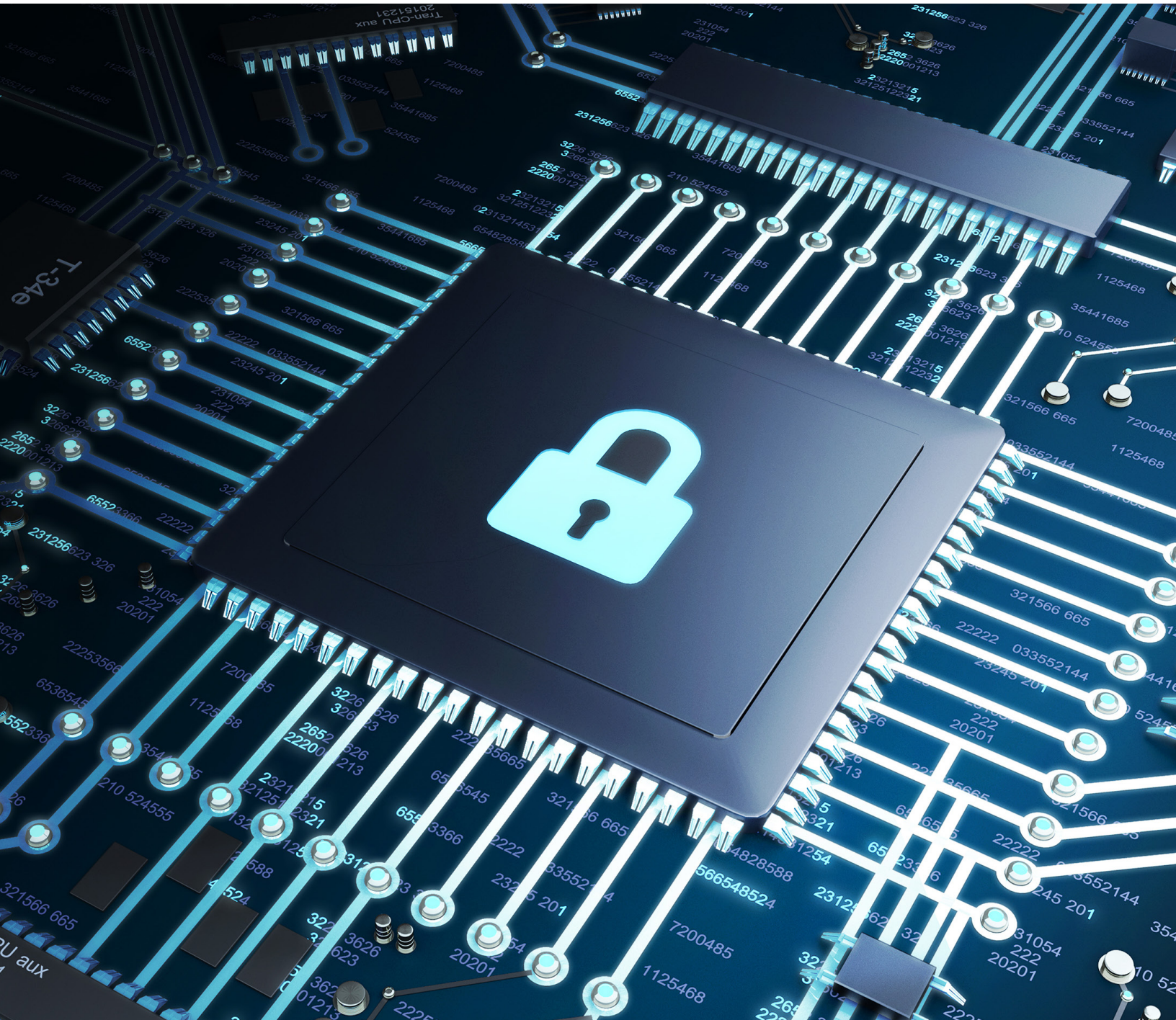
DELL Technologies

Microsoft

Whitepaper

# Verbesserte durchgängige Datensicherheit mit Microsoft SQL Server, Dell™ PowerEdge™-Servern und Windows Server 2022



Mit der gewaltigen Umstellung auf Remotearbeit in vielen Branchen stellen sich Unternehmen auf die neue Normalität ein und legen mehr Wert auf Sicherheit als je zuvor. Im Jahr 2021 gaben die meisten Führungskräfte an, dass Remotearbeit in absehbarer Zukunft fortgesetzt wird.[1] Da immer mehr MitarbeiterInnen geografisch auf mehr Gebiete verteilt und mehrere anfällige Endpunkte vorhanden sind, müssen IT-Manager in Unternehmen außerdem einen ganzheitlicheren Sicherheitsansatz verfolgen.

