Weniger Datensicherheitslücken durch

eine 85 % schnellere Deaktivierung der vorderen USB-Anschlüsse

in iDRAC9 im Vergleich zum BMC von Anbieter K

Reduzierung der Kohlendioxidemissionen mit

25 anpassbaren Stromverbrauchsberichten

in OME im Vergleich zu 0 Berichten in der Enterprise-Managementkonsole von Anbieter K

Planung automatischer

Firmwareupdates in nur 41 Sekunden

in Dell APEX AIOps Infrastructure Observability (ehemals CloudIQ)

Mehr Sicherheit, Nachhaltigkeit und Managementeffizienz mit Dell Servermanagementtools

als bei vergleichbaren Servermanagementtools von Anbieter K

Mit den weiter wachsenden Rechenzentren nehmen auch die Aufgaben von AdministratorInnen zu. Eine Infrastruktur, die native robuste Management- und Monitoringtools mit Automatisierung bietet, kann das Sichern und Managen des Rechenzentrums für häufig überlastete AdministratorInnen zu einer einfacheren Aufgabe machen. Wir haben die Funktionen und Merkmale der Managementportfolios von Dell und einem Mitbewerber verglichen, den wir als Anbieter K bezeichnen:

Tabelle 1: Die von uns getesteten Managementtools

	Dell	Anbieter K
Integriertes/ Remoteservermanagement	Dell Technologies Integrated Dell Remote Access Controller 9 (iDRAC9)	Baseboard Management Controller (BMC) von Anbieter K
1:n-Geräte- und Konsolenmanagement	Dell Technologies OpenManage™ Enterprise (OME) APEX AIOps Infrastructure Observability (ehemals CloudIQ)	Enterprise-Managementkonsole von Anbieter K

Wir haben festgestellt, dass iDRAC9, OME und Dell APEX AIOps Infrastructure Observability (ehemals CloudIQ) robuste Managementtools bieten, die die Sicherheit verbessern, Nachhaltigkeitsmaßnahmen unterstützen und alltägliche Administratoraufgaben im Vergleich zu ähnlichen Tools von Anbieter K vereinfachen können.

Verstärkung der Rechenzentrumssicherheit

Unternehmen, die sensible Kundendaten speichern, müssen aufgrund der anhaltenden Bedrohung durch Cyberangriffe mit robusten End-to-End-Sicherheitsfunktionen sicherstellen, dass Daten nicht in die falschen Hände gelangen. Tatsächlich haben bis zu „83 % der Unternehmen im Jahr 2022 mehr als eine Datenschutzverletzung erlebt“,[1] eine Statistik, die unterstreicht, wie wichtig es ist, Vorsichtsmaßnahmen für Kundendaten zu ergreifen, um das Vertrauen von VerbraucherInnen zu steigern.

Um Ihr Unternehmen und seine Daten vor kostspieligen Cyberangriffen zu schützen, bieten Dell Managementtools robuste Sicherheitsfunktionen, die sowohl über iDRAC9 in den Server als auch in die übergreifende Konsolen- und Cloud-Managementsoftware integriert sind. Nachfolgend sehen wir uns einige der wichtigsten Sicherheitsfunktionen an, die Dell Tools zum Schutz Ihres Systems verwenden, und vergleichen sie mit den entsprechenden Angeboten von Anbieter K.

Integrierte Sicherheit

Über iDRAC9 sind Sicherheitsfunktionen in jeden Dell PowerEdge-Server integriert, die verhindern, dass böswillige AkteurInnen Zugriff auf Daten erhalten. Drei dieser wichtigen Funktionen sind:

- **Dynamische Systemsperre**: Die Systemsperre verhindert, dass unbeabsichtigte oder bösartige Aktivitäten zu Änderungen der System-BIOS-, iDRAC- und Firmwareeinstellungen führen. „Dynamisch“ bezieht sich auf die Möglichkeit, diese Funktionen einmal einzurichten und dann nach Bedarf zu implementieren. (Hinweis: Diese Funktion ist mit iDRAC9 Enterprise- und Datacenter-Lizenzen verfügbar.)
- **Multi-Faktor-Authentifizierung (MFA)**: Mit MFA müssen AdministratorInnen zusätzlich zu ihren Anmeldedaten einen Passcode eingeben, um die Sicherheit zu erhöhen.
- **Aktivierung/Deaktivierung des dynamischen USB-Anschlusses**: Durch das Deaktivieren und Aktivieren von USB-Anschlüssen können AdministratorInnen den Zugriff auf den Server über einen USB-Anschluss steuern. „Dynamisch“ bezieht sich auf die Möglichkeit, diese USB-Anschlüsse zu aktivieren und zu deaktivieren, ohne den Server oder das Betriebssystem neu starten zu müssen. Solange AdministratorInnen keinen Zugriff gewähren, kann niemand einen USB-Stick oder eine Tastatur anschließen, um Konfigurationseinstellungen des Systems, des Betriebssystems oder des BIOS zu ändern.

Wie in Tabelle 2 gezeigt, bietet Anbieter K keine dynamische Systemsperre oder MFA an. Zudem sind für die dynamischen USB-Funktionen Systemausfallzeiten erforderlich (was für Unternehmen sehr kostspielig sein kann), wodurch die Lösung weniger nützlich und teurer als die von Dell ist.

Tabelle 2: Vergleich der integrierten Sicherheitsfunktionen der Servermanagementtools. Quelle: Principled Technologies.

	iDRAC9	BMC von Anbieter K
Dynamische Systemsperre	✓	✗
MFA	✓	✗
Dynamisches USB	✓	✓*

** Systemausfallzeit erforderlich*

Informationen zu Dell Technologies Integrated Dell Remote Access Controller 9

Dell PowerEdge™-Server umfassen iDRAC9 mit Dell Lifecycle Controller, um Systemmanagementfunktionen bereitzustellen, die Systemwarnmeldungen und Remotemanagementfunktionen umfassen. Laut Dell bietet iDRAC9 u. a. die folgenden wichtigen Vorteile:

- Skalierbare Automatisierung mit standardbasierten APIs wie Redfish und robusten Scripting-Tools wie RedHat Ansible, Python, PowerShell und Terraform, mit denen Tausende von Servern gemanagt werden können
- Integrierter Support, der eine Ansicht der Serverintegrität und des Serverstatus bietet und Tausende von Parametern überwacht
- Robuste Sicherheitsfunktionen und -optionen[2]

Weitere Informationen zu den Funktionen von iDRAC9 finden Sie unter https://www.dell.com/en-us/lp/dt/open-manage-idrac.

