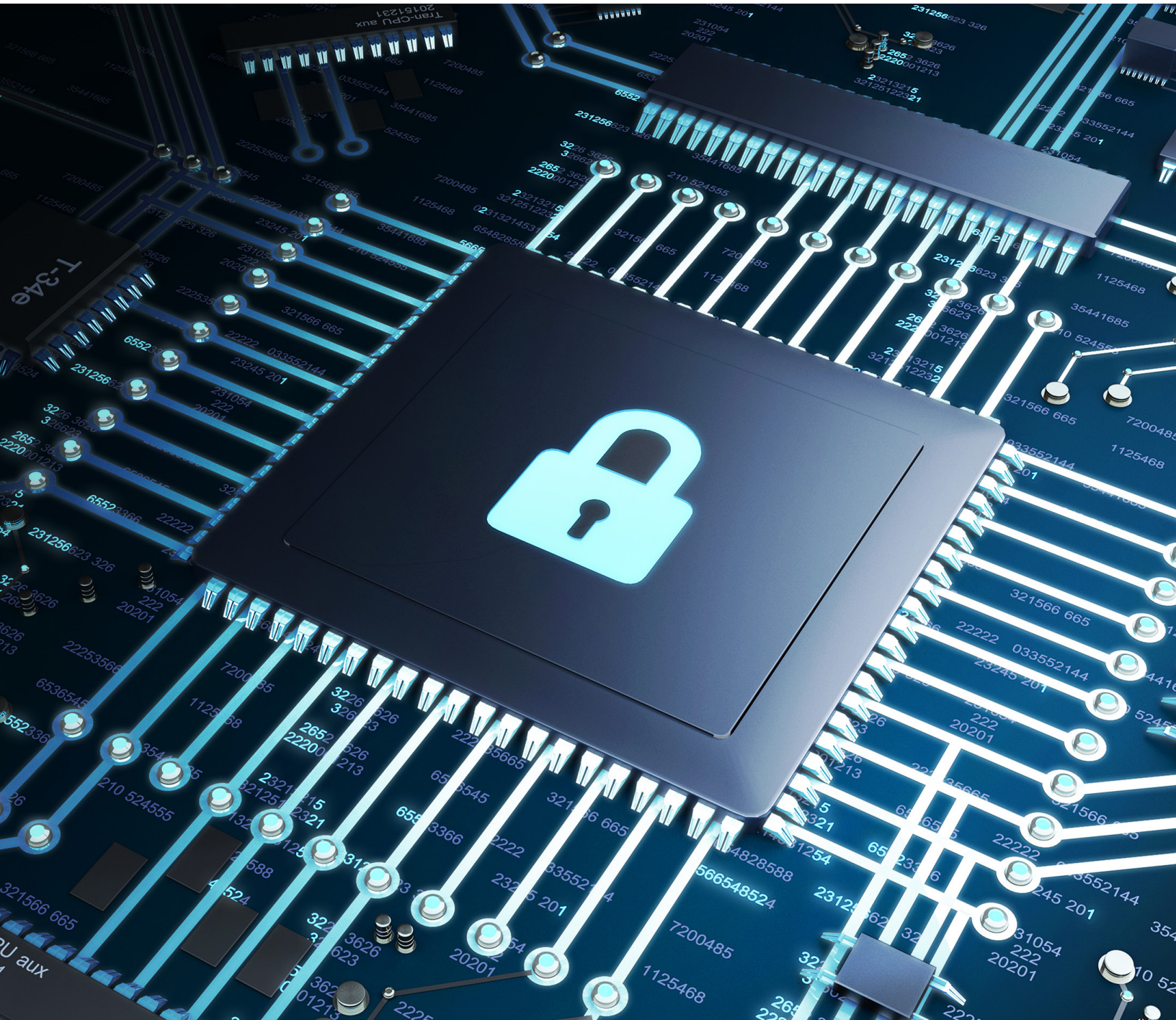
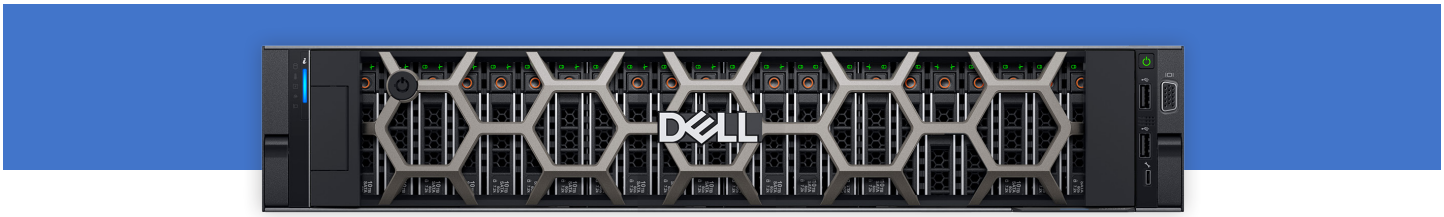
DELL Technologies