88 % der befragten IT-Führungskräfte gehen davon aus, dass irgendeine Form von Remotearbeit fortgesetzt wird, und die Verwendung mehrerer Content Repositorys wahrscheinlich kurzfristig ein Problem bleiben wird.[1]

IT-Teams können die Datensicherheit im gesamten Unternehmen verbessern, indem sie im Rechenzentrum einen „Whole-Stack“-Ansatz verfolgen, der von der Hardware über die Datenbankanwendung bis hin zum Betriebssystem reicht. Die Modernisierung der Infrastruktur und die Konsolidierung von Daten auf der neuesten Version von Microsoft SQL Server auf Dell™ PowerEdge™-Servern und Windows Server 2022 bieten Unternehmen eine solide Grundlage für den durchgängigen Schutz von Daten in einer sich wandelnden Arbeitsplatzlandschaft.

## Sicherheitsherausforderungen, mit denen Unternehmen heute konfrontiert sind

Durch die zunehmende Remotearbeit sind Unternehmen ohnehin schon anfällig für Cyberangriffe:

- **Unkontrollierte Ausbreitung von Inhalten.** Die unkontrollierte Ausbreitung von Inhalten ist die natürliche Folge davon, dass viele MitarbeiterInnen seit Jahren im Laufe des Tages auf Unternehmensdaten und -anwendungen zugreifen und diese nutzen. Daten werden an verschiedenen Orten und in mehreren Repositorys gespeichert. Und die Datenmenge wächst weiter an. IDC schätzt, dass Daten in den nächsten 5 Jahren mit einer durchschnittlichen jährlichen Wachstumsrate (CAGR) von 24 % weiter zunehmen werden.[2] Mehr als die Hälfte der befragten IT-Führungskräfte (52 %) gibt an, dass ihr Unternehmen über mindestens 10 Datei-Storage-Repository verfügt.[1] Genauso wie viele Gegenstände in einem Haus zu Unordnung und Verlustrisiko führen können, können Inhalte, die über mehrere Server und Datenbanken hinweg gespeichert oder dupliziert werden, Daten gefährden.

41 % der IT-Führungskräfte geben an, dass ihre größte Sorge bei der Ausbreitung von Inhalten das erhöhte Risiko von Datenschutzverletzungen und Datenlecks ist.[1]

- **Bring Your Own Device (BYOD) und Schatten-IT** Erhöhte Sicherheitsrisiken durch die unkontrollierte Ausbreitung von Inhalten werden durch BYOD-Richtlinien verschärft, bei denen Unternehmen die Verwendung persönlicher Smartphones und Tablets für die Arbeit erlauben. Diese Geräte werden möglicherweise nicht regelmäßig mit den neuesten Sicherheitspatches aktualisiert und zudem in ungesicherten Wi-Fi-Netzwerken verwendet. „Schatten-IT“ oder das Vertrauen auf die selbsterklärten Sicherheitsfunktionen von cloudbasierten Anwendungen ist ein weiterer potenzieller Angriffsvektor für HackerInnen, da es an internen Kontrollen und Transparenz mangelt.
- **Unterschiedliche Zeitpläne für Sicherheitspatches.** Viele Unternehmen verwenden SQL Server als Datenplattform, sammeln im Laufe der Zeit jedoch unterschiedliche Versionen der Datenbanksoftware an, was das Datenmanagement und Sicherheitspatching erschwert. Und da das Patching Systeme verlangsamen und Serverausfallzeiten erfordern kann, müssen IT-Teams den idealen Zeitrahmen für das Patchen der einzelnen Versionen festlegen, was Updates verzögern kann.
- **Unterschiedliche Mitarbeiterzugriffsebenen.** IT-AdministratorInnen müssen versuchen, die Berechtigungseinstellungen beizubehalten, wenn MitarbeiterInnen eingestellt werden oder ein Unternehmen verlassen. Wenn Unternehmens- und Kundendaten nicht ordnungsgemäß eingerichtet oder aktualisiert werden, können sie versehentlich oder absichtlich Ransomware und HackerInnen ausgesetzt sein.