In Abbildung 1 sind die Ergebnisse unseres praktischen Vergleichs beim dynamischen Deaktivieren von USB-Anschlüssen mit iDRAC9 und dem BMC von Anbieter K gezeigt.

Bei iDRAC9 haben wir festgestellt, dass AdministratorInnen die vorderen USB-Anschlüsse auf einem einzigen Server in nur 41 Sekunden mit 4 Schritten deaktivieren konnten. Im Vergleich dazu dauerte derselbe Prozess mit dem BMC von Anbieter K 4 Minuten und 43 Sekunden und umfasste 8 Schritte pro Server. Das bedeutet, dass **die Lösung von Dell pro Server 85 % weniger Zeit und die Hälfte der Schritte benötigt, um die vorderen USB-Anschlüsse zu deaktivieren**.[3] Wenn Sie in Betracht ziehen, diese Schritte in einem Rechenzentrum durchzuführen, summiert sich die Zeitersparnis. Bei einer Bereitstellung mit 100 Servern können AdministratorInnen mit iDRAC9 im Vergleich zum BMC von Anbieter K 6 Stunden und 43 Minuten einsparen.

Diese Funktionen sind mit iDRAC9 nicht nur einfacher und schneller zugänglich als mit dem BMC von Anbieter K, sondern AdministratorInnen können mit iDRAC9 auch Server in der Produktion halten (ohne Ausfallzeiten), während sie diese Funktionen aktivieren oder deaktivieren. Bei der Methode von Anbieter K ist eine Ausfallzeit erforderlich, die erhebliche Kosten verursachen kann. Außerdem muss die Systemkonfiguration jedes Mal geändert werden.

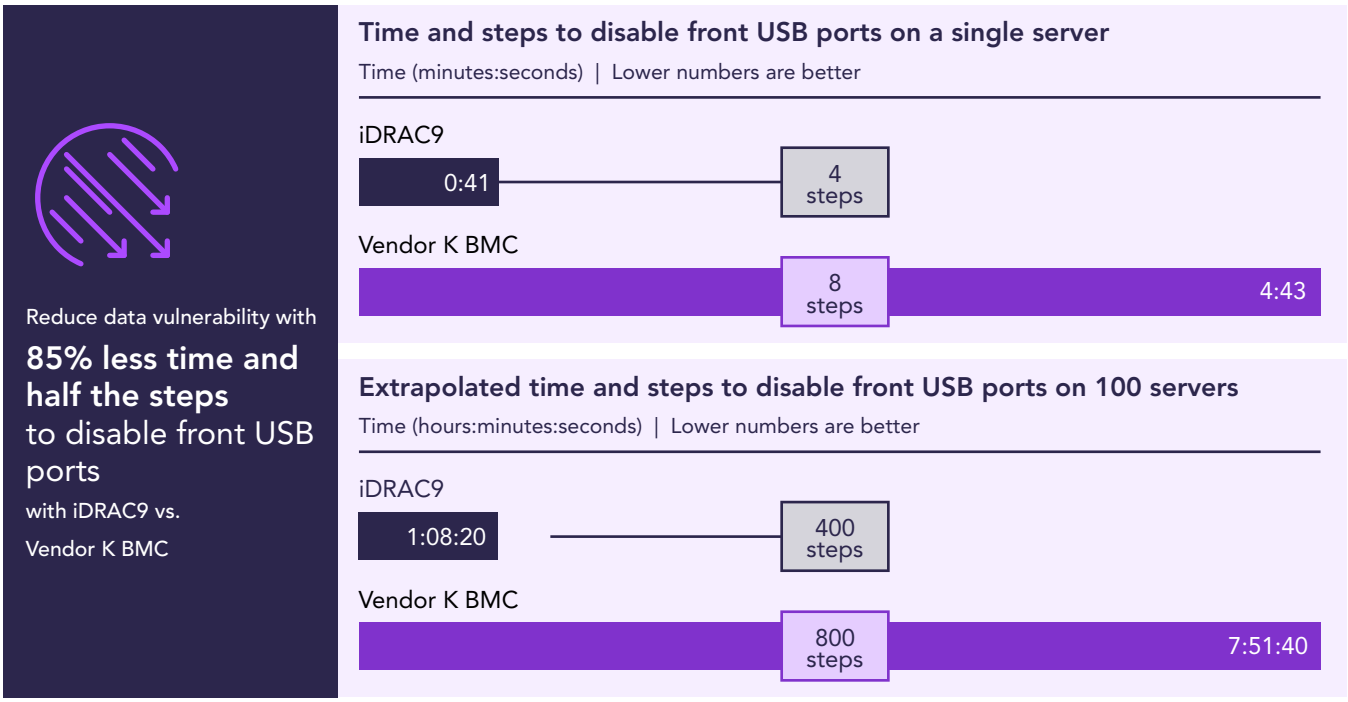

Abbildung 1: Zeit zum Deaktivieren der vorderen USB-Anschlüsse für einen einzelnen Server und hochgerechnete Zeit zum Deaktivieren der vorderen USB-Anschlüsse für 100 Server. Weniger Zeit und weniger Schritte sind besser. Quelle: Principled Technologies.

Sicherheit durch ein einfacheres Zugangsdatenmanagement in OME

OME bietet AdministratorInnen eine unkomplizierte Möglichkeit für das Management der iDRAC9-Kennwortrotation. Statt ein statisches, bekanntes Administratorkonto zu benötigen, managt OME iDRACs über ein Servicekonto, bei dem Kunden die erforderliche Kennwortrotationsrichtlinie auswählen, bei der das Kennwort nie offengelegt wird. Alternativ können AdministratorInnen das Management extern mit einem Drittanbieter durchführen. **Die Enterprise-Managementkonsole von Anbieter K verfügt nicht über interne Kennwortrotation, sodass AdministratorInnen sich auf einen Drittanbieter verlassen müssen, wenn sie diese Funktion nutzen möchten.** Wir haben bestätigt, dass mit iDRAC9 gemanagte Server in das OME-Konto integriert sind und vollständige Administratorrechte für ein einfacheres Zugangsdatenmanagement bieten.