Microsoft

Whitepaper

Verbeter end-to-end databeveiliging met Microsoft SQL Server, Dell™ PowerEdge™ servers en Windows Server 2022





Met de enorme verschuiving naar werken op afstand in veel sectoren, passen bedrijven zich aan het nieuwe normaal aan en kennen ze nu meer prioriteit aan beveiliging toe dan ooit tevoren. In 2021 zeiden de meeste bedrijfsleiders dat werken op afstand in de nabije toekomst zal blijven bestaan.[1] En nu meer werknemers geografisch verspreid zijn over meer gebieden dan ooit, met meerdere kwetsbare eindpunten, moeten IT-managers van bedrijven een meer holistische benadering van beveiliging hanteren.

88 procent van de ondervraagde IT-leiders verwacht dat een vorm van werken op afstand zal blijven bestaan, en het gebruik van meerdere storagelocaties voor content zal op korte termijn waarschijnlijk een probleem blijven.[1]

IT-teams kunnen de databeveiliging in de hele onderneming verbeteren door een 'hele stack'-aanpak te hanteren in het datacenter: van hardware tot databaseapplicatie tot besturingssysteem. Het moderniseren van de infrastructuur en het consolideren van data op de nieuwste versie van Microsoft SQL Server op Dell™ PowerEdge™ servers en Windows Server 2022 biedt ondernemingen een sterke basis om data end-to-end te beschermen in een veranderende werkomgeving.

Beveiligingsuitdagingen voor moderne ondernemingen

Door de opkomst van werken op afstand zijn ondernemingen nog kwetsbaarder voor cyberaanvallen:

- **Wildgroei aan content.** De wildgroei aan content is het natuurlijke gevolg van het feit dat veel werknemers jarenlang de hele dag door toegang hebben tot en gebruikmaken van bedrijfsdata en applicaties. Data worden uiteindelijk op verschillende locaties en in meerdere storagelocaties opgeslagen. En de hoeveelheid data blijft toenemen. IDC schat dat de hoeveelheid data de komende vijf jaar zal blijven toenemen met een samengesteld jaarlijks groeipercentage (CAGR) van 24 procent.[2] Meer dan de helft van de ondervraagde IT-leiders (52 procent) zegt dat hun bedrijf ten minste 10 storagelocaties voor bestanden heeft.[1] Net zoals het hebben van veel items in een huis kan leiden tot rommel en risico op verlies, kan content die is opgeslagen of gedupliceerd op meerdere servers en databases data in gevaar brengen.

41 procent van de IT-leiders zegt dat hun grootste zorg over de wildgroei aan content het verhoogde risico op datalekken is.[1]

- **Bring Your Own Device (BYOD) en schaduw-IT.** Verhoogde beveiligingsrisico's door wildgroei aan content worden verergerd door BYOD-beleid, waarbij organisaties het gebruik van persoonlijke smartphones en tablets voor het werk toestaan. Deze apparaten worden mogelijk niet regelmatig bijgewerkt met de nieuwste beveiligingspatches en worden mogelijk gebruikt op onbeveiligde Wi-Fi-netwerken. Schaduw-IT, of de afhankelijkheid van de zelfbenoemde beveiligingsfuncties van cloudgebaseerde apps, is een andere potentiële aanvalsvector voor hackers vanwege het inherente gebrek aan interne controles en zichtbaarheid.