## Modernisierung des Datenmanagements auf einer sicheren Grundlage

Die Ausführung von SQL Server auf Dell PowerEdge-Servern und Windows Server 2022 hilft IT-AdministratorInnen, diese Herausforderungen zu überwinden und geschäftskritische Workloads in einer modernen Infrastruktur auf Hardware-, Betriebssystem- (BS) und Softwareebene zu sichern.

65 % der CIOs und anderer IT-Führungskräfte vermuten, dass Dateien und Dokumente mit vertraulichen Informationen lokal auf den persönlichen Geräten von MitarbeiterInnen gespeichert werden.[1]

### Dell PowerEdge-Server

Dell PowerEdge-Server helfen Unternehmen, die Risiken der heutigen Umgebung mit einer sicherheitsfähigen Infrastruktur abzuwehren, die ein umfassendes Angebot an modernen Workloads und Zielen unterstützt. PowerEdge-Server wurden entwickelt, um die Bereitstellung zu beschleunigen und die Performance für Datenbankanwendungen, High-Performance-Computing (HPC), Virtualisierungsumgebungen und Edge Computing zu verbessern. Mit den Dell™ OpenManage™-Tools können IT-AdministratorInnen große Cluster einfach und effektiv managen.

PowerEdge-Server basieren auf einer unveränderlichen, chipbasierten Root of Trust und bieten Sicherheitsfunktionen wie End-to-End-Startverifizierung, darunter UEFI (Unified Extensible Firmware Interface) Secure Boot-Anpassung, ein vertrauenswürdiges BIOS, Firmwaresicherheit und ein verifizierter BS-Bootloader. Die Firmware wird mithilfe Richtlinien des National Institute of Standards and Technology (NIST) geschützt, einschließlich signierter Firmwareupdates. Das Zertifikatmanagement wird durch eine automatische Verlängerung vereinfacht.

PowerEdge-Server bieten außerdem Schutz für ruhende Daten mit SEKM (Secure Enterprise Key Manager) und Schutz für verwendete Daten mit vertraulichen Compute-CPU-Technologien. Um Bedrohungen wie gefälschte Komponenten, Malware und Firmwaremanipulationen vorzubeugen, verfolgt Dell Technologies einen umfassenden Ansatz für die Lieferkettensicherheit mit verschiedenen Tools wie die Vermeidung von Fälschungen, eine Beweiskette in der Fertigung, Codesignierung, Schutz vor Gehäuseeingriffen und manipulationssichere Verpackungen. Darüber hinaus erweitert SCV (Secured Component Verification) die Lieferkettensicherheit durch die Verifizierung der Integrität von Serverkomponenten.

Als einer der größten Partner von Microsoft arbeitet Dell Technologies seit fast vier Jahrzehnten eng mit Microsoft zusammen, um branchenführende, sicherheitsverstärkte Hardware- und Softwarelösungen zu entwickeln. Dank dieser Zusammenarbeit kann Microsoft-Software wie Windows Server und SQL Server optimal auf Dell PowerEdge-Servern ausgeführt werden.

### Windows Server 2022

Windows Server 2022 verfügt über einen auf Windows basierenden Secured-Core-Server, der Hardware-, Firmware- und BS-Funktionen nutzt, um vor aktuellen und zukünftigen Bedrohungen zu schützen. Secured-Core-Server nutzen die Prozessorunterstützung für die DRTM-Technologie (Dynamic Root of Trust for Measurement), um die Firmware zu isolieren, sodass bei Sicherheitsverletzungen die Wahrscheinlichkeit einer Auswirkung auf den Firmwarecode geringer ist. Darüber hinaus isoliert die virtualisierungsbasierte Sicherheit (VBS) kritische Teile des Betriebssystems wie den Kernel vom Rest des Systems, um Anwendungen und Daten zu schützen und gleichzeitig sicherzustellen, dass Server kritische Workloads weiter ausführen können.

Diese Secured-Core-Funktion sorgt für eine proaktive Abwehr und Unterbrechung vieler der Pfade, die AngreiferInnen für einen Exploit von Systemen nutzen. Mehrere Microsoft-Sicherheitstechnologien werden standardmäßig auf Secured-Core-Servern bereitgestellt oder unterstützt, einschließlich Hypervisor-geschützter Codeintegrität in VBS, Trusted Platform Module (TPM) 2.0, BitLocker-Laufwerkverschlüsselung und UEFI Secure Boot.