Hinweis: In den Diagrammen in diesem Bericht werden unterschiedliche Skalierungen verwendet. Achten Sie beim Vergleich auf den Datenbereich jedes Diagramms.

Erreichen von Nachhaltigkeitszielen

Laut dem US-Energieministerium machen „Rechenzentren etwa 2 % des gesamten Stromverbrauchs in den USA aus, während der Kühlung im Rechenzentrum bis zu 40 % des Gesamtenergieverbrauchs im Rechenzentrum zuzuschreiben sind.“[4] Da Daten weiter stark zunehmen, werden diese Zahlen nur noch steigen, sodass das Temperatur- und Energiemanagement unerlässlich ist, um die Kosten für Rechenzentren niedrig zu halten und Nachhaltigkeitsziele zur Reduzierung der Kohlendioxidemissionen zu erreichen. Damit Unternehmen den Stromverbrauch reduzieren können, umfasst OME mehrere Funktionen für das Monitoring und Management des Stromverbrauchs. Tabelle 3 enthält die wichtigsten Vorteile dieser Funktionen, die weiter unten ausführlicher beschrieben sind.

Tabelle 3: Übersicht über die wichtigsten Nachhaltigkeitsmerkmale, die in OME verfügbar sind, im Vergleich zu den Merkmalen in der Enterprise-Managementkonsole von Anbieter K. Quelle: Principled Technologies.

Funktion	Wichtige Vorteile der Dell Managementtools	Nachteile der Managementtools von Anbieter K
Rechner für die Kohlendioxidemissionsnutzung und Kapazitätsplanungstool	Möglichkeit, **Treibhausgasemissionen** mit anpassbaren Werten zu schätzen, um Nachhaltigkeitsziele zu erreichen	**Keine vergleichbare Funktion** in der Enterprise-Managementkonsole von Anbieter K
Richtlinien für eine Stromobergrenze	**Management von Stromobergrenzen** für Geräte oder Gerätegruppen im OME Power Manager-Plug-in zum Erzwingen von Strombegrenzungen, wenn die Obergrenzen aktiviert sind	**Keine vergleichbare Funktion** in der Enterprise-Managementkonsole von Anbieter K
Automatisiertes Energie- und Temperaturmanagement	**Energie- und temperaturgesteuerte Richtlinienoptionen** mit der Möglichkeit zum Auslösen, wenn der Server einen Stromverbrauchs- oder Temperaturschwellenwert überschreitet	**Keine vergleichbare Funktion** in der Enterprise-Managementkonsole von Anbieter K
Dashboard für den Stromverbrauch	OME Power Manager-Plug-in-**Dashboard für den schnellen Zugriff** auf Power Manager-Daten und **mit 11 Kennzahlen 2,75-mal mehr Kennzahlen**	**Nur 4 Kennzahlen** im Dashboard der Enterprise-Managementkonsole von Anbieter K
Berichte zum Stromverbrauch	**25 verschiedene standardmäßige und zusätzliche anpassbare Berichte** im OME Power Manager-Plug-In	**Keine Energiemanagementberichte** in der Enterprise-Managementkonsole von Anbieter K
Energiemanagementkennzahlen	Bis zu **3-mal mehr Kennzahlen**, d. h. insgesamt **21 Kennzahlen**, die detailliertere Einblicke in das Stromverbrauchsmanagement bieten	**Nur 7 Kennzahlen** im Zusammenhang mit dem Energiemanagement in der Enterprise-Managementkonsole von Anbieter K

Automatisiertes Energie- und Temperaturmanagement

OME Power Manager bietet ein automatisiertes Energie- und Temperaturmanagement über statische energie- und temperaturgesteuerte Richtlinienoptionen, mit denen AdministratorInnen Grenzwerte für den Stromverbrauch oder Temperaturschwellenwerte festlegen können, um die Kühlkosten zu senken, die Strategien zur Reduzierung des Energieverbrauchs zu unterstützen und auf Temperaturereignisse zu reagieren. Im Gegensatz dazu **bietet Anbieter K keine automatisierte Energie- und Temperaturmanagementfunktion**. Ohne die Möglichkeit, temperaturbasierte Grenzwerte festzulegen, könnte der Energieverbrauch die Erwartungen übertreffen und eine nachhaltige Planung erschweren. Die Optimierung des Stromverbrauchs ist eine wichtige Strategie, um Nachhaltigkeitsziele zu erreichen. Das OME Power Manager-Plug-in bietet **25 standardmäßige und/oder anpassbare Power Manager-bezogene Berichte** (17 für Power Manager-Geräte und 8 weitere für Power Manager-Gruppen), mit denen AdministratorInnen die Kapazitätsplanung optimieren und den Stromverbrauch managen können, um die Effizienz zu maximieren. **Die Enterprise-Managementkonsole von Anbieter K bietet keine ähnlichen Energiemanagementberichte** (siehe Abbildung 2).