- **Verschillende schema's voor beveiligingspatches.** Veel organisaties gebruiken SQL Server als hun dataplatform, maar na verloop van tijd eindigen ze met verschillende versies van de databasesoftware, wat het databeheer en het patchen van de beveiliging bemoeilijkt. En omdat patching systemen kan vertragen en serverdowntime vereist, moeten IT-teams het ideale tijdsbestek bepalen om elke versie te patchen, waardoor updates kunnen worden vertraagd.

- **Verschillende toegangsniveaus voor medewerkers.** IT-beheerders moeten proberen de machtigingsinstellingen bij te houden wanneer werknemers worden aangenomen of een organisatie verlaten. Wanneer deze niet op de juiste manier worden ingesteld of niet tijdig worden bijgewerkt, kan iemand in de organisatie per ongeluk of opzettelijk bedrijfs- en klantdata blootstellen aan ransomware en hackers.

Databeheer moderniseren op een veilige basis

Door SQL Server uit te voeren op Dell PowerEdge servers en Windows Server 2022 kunnen IT-beheerders deze uitdagingen overwinnen en bedrijfskritieke workloads beveiligen op moderne infrastructuur op hardware-, besturingssysteem- (OS) en softwareniveau.

> 65 procent van de CIO's en andere IT-leiders vermoedt dat bestanden en documenten met gevoelige informatie lokaal worden opgeslagen op de persoonlijke apparaten van werknemers.[1]

Dell PowerEdge servers

Met Dell PowerEdge servers kunnen ondernemingen zich verdedigen tegen de risico's die inherent zijn aan de huidige omgeving met een beveiligde infrastructuur die een volledige reeks moderne workloads en doelstellingen ondersteunt. PowerEdge servers zijn ontworpen om de implementatie te versnellen en prestaties te verbeteren voor databaseapplicaties, high-performance computing (HPC), virtualisatieomgevingen en edge-computing. En met Dell™ OpenManage™ tools kunnen IT-beheerders grote clusters eenvoudig en effectief beheren.

PowerEdge servers zijn gebouwd op een onveranderlijke, op silicium gebaseerde root-of-trust en maken beveiligingsfuncties mogelijk zoals end-to-end opstartverificatie met inbegrip van Unified Extensible Firmware Interface (UEFI), vertrouwd BIOS, chain of trust voor firmware en geverifieerde OS-bootloader. Firmware wordt beschermd met behulp van NIST-richtlijnen (National Institute of Standards and Technology), waaronder ondertekende firmware-updates. Certificaatbeheer wordt vereenvoudigd door automatische verlenging.

PowerEdge servers bieden ook 'data-at-rest'-bescherming met behulp van Secure Enterprise Key Manager (SEKM) en 'data-in-use'-bescherming met CPU-technologieën van Confidential Compute. Ter bescherming tegen bedreigingen zoals vervalste componenten en verstoring via malware en firmware, hanteert Dell Technologies een uitgebreide aanpak van de beveiliging van de toeleveringsketen gebruik van tools ter voorkoming van vervalsingen, chain of custody bij productie, codeondertekening, detectie van chassisintrusie en tamper-evident verpakking. Verder breidt Secured Component Verification (SCV) de beveiliging van de toeleveringsketen uit door de integriteit van servercomponenten te verifiëren.

Als een van de grootste partners van Microsoft, werkt Dell Technologies al bijna vier decennia nauw samen met Microsoft om toonaangevende, op beveiliging gebaseerde hardware- en softwareoplossingen te ontwikkelen. Met deze samenwerking draait Microsoft-software, zoals Windows Server en SQL Server, optimaal op Dell PowerEdge servers.

Windows Server 2022

Windows Server 2022 beschikt over een Secured-core server op basis van Windows die hardware-, firmware- en besturingssysteemmogelijkheden gebruikt om bescherming te bieden tegen huidige en toekomstige dreigingen. Secured-core servers gebruiken processorondersteuning voor DRTM-technologie (Dynamic Root of Trust for Measurement) om firmware te isoleren, zodat een eventuele inbreuk minder kans heeft om firmwarecode te beïnvloeden. Bovendien isoleert VBS (Virtualization Based Security) essentiële onderdelen van het besturingssysteem, zoals de kernel, van de rest van het systeem om applicaties en data te beschermen en er tegelijkertijd voor te zorgen dat servers zich kunnen blijven richten op het uitvoeren van kritieke workloads.