Weitere Informationen zu den erweiterten Schutzfunktionen von Windows Server 2022 auf Dell PowerEdge-Servern finden Sie im Whitepaper „Gain Advanced Security Protection with the Combined Capabilities of Windows Server 2022 and Next-Generation Dell EMC PowerEdge Servers“.

## Schutzvon Daten auf Datenbankanwendungsebene

Bei der Entwicklung von SQL Server wurde großer Wert auf Sicherheit gelegt. Wie bereits erwähnt, führen viele Unternehmen jedoch mehrere Versionen von SQL Server aus und IT-Abteilungen suchen nach einer einfacheren, konsolidierten Datenbankstrategie.

Darüber hinaus wurde der erweiterte Support für SQL Server 2012 im Juli 2022 eingestellt, wodurch die Datenbankkonsolidierung auf der neuesten Version von SQL Server zu einem dringenderen Problem wird. Ältere SQL Server-Datenbankversionen funktionieren weiterhin, aber ein vom Hersteller unterstützter Fix ist nicht verfügbar, wenn Probleme auftreten. Patches oder Sicherheitsupdates werden ebenfalls nicht bereitgestellt, was Systeme anfällig für bösartige Angriffe machen könnte.

Der einfachste und praktischste Weg zur Konsolidierung besteht für viele Unternehmen darin, ein Upgrade auf die neueste Version von SQL Server durchzuführen und ältere Versionen im Kompatibilitätsmodus auszuführen. DatenbankadministratorInnen können einfach eine SQL Server-Legacy-Datenbank sichern und diese dann in SQL Server 2019/2022 im Kompatibilitätsmodus laden und starten. Dieser Ansatz kann eine schnelle und einfache Möglichkeit für ein Upgrade sein, wenn keine vollständigen Regressionstests erforderlich sind. SQL Server 2019 (mit einem Kompatibilitätslevel von 150) kann Versionen bis zurück zu SQL Server 2008 R2 (Kompatibilitätslevel 100) unterstützen.

## Best Practices für die Sicherheit

Um Daten weiter zu schützen, sollten IT-Teams sicherstellen, dass sie die Best Practices für die Sicherheit von SQL Server befolgen (weitere Informationen zu diesen Best Practices und Möglichkeiten zu ihrer Implementierung finden Sie im Microsoft-Blogbeitrag „Securing SQL Server“). Diese Best Practices für die Sicherheit gelten für alle Ebenen der Rechenzentrumsinfrastruktur, einschließlich Hardware und Betriebssystem, und umfassen Folgendes:

- **Erhöhen Sie die physische Sicherheit.** Physische Sicherheit schränkt den Zugriff auf die physischen Server- und Hardwarekomponenten strikt ein. Das bedeutet, dass verschlossene Räume mit eingeschränktem Zugang zu Servern und Netzwerkgeräten verwendet werden. Der Zugriff auf Backupmedien ist eingeschränkt, da diese an einem sicheren, externen Ort aufbewahrt werden. Dabei wird ein mehrstufiger Ansatz empfohlen: Verhinderung des Zugriffs oder Anforderung einer Schlüsselkarte/Genehmigung für den Zutritt zur Einrichtung und zum Gebäude, innerhalb des Gebäudes und auf der Etage des Rechenzentrums.
- **Halten Sie das Betriebssystem auf dem neuesten Stand.** Service Packs und Upgrades für das BS enthalten wichtige Sicherheitsverbesserungen. Updates und Upgrades für das BS können angewendet werden, nachdem sie mit Datenbankanwendungen getestet wurden.
- **Verwenden Sie Firewalls.** Firewalls erhöhen die Sicherheit auf Betriebssystemebene, indem sie einen Engpass bieten, an dem sich Sicherheitsmaßnahmen konzentrieren können.
- **Verkleinern Sie die Angriffsfläche.** Begrenzen Sie die Bereiche, die anfällig für Verstöße sind, indem Sie nicht verwendete Funktionen und Komponenten ausschalten oder deaktivieren. Die Angriffsfläche von SQL Server kann reduziert werden, indem die erforderlichen Dienste ausgeführt werden, die über die „geringsten Berechtigungen“ verfügen und Services und NutzerInnen Rechte auf der entsprechenden Ebene gewähren.
- **Implementieren Sie eine rollenbasierte Zugriffskontrolle (Role-Based Access Control, RBAC) für „sicherungsfähige Elemente“.**[3] Sicherungsfähige Elemente umfassen Komponenten wie den Server, die Datenbank und die in der Datenbank enthaltenen Objekte. Sicherungsfähige Elemente sind die Ressourcen, bei denen der Zugriff durch das Autorisierungssystem des SQL Server-Datenbankmoduls geregelt wird.
- **Verschlüsseln Sie Daten auf allen Ebenen.** Dazu gehört auch die Verschlüsselung von Anwendungs- und Storage-Daten.
- **Erstellen und nutzen Sie Zertifikate.** Zertifikate sind Softwareschlüssel, über die zwei Server sicher miteinander kommunizieren können.
  In SQL Server verbessern Zertifikate die Objekt- und Verbindungssicherheit.
- **Beschränken Sie den Zugriff auf BS-Dateien, die von SQL Server verwendet werden.**
- **Verwenden Sie im gesamten Unternehmen sichere Kennwörter.** Dies ist eine einfache, aber oft zu wenig priorisierte Sicherheitsmaßnahme.
- **Führen Sie Audits durch.** Stellen Sie sicher, dass die Recovery nach dem Backup wie erwartet funktioniert und der Zugriff entsprechend angewendet wird.
- **Verwenden Sie Microsoft Defender für SQL Server-Datenbanken.** Microsoft Defender für SQL Server-Datenbanken überprüft Datenbanken auf Sicherheitslücken. Das Tool erkennt Anomalien, die auf ungewöhnliche und potenziell schädliche Versuche hindeuten, auf Datenbanken zuzugreifen oder diese auszunutzen. Zu diesen Anomalien zählen verdächtige Datenbankaktivitäten, potenzielle Sicherheitslücken, SQL-Injektionsangriffe sowie anomale Datenbankzugriffe und Abfragemuster.

Schließlich enthält jede neue Version von SQL Server neue Sicherheitsfunktionen, die die Data Protection verbessern. Die neue Ledger-Funktion, die für SQL Server 2022 angekündigt wurde, trägt zum Schutz der Datenintegrität bei, indem sie eine unveränderliche Nachverfolgung der Datenänderungen im Laufe der Zeit erstellt. Dies kann dazu beitragen, Daten vor Manipulationen durch bösartige AkteurInnen zu schützen, und ist für Szenarien wie interne und externe Audits von Vorteil.

## SQL Server Ledger

- Verwendet einen unveränderlichen Ledger, um Daten vor Manipulationen durch bösartige AkteurInnen zu schützen
- Baut digitale Vertrauenswürdigkeit in einem zentralisierten System mithilfe der Blockchain-Technologie auf
- Bestätigt anderen Parteien, dass die Datenintegrität nicht beeinträchtigt wurde

## Konsolidierung und Schutz von der Hardware bis zur Datenbank

Die Rolle der IT wird mit dem Datenwachstum im digitalen Unternehmen weiter zunehmen. Da diese Fülle an Daten mit immer intelligenteren und häufigeren Cyberangriffen einhergeht, müssen IT-Teams eine Datensicherheitsstrategie verfolgen, die zum Schutz der Infrastruktur auf allen Ebenen beiträgt. Durch ein Upgrade auf die neueste Version von SQL Server und Windows Server auf Dell PowerEdge-Servern können Unternehmen sensible Unternehmens- und Kundendaten schützen.

**Verfolgen Sie einen sicherheitszentrierten Ansatz für Ihre Infrastruktur. Erfahren Sie mehr darüber, wie Lösungen von Dell und Microsoft Sie unterstützen können:** www.dell.com/en-us/dt/solutions/microsoft-data-platform/index.htm.

**Lesen Sie** „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“. März 2021.
[3] Weitere Informationen zu sicherungsfähigen Elementen finden Sie unter https://docs.microsoft.com/en-us/sql/relational-databases/security/securables.



DELL Technologies

Microsoft



Modernisierung mit Windows Server 2022.
Das Cloud-fähige Betriebssystem, das On-Premise-Investitionen mit hybriden Funktionen optimiert.