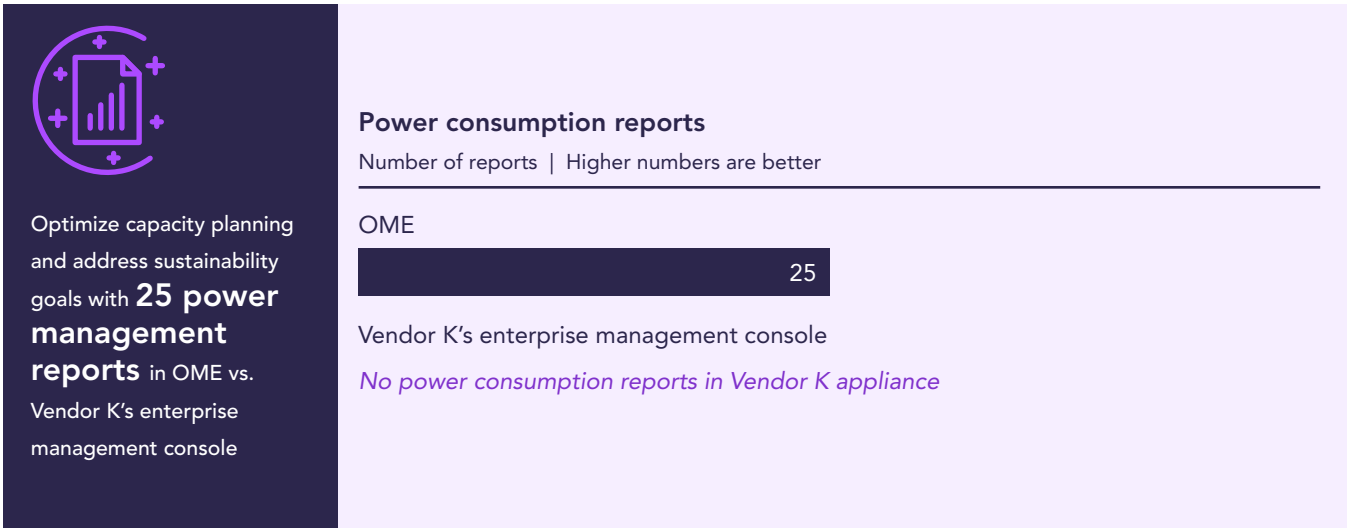

Abbildung 2: Vergleich der Anzahl der Energiemanagementberichte, die in OME und der Enterprise-Managementkonsole von Anbieter K verfügbar sind. Mehr Berichte sind besser. Quelle: Principled Technologies

Um das Energiemanagement weiter zu optimieren, können AdministratorInnen mit dem OME Power Manager-Plug-in bis zu **3-mal mehr Kennzahlen im Vergleich zur Enterprise-Managementkonsole von Anbieter K** anzeigen (siehe Abbildung 3). OME bietet 21 verschiedene Kennzahlen, einschließlich Stromverbrauch durch einzelne Komponenten, Luftstrom und Komponentenauslastung, während die Enterprise-Managementkonsole von Anbieter K nur 7 verschiedene Kennzahlen bereitstellt.

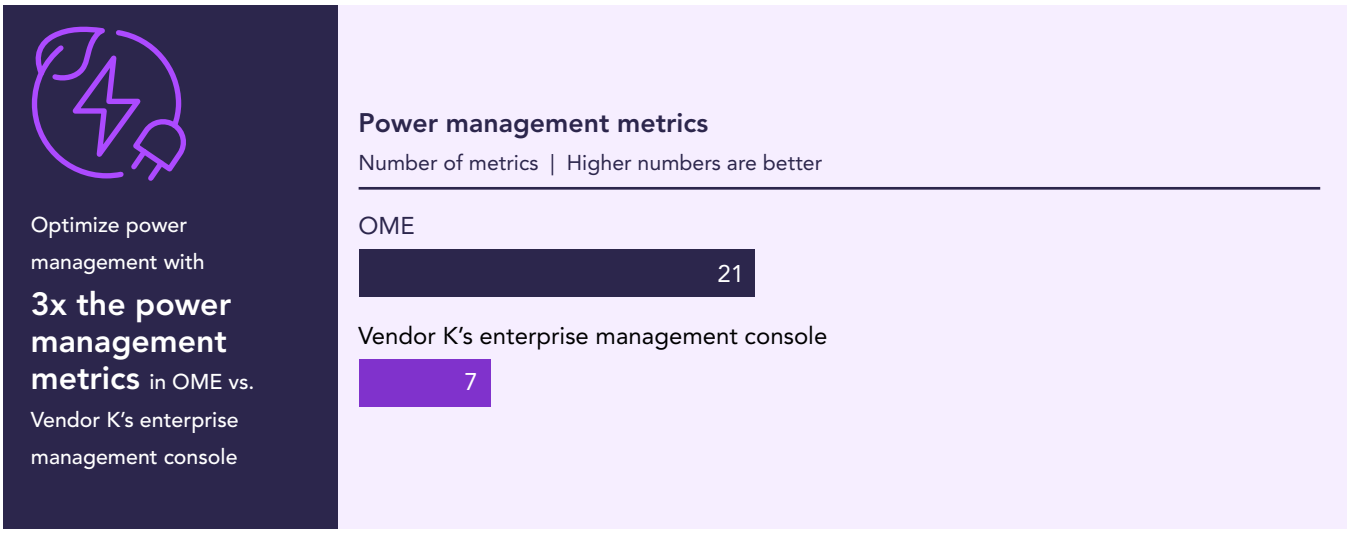

Abbildung 3: Vergleich der Anzahl der Energiemanagementkennzahlen, die in OME und der Enterprise-Managementkonsole von Anbieter K verfügbar sind. Mehr Kennzahlen sind besser. Quelle: Principled Technologies.

Analyse der Kohlendioxidemissionen und des CO_2-Fußabdrucks

Eine wichtige Nachhaltigkeitsfunktion von **OME ist ein Tool für die Berechnung der Kohlendioxidemissionsnutzung und die Kapazitätsplanung**. Mit diesem Tool können Unternehmen ihre Treibhausgasemissionen schätzen und Standardwerte für Stromkosten und Kohlendioxidemissionen pro verbrauchter Energieeinheit bereitstellen. Diese Funktion ermöglicht außerdem eine Anpassung, sodass Unternehmen Werte für die Stromkosten und Kohlendioxidemissionen ihrer eigenen Region für die Daten eingeben können, die für das Nutzungsmodell ihres Rechenzentrums spezifisch sind. **Die Enterprise-Managementkonsole von Anbieter K bietet keine vergleichbare Funktion**, was Unternehmen eine auf Nachhaltigkeit ausgelegte Planung erschweren kann.

Weniger Managementaufwand durch robuste Monitoring- und Managementfunktionen

In einer wachsenden Infrastruktur können auch die Verantwortlichkeiten von RechenzentrumsadministratorInnen zunehmen. Durch die Auswahl von Servermanagementtools, die bestimmte Aufgaben automatisieren und das alltägliche Management verbessern, können Unternehmen AdministratorInnen dabei unterstützen, effizienter zu arbeiten und mehr Zeit für die Planung der Zukunft aufzuwenden. Wir haben festgestellt, dass das Servermanagementportfolio von Dell eine Reihe von Funktionen bietet, die Administratoraufgaben vereinfachen können. Tabelle 4 enthält eine Zusammenfassung der wichtigsten nutzerfreundlichen Funktionen, die im Dell Managementportfolio im Vergleich zu den Managementtools von Anbieter K verfügbar sind.