Deze Secured-core-functionaliteit helpt op proactieve wijze bescherming te bieden tegen veel van de paden die aanvallers gebruiken om systemen te misbruiken en deze te verstoren. Meerdere beveiligingstechnologieën van Microsoft zijn standaard of worden ondersteund op Secured-core servers, waaronder door een hypervisor beschermde code-integriteit in VBS, Trusted Platform Module (TPM) 2.0, BitLocker Drive Encryption en UEFI Secure Boot.

Lees voor meer informatie over de geavanceerde beveiligingsmogelijkheden van Windows Server 2022 op Dell PowerEdge servers de whitepaper, "Geavanceerde beveiliging verwerven met de gecombineerde mogelijkheden van Windows Server 2022 en de Dell EMC PowerEdge servers van de volgende generatie".

Data beschermen op het applicatieniveau van de database

SQL Server is gebouwd met het oog op beveiliging. Zoals eerder vermeld, gebruiken veel ondernemingen echter verschillende versies van SQL Server en zijn IT-afdelingen op zoek naar een eenvoudigere, geconsolideerde databasestrategie.

Bovendien eindigt de uitgebreide support voor SQL Server 2012 in juli 2022, waardoor databaseconsolidatie op de nieuwste versie van SQL Server een urgenter probleem wordt. Hoewel oudere SQL Server-databaseversies blijven werken, is er bij problemen geen door de fabrikant ondersteunde oplossing beschikbaar. Er worden ook geen patches of beveiligingsupdates geleverd, waardoor systemen kwetsbaar kunnen worden voor schadelijke aanvallen.

De meest eenvoudige, praktische weg naar consolidatie voor veel ondernemingen is upgraden naar de nieuwste versie van SQL Server en oudere versies uitvoeren in de compatibiliteitsmodus. Databasebeheerders kunnen eenvoudig een back-up maken van een verouderde SQL Server-database en deze vervolgens laden en in de compatibiliteitsmodus starten in SQL Server 2019/2022. Deze aanpak kan een snelle en eenvoudige manier zijn om te upgraden als volledige regressietests niet nodig zijn. SQL Server 2019 (met een compatibiliteitsniveau van 150) kan versies ondersteunen tot SQL Server 2008 R2 (compatibiliteitsniveau van 100).

Best practices voor beveiliging

Om data verder te beschermen, kunnen IT-teams ervoor zorgen dat ze de best practices voor beveiliging voor SQL Server volgen (lees voor meer informatie over deze best practices en manieren om ze te implementeren het Microsoft-blogbericht "Securing SQL Server"). Deze best practices voor beveiliging gelden voor alle niveaus van de datacenterinfrastructuur, inclusief de hardware en het besturingssysteem, en omvatten:

- **Fysieke beveiliging verbeteren.** Fysieke beveiliging zorgt voor een strikte beperking van de toegang tot de fysieke server en hardwarecomponenten. Dit betekent het gebruik van afgesloten ruimtes met beperkte toegang tot servers en netwerkapparaten. Toegang tot back-upmedia wordt beperkt door deze op een veilige externe locatie op te slaan. Er wordt een gelaagde aanpak aanbevolen: het voorkomen van toegang of het vereisen van een keycard/goedkeuring aan de rand van de faciliteit, aan de rand van het gebouw, binnen het gebouw en op de vloer van het datacenter.
- **Besturingssysteem up-to-date houden.** Servicepacks en upgrades voor besturingssystemen bevatten belangrijke beveiligingsverbeteringen. Updates en upgrades van het besturingssysteem kunnen worden toegepast nadat ze zijn getest met databaseapplicaties.
- **Firewalls gebruiken.** Firewalls verhogen de beveiliging op het niveau van het besturingssysteem door een knelpunt te bieden waarop beveiligingsmaatregelen kunnen worden gericht.
- **Oppervlak verkleinen.** Beperk de gebieden die kwetsbaar zijn voor inbreuken door functies en onderdelen die niet worden gebruikt uit te schakelen of te deactiveren. Het oppervlak van SQL Server kan worden verkleind door vereiste services uit te voeren die 'minste bevoegdheden' hebben en die services en gebruikersrechten op het juiste niveau verlenen.
- **Op rollen gebaseerde toegangscontrole (RBAC) implementeren voor 'beveiligbare items'.**[3] Beveiligbare materialen omvatten componenten zoals de server, de database en objecten in de database. Beveiligbare items zijn de bronnen waartoe het SQL Server Database Engine-autorisatiesysteem de toegang regelt.
- **Data versleutelen op alle niveaus.** Dit omvat versleuteling van applicatie- en storagedata.
- **Certificaten maken en gebruiken.** Certificaten zijn softwaresleutels waarmee twee servers veilig kunnen communiceren. In SQL Server verbeteren certificaten de beveiliging van objecten en verbindingen.
- **Toegang beperken tot besturingssysteembestanden die door SQL Server worden gebruikt.**
- **Sterke wachtwoorden gebruiken in de hele organisatie.** Dit is een eenvoudige beveiligingspraktijk die vaak onvoldoende prioriteit krijgt.
- **Audits uitvoeren.** Controleer of herstel na de back-up werkt zoals verwacht en of de toegang correct wordt toegepast.
- **Microsoft Defender for SQL Server-databases gebruiken.** Microsoft Defender for SQL Server-databases scant databases op beveiligingslekken. Hierbij wordt gedetecteerd op afwijkingen die wijzen op ongebruikelijke en potentieel schadelijke pogingen om toegang te krijgen tot databases of deze te misbruiken. Deze afwijkingen zijn onder andere verdachte databaseactiviteiten, mogelijke beveiligingslekken, SQL-injectieaanvallen en afwijkende databasetoegang en querypatronen.

Tot slot bevat elke nieuwe versie van SQL Server nieuwe beveiligingsfuncties die de databescherming verbeteren. De nieuwe grootboekfunctie, die werd aangekondigd voor SQL Server 2022, helpt de data-integriteit te beschermen door een onveranderlijke trackrecord van datawijzigingen in de loop van de tijd te creëren. Hiermee kunnen data worden beschermd tegen manipulatie door kwaadwillenden en de functie is gunstig in scenario's zoals interne en externe audits.

SQL Server Ledger

- Maakt gebruik van een onveranderlijk grootboek om data te beschermen tegen manipulatie door kwaadwillenden
- Zorgt voor digitaal vertrouwen in een gecentraliseerd systeem met behulp van blockchain-technologie
- Bevestigt aan andere partijen dat de data-integriteit niet in gevaar is gebracht

Van hardware tot database consolideren en beschermen

Naarmate de groei van data in de digitale omgeving verder toeneemt, zal de rol van IT alleen maar toenemen. En omdat die schat aan data gepaard gaat met slimmere en frequentere cyberaanvallen, moeten IT-teams een strategie voor databeveiliging toepassen die helpt de infrastructuur op alle niveaus te beschermen. Door te upgraden naar de nieuwste versie van SQL Server en Windows Server op Dell PowerEdge servers, kunnen bedrijven gevoelige bedrijfs- en klantdata beschermen.

Kies een beveiligingsgerichte aanpak voor uw infrastructuur. Meer informatie over hoe oplossingen van Dell en Microsoft nuttig voor u kunnen zijn: www.dell.com/en-us/dt/solutions/microsoft-data-platform/index.htm.

Lees "Geavanceerde beveiliging verwerven met de gecombineerde mogelijkheden van Windows Server 2022 en de Dell EMC PowerEdge servers van de volgende generatie."

[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." Maart 2021.
[3] Lees https://docs.microsoft.com/en-us/sql/relational-databases/security/securables voor meer informatie over beveiligbare objecten (securables).

DELL Technologies

Microsoft

Moderniseer met Windows Server 2022.
Het besturingssysteem dat klaar is voor de cloud en on-premise investeringen een boost geeft met hybride opties.