Tabelle 4: Übersicht über die wichtigsten nutzerfreundlichen Funktionen der Managementtools von Dell im Vergleich zu den Managementtools von Anbieter K. Quelle: Principled Technologies.

Funktion	Wichtige Vorteile der Dell Managementtools	Nachteile der Managementtools von Anbieter K
Mehr Remote-BIOS-Funktionen	Einfacheres Remotemanagement mit **51 Remote-BIOS-Funktionen in iDRAC9**.	Der BMC von Anbieter K bietet **nur 1** Remote-BIOS-Funktion.
Einfachere BIOS-Konfigurationsänderungen	Für eine Änderung der BIOS-Konfiguration sind **87 % weniger Zeit und die Hälfte der Schritte** erforderlich.	Bei Anbieter K sind **manuelle Administratoreingriffe** erforderlich, um Änderungen innerhalb der Systemdienstprogramme vorzunehmen.
Importieren/Exportieren der vollständigen Serverkonfiguration	**Schnellere Konfiguration mehrerer identischer Server** mit der Möglichkeit, Konfigurationseinstellungen für einen vollständig konfigurierten Server zu exportieren/importieren.	Anbieter K bietet **nur Backup und Wiederherstellung des BMC für jeden einzelnen Server**.
Automatisierte geplante Updates	iDRAC9 ermöglicht AdministratorInnen die **Planung automatisierter Updates** von einem Repository während eines Wartungsfensters ohne zusätzliche Administratoreingriffe.	Der BMC von Anbieter K **bietet keine geplanten automatisierten Updates**.
Umfassende Übersicht über den Storage-Status	iDRAC9 bietet eine visuelle Darstellung des Storage-Status für die **schnelle Identifizierung von Laufwerken mit Warnmeldungsstatus**.	Der BMC von Anbieter K stellt **keine** ähnliche Ansicht bereit.
Telemetrie-Streaming	iDRAC9 **bietet Telemetrie für 2-mal so viele Kennzahlenkategorien, insgesamt 8**.	Der BMC von Anbieter K stellt Telemetrie für **nur 4 Kategorien** bereit.
Verbindungsanzeige	Die Verbindungsanzeige in iDRAC9 **bietet Details zur physischen Zuordnung von Switchports zu den Netzwerkports des Servers und zu dedizierten iDRAC-Portverbindungen**.	Der BMC von Anbieter K stellt **keine physischen Verbindungsinformationen** zu Upstreamswitches bereit.
Skalierbarkeit	OME **kann bis zu 8.000 Geräte** managen.[5]	Anbieter K kann **nur** bis zu **1.000 Geräte** managen.

Funktion	Wichtige Vorteile der Dell Managementtools	Nachteile der Managementtools von Anbieter K
Warnmeldungsbasierte Aktionen	OME bietet **2-mal mehr warnmeldungsbasierte Aktionen (insgesamt 12)**, die Aktionen basierend auf der Eingabe einer Warnmeldung auslösen.	Anbieter K stellt nur **4 warnmeldungsbasierte Aktionen** bereit.
Plug-in-Architektur	OME bietet die Möglichkeit, **die Funktionalität mit Plug-ins zu erweitern**, die AdministratorInnen der Konsole hinzufügen können, ohne dass zusätzliche Anwendungen verwaltet werden müssen	Die Enterprise-Managementkonsole von Anbieter K **bietet keine Plug-in-basierte Architektur** für Erweiterbarkeit
Monitoring von Drittanbietergeräten	OME **unterstützt das Monitoring von Drittanbietergeräten und -servern**.	Die Enterprise-Managementkonsole von Anbieter K **unterstützt kein** Monitoring von Drittanbietergeräten und -servern
Berichterstellung	OME bietet AdministratorInnen **42 integrierte Berichte** mit Anpassung, sodass AdministratorInnen die wichtigsten Daten für ihre Zwecke granular auswählen können	Die Enterprise-Managementkonsole von Anbieter K stellt **keine native Berichterstellung** bereit.

Remotemanagement

Mit iDRAC9 müssen AdministratorInnen nicht bei jeder Änderung das Rechenzentrum betreten. iDRAC9 bietet 51 Remote-BIOS-Funktionen, damit AdministratorInnen mehr Änderungen außerhalb des Rechenzentrums vornehmen können, im Vergleich zu nur einer Funktion im BMC von Anbieter K. Damit profitieren AdministratorInnen von überall aus von einer deutlich feiner abgestimmten Kontrolle über die BIOS-Konfiguration (siehe Abbildung 4).

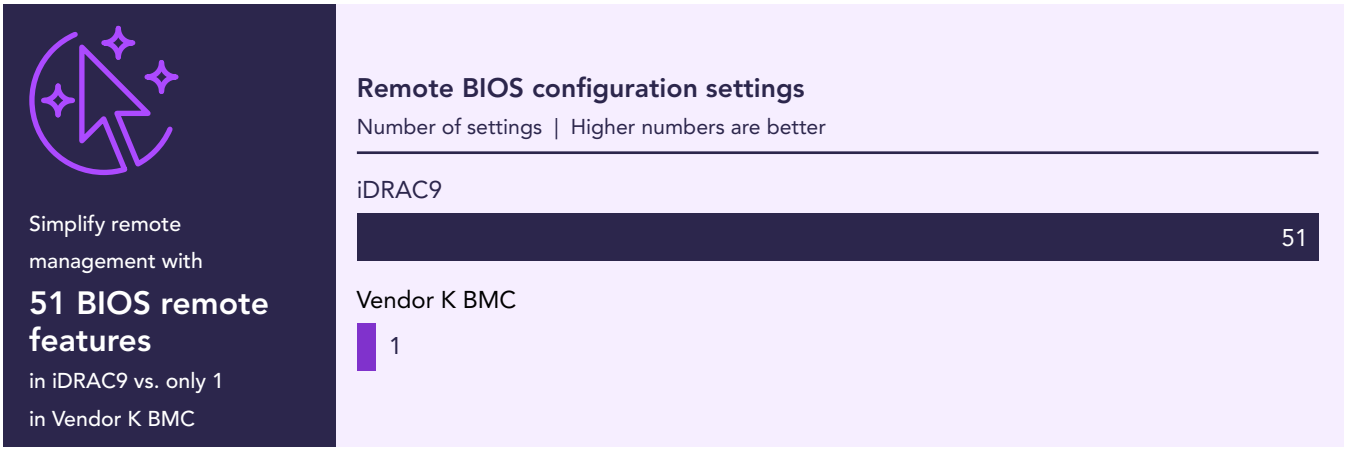

Abbildung 4: Vergleich der BIOS-Remotefunktionen, die das jeweilige Managementtool bietet. Mehr Funktionen sind besser. Quelle: Principled Technologies.

Durchführung von Konfigurationsänderungen

Mit iDRAC9 können AdministratorInnen BIOS-Konfigurationseinstellungen ändern und das Update für einen späteren Neustart bereitstellen, ohne dass AdministratorInnen anwesend sein müssen. Beim BMC von Anbieter K müssen Änderungen dagegen innerhalb der Systemdienstprogramme durchgeführt werden, was bedeutet, dass während der Änderung manuelle Administratoreingriffe erforderlich sind. Wie in Abbildung 5 gezeigt, nahm die Bereitstellung der BIOS-Konfigurationsänderung für einen geplanten Neustart mit iDRAC9 im Vergleich zum BMC von Anbieter K 87 % weniger Zeit und die Hälfte der Schritte in Anspruch. Wenn Sie diese Einsparungen auf große Bereitstellungen hochrechnen, wachsen die Zeiteinsparungen für AdministratorInnen. Bei einer 100-Server-Bereitstellung können AdministratorInnen beispielsweise mehr als 6 Stunden beim Ändern von BIOS-Konfigurationselementen einsparen.

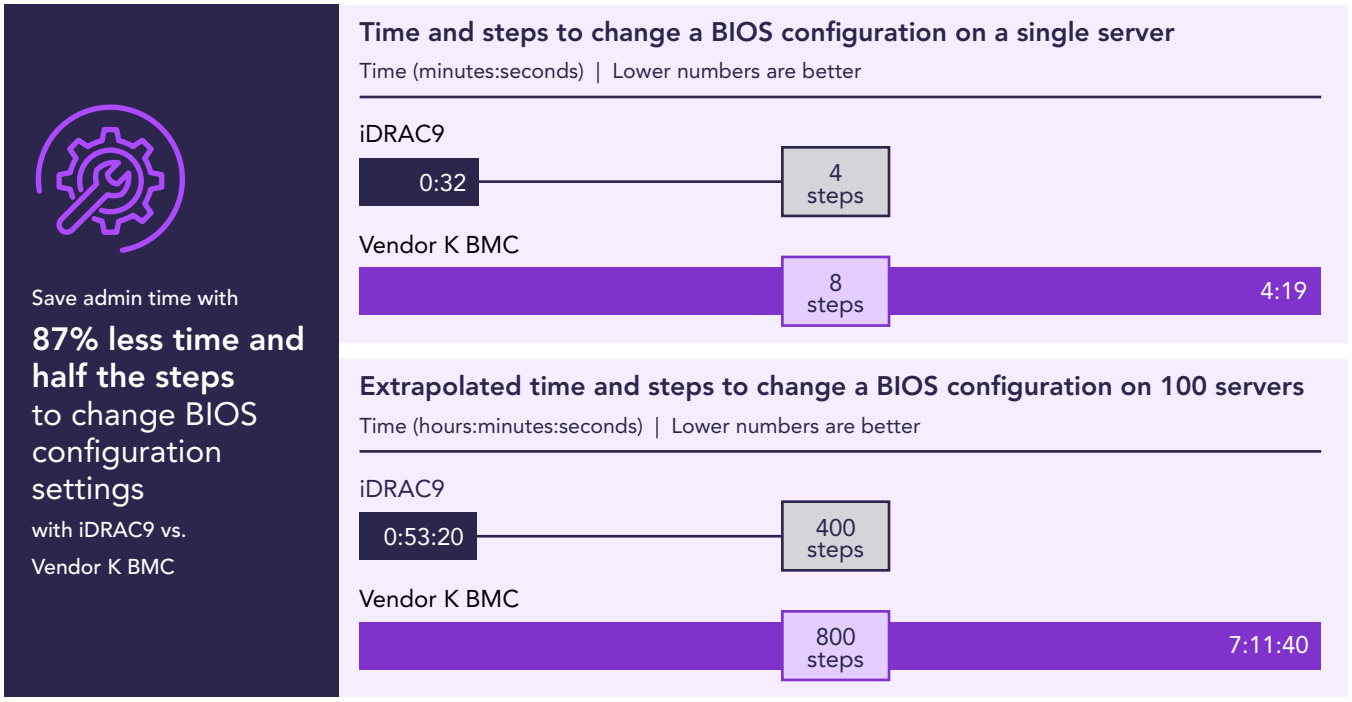

Abbildung 5: Erforderliche Zeit für die Änderung der BIOS-Konfigurationseinstellungen und die Bereitstellung des Updates für einen späteren Neustart für einen einzelnen Server und hochgerechnete Zeit für 100 Server. Weniger Zeit und weniger Schritte sind besser. Quelle: Principled Technologies.

Einrichtung von warnmeldungsbasierten Aktionen

AdministratorInnen können ihre Zeit besser nutzen, wenn sie beim Monitoring der Integrität der Umgebung nicht an einen Schreibtisch gebunden sind. Wie in Abbildung 6 gezeigt, bietet OME 12 richtliniengesteuerte Optionen für warnmeldungsbasierte Aktionen, sodass die Problemkorrektur automatisch gestartet wird, wenn die Umgebung bestimmte Schwellenwerte erreicht. Im Gegensatz dazu können AdministratorInnen mit der Enterprise-Managementkonsole von Anbieter K nur 4 warnmeldungsbasierte Ereignisse konfigurieren.

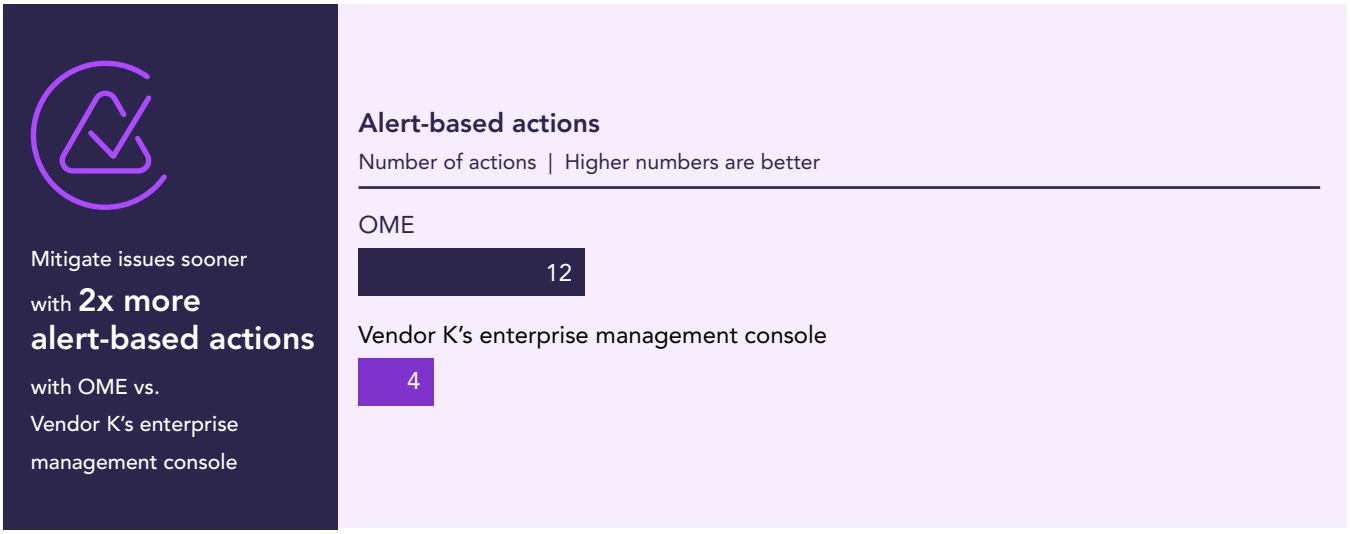

Abbildung 6: Vergleich der warnmeldungsbasierten Aktion, die das jeweilige Managementtool bietet. Mehr Aktionen sind besser. Quelle: Principled Technologies.

Informationen zu Dell Technologies OpenManage Enterprise

OME ist eine 1:n-Systemmanagementkonsole für das Rechenzentrum. Die Konsole bietet eine moderne grafische HTML5-Benutzeroberfläche und wird als virtuelle Appliance für VMware ESXi™-, Microsoft Hyper-V- und KVM-Umgebungen (kernelbasierte virtuelle Maschine) bereitgestellt. OME kann IPV4- und IPV6-Netzwerke für bis zu 8.000 Geräte ermitteln und inventarisieren, einschließlich Dell Rack-Server, Dell Tower-Server sowie Dell Blades und Gehäuse.[6] In einer kürzlich durchgeführten PT-Studie haben wir festgestellt, dass eine Dell Umgebung mit OME und OpenManage Enterprise Modular (OME-M) Zeit bei Änderungen an VLANs einsparen und Interventionen während geplanter Firmwareupdates vermeiden kann.[7]

Weitere Informationen zu OME finden Sie unter https://www.dell.com/en-us/lp/dt/open-manage-enterprise.

Cloudbasiertes Management mit Dell APEX AIOps Infrastructure Observability (ehemals CloudIQ)

Integrierte Tools und Enterprise-Managementkonsolen sind nicht die einzigen Tools im Dell Servermanagementportfolio. Mit Dell APEX AIOps Infrastructure Observability (ehemals CloudIQ) erhalten AdministratorInnen eine weitere nutzerfreundliche und automatisierte Möglichkeit, die Integrität und Sicherheit ihrer Infrastruktur unter Kontrolle zu halten – diesmal über die Cloud.

Zusätzliche Sicherheitsfunktionen in Dell APEX AIOps Infrastructure Observability (ehemals CloudIQ)

Dell APEX AIOps Infrastructure Observability (ehemals CloudIQ) bietet mehrere Sicherheitsfunktionen, die den Schutz Ihres Unternehmens vor Angriffen weiter stärken. In Tabelle 5 sind einige dieser wichtigsten Sicherheitsfunktionen gezeigt.

Tabelle 5: Übersicht über die wichtigsten Sicherheitsfunktionen, die in Dell APEX AIOps Infrastructure Observability (ehemals CloudIQ) verfügbar sind. Quelle: Principled Technologies.

Funktion	So schützt Dell APEX AIOps Infrastructure Observability (ehemals CloudIQ) Ihre Umgebung
Warnmeldungen auf Cybersicherheitsrisiko-Ebene	Automatisierte Einblicke in die Cybersicherheit mit **spezifischen Warnmeldungen auf Sicherheitsrisikoebene**, damit AdministratorInnen schneller reagieren und Probleme schnell beheben können, um ihre Daten zu schützen
Richtlinienbasierte Sicherheitskonfiguration	**Richtlinienbasierte Sicherheitskonfigurationseinstellungen und einfach anzuwendende Vorlagen**, mit denen AdministratorInnen sicherstellen können, dass Best-Practice-Einstellungen für die Sicherheit vorhanden sind, um die PowerEdge-Umgebung zu schützen
Cybersicherheitsratgeber	**Relevante Sicherheitsratgeber** mit Details zu spezifischen Sicherheitslücken und Empfehlungen zur Korrektur, sodass schnelle Maßnahmen zum Schließen von Sicherheitslücken ergriffen werden können

Informationen zu Dell APEX AIOps Infrastructure Observability (ehemals CloudIQ)

Dell APEX AIOps Infrastructure Observability (ehemals CloudIQ) ist ein cloudbasiertes AIOps-Tool, das „proaktives Monitoring, maschinelles Lernen und vorausschauende Analysen" für eine große Anzahl von Dell Produkten und Services bietet, darunter Server, Storage, Data Protection Appliances und hyperkonvergente Infrastruktur.[8] In einer Studie von Principled Technologies aus dem Jahr 2022 haben wir festgestellt, dass CloudIQ vernachlässigbare Auswirkungen auf die Netzwerkbandbreite hatte und es uns gleichzeitig ermöglichte, Telemetrie, Integritätsstatus, Warnmeldungen und Bestandsaufnahme über eine einzige Konsole zu überwachen.[9]

Weitere Informationen zu Dell APEX AIOps Infrastructure Observability (ehemals CloudIQ) finden Sie unter https://www.dell.com/en-us/dt/apex/aiops.htm.

Zusätzliche Nachhaltigkeits- und Effizienzfunktionen in Dell APEX AIOps Infrastructure Observability (ehemals CloudIQ)

Dell APEX AIOps Infrastructure Observability (ehemals CloudIQ) bietet Funktionen, die Nachhaltigkeit und Effizienz fördern und in iDRAC9 und OME integriert sind, um AdministratorInnen das Monitoring der Integrität ihrer PowerEdge-Umgebung zu erleichtern. In Tabelle 6 sind einige dieser Funktionen gezeigt.

Tabelle 6: Übersicht über die in Dell APEX AIOps Infrastructure Observability (ehemals CloudIQ) verfügbaren Funktionen für Nachhaltigkeit und ein nutzerfreundliches Management. Quelle: Principled Technologies.

Funktion	Wichtige Vorteile von Dell APEX AIOps Infrastructure Observability (ehemals CloudIQ)
Analyse des CO_2-Fußabdrucks	Bessere Übersicht und **Prognose der Kohlendioxidemissionen** in allen Umgebungen mit diesem Tool im Abschnitt „Monitoring"
Performanceansichten	Performanceansichten und Diagramme zu Anomalien und Auslastung, mit denen **AdministratorInnen beim ersten Anzeichen von Problemen gewarnt werden**
Kundenspezifische Complianceberichte	Möglichkeit für NutzerInnen, **kundenspezifische Complianceberichte** für ausgewählte Geräte zu erstellen
Anpassbare Performance- und Bestandsberichte	**Kundenspezifische Reportingoptionen** für Serverperformance- und Bestandsdaten, sodass AdministratorInnen mehr Kontrolle über die Performance- und Gerätekennzahlen haben, die sie verfolgen möchten
Planung von Energiemaßnahmen	Durchführung von Energiemaßnahmen wie eine Strombegrenzung auf mehreren überwachten Dell PowerEdge-Servern in **nur 35 Sekunden und 6 Schritten**
Planung von Firmwareupdates	Planung von PowerEdge-Firmwareupdates für mehrere überwachte Server in **nur 41 Sekunden und 9 Schritten**

Entscheidung

In unserem Vergleich der Sicherheits-, Nachhaltigkeits- und Management-/Monitoringfunktionen haben wir festgestellt, dass das Portfolio der Dell Servermanagementtools robustere Management- und Monitoringfunktionen bietet als das Portfolio von Anbieter K. Im Bereich der Sicherheit stellt iDRAC9 mehr Funktionen bereit, einschließlich dynamischer Systemsperre und Multi-Faktor-Authentifizierung, die bei Anbieter K gar nicht verfügbar sind. Darüber hinaus ermöglicht iDRAC9 eine wesentlich schnellere Deaktivierung von USB-Anschlüssen, um Datensicherheitslücken zu reduzieren.

Dank Tools für die Analyse des CO_2-Fußabdrucks und ein robustes Energiemanagement unterstützt OME unseren Ergebnissen zufolge Unternehmen besser bei der Planung von Nachhaltigkeitszielen als die Enterprise-Managementkonsole von Anbieter K. Darüber hinaus haben wir festgestellt, dass das Servermanagementportfolio von Dell mehr Automatisierungs- und Remotemanagementoptionen bietet, wodurch der Zeit- und Arbeitsaufwand für AdministratorInnen bei bestimmten Routineaufgaben für Monitoring und Wartung reduziert wird. Diese Vorteile in den Bereichen Sicherheit, Nachhaltigkeit und Management-/Monitoringfunktionen machen das Servermanagementportfolio von Dell zu einer attraktiven Option für Unternehmen, die sich ein effizienteres und sichereres Rechenzentrum wünschen.

---

1. Harvard Business Review, „The Devastating Business Impacts of a Cyber Breach", abgerufen am 10. April 2024, https://hbr.org/2023/05/the-devastating-business-impacts-of-a-cyber-breach.
2. Dell, „Integrated Dell Remote Access Controller (iDRAC)", abgerufen am 17. Mai 2024, https://www.dell.com/en-us/lp/dt/open-manage-idrac.
3. Hinweis: Die Deaktivierung des USB-Anschlusses von Anbieter K ist anpassbar. Dies bedeutet jedoch, dass AdministratorInnen den Anschluss für die Deaktivierung einzeln statt nach Gruppe auswählen müssen.
4. DOE, „DOE Announces $40 Million for more Efficient Cooling for Data Centers", abgerufen am 20. Mai 2024, https://www.energy.gov/articles/doe-announces-40-million-more-efficient-cooling-data-centers.
5. Dell, „OpenManage Enterprise – Supportmatrix", abgerufen am 21. Mai 2024, https://www.dell.com/support/kbdoc/en-us/article/lkbprint?ArticleNumber=000217909&AccessLevel=10&Lang=en.
6. Dell, „OpenManage Enterprise", abgerufen am 17. Mai 2024, https://www.dell.com/en-us/work/learn/openmanage-enterprise.
7. Principled Technologies, „A Dell PowerEdge MX Environment using OpenManage Enterprise and OpenManage Enterprise Modular CAN make Life Easy for Administrators", abgerufen am 17. Mai 2024, https://www.principledtechnologies.com/Dell/PowerEdge-MX-OME-OME-M-0124.pdf.
8. Dell, „APEX AIOps: Bewältigung der IT-Komplexität in Ihrem digitalen Unternehmen", abgerufen am 11. Juni 2024, https://www.dell.com/en-us/dt/apex/aiops.htm.
9. Principled Technologies, „Dell CloudIQ provides a single console for proactive monitoring and had negligible impact on network bandwidth in our tests", abgerufen am 9. April 2024, https://www.principledtechnologies.com/dell/CloudIQ-network-0422.pdf.

Lesen Sie den wissenschaftlichen Hintergrund dieses Berichts

Lesen Sie die Originalversion dieses Berichts in englischer Sprache

Principled Technologies®

Facts matter.®

Dieses Projekt wurde in Auftrag gegeben von Dell Technologies.