



Verminder
datakwetsbaarheid met
**85% minder tijd om
USB-poorten aan
de voorzijde uit te
schakelen**

*in iDRAC9 versus BMC van
leverancier K*



Help de CO2-uitstoot te
beperken met
**25 aanpasbare
rapporten over
energieverbruik**

*in OME versus 0 rapporten in
de bedrijfsbeheerconsole van
leverancier K*



Automatische planning van
**firmware-updates in
slechts 41 seconden**

*in APEX AIOps Infrastructure
Observability (voorheen CloudIQ)*

Dell serverbeheertools kunnen helpen de beveiliging, duurzaamheid en efficiëntie van beheer te verbeteren

vergeleken met vergelijkbare serverbeheertools
van leverancier K

Naarmate datacenters blijven groeien, groeien ook de taken van beheerders. Infrastructuur die beschikt over robuuste beheer- en bewakingstools met automatisering, kan het beveiligen en beheren van het datacenter een eenvoudigere taak maken voor beheerders die vaak overbelast zijn. We hebben de functies en mogelijkheden van de beheerportefeuilles van Dell en een concurrent die we leverancier K noemen, vergeleken:

Tabel 1: De beheertools die we hebben getest.

	Dell	Leverancier K
Geïntegreerd/extern serverbeheer	Support voor Integrated Dell Remote Access Controller 9 (iDRAC9) van Dell Technologies	Baseboard Management Controller (BMC) van leverancier K
Eén-naar-veel apparaat- en consolebeheer	Dell Technologies OpenManage™ Enterprise (OME) APEX AIOps Infrastructure Observability (voorheen CloudIQ)	Enterprise Management Console van leverancier K

We ontdekten dat iDRAC9, OME en APEX AIOps Infrastructure Observability (voorheen CloudIQ) een krachtige reeks beheertools boden die de beveiliging konden verbeteren, konden helpen bij duurzaamheidsmaatregelen en dagelijkse beheertaken konden vereenvoudigen in vergelijking met vergelijkbare tools van leverancier K.

Versterking van de beveiliging van datacenters

Voor organisaties die gevoelige klantdata opslaan, vereist de aanhoudende dreiging van cyberaanvallen sterke end-to-end beveiligingsfuncties om ervoor te zorgen dat data niet in verkeerde handen terechtkomen. Sterker nog, tot '83% van de organisaties ervaart meer dan één datalek in 2022'¹, een statistiek die benadrukt hoe belangrijk het is om voorzorgsmaatregelen te nemen met klantdata om het vertrouwen van de consument te vergroten.

Om uw organisatie en haar data te beschermen tegen kostbare cyberaanvallen, bieden de beheertools van Dell sterke beveiligingsfuncties, zowel geïntegreerd in de server via iDRAC9 als in overkoepelende console- en cloudbeheerssoftware. Hieronder bekijken we enkele van de belangrijkste beveiligingsfuncties die Dell tools gebruiken om uw systeem te beschermen en vergelijken we deze met het bijbehorende aanbod van leverancier K.

Ingebouwde beveiliging

In elke Dell PowerEdge server via iDRAC9 zijn beveiligingsfuncties ingebouwd die ervoor zorgen dat kwaadwillenden geen toegang krijgen tot data. Drie van deze belangrijke functies zijn:

- **Dynamic System Lockdown:** System Lockdown voorkomt dat onbedoelde of schadelijke activiteit de BIOS-, iDRAC- en firmware-instellingen van het systeem wijzigt. Dynamisch verwijst naar de mogelijkheid om deze mogelijkheden eenmaal in te stellen en vervolgens naar behoefte uit te voeren. (Opmerking: Deze functie is beschikbaar met iDRAC9 Enterprise- en Datacenter-licenties.)
- **Meervoudige verificatie (MFA):** MFA vraagt beheerders om een toegangscode naast hun aanmeldingsreferenties om de beveiliging te versterken.
- **Dynamisch USB-poorten inschakelen/uitschakelen:** Door USB-poorten uit te schakelen en in te schakelen, hebben beheerders controle over de toegang tot de server via een USB-poort. Dynamisch verwijst naar de mogelijkheid om deze USB-poorten in en uit te schakelen zonder de server opnieuw op te starten of het besturingssysteem opnieuw op te starten. Totdat de beheerder toegang biedt, kan niemand een geheugenstick of toetsenbord aansluiten om configuratie-instellingen van het systeem, het besturingssysteem of het BIOS te wijzigen.

Zoals tabel 2 laat zien, bood leverancier K geen dynamische systeembeveiliging of MFA, en hun dynamische USB-capaciteiten vereisen systeemonderbreking (wat erg kostbaar kan zijn voor organisaties), waardoor het minder nuttig en duurder is dan de Dell oplossing.

Tabel 2: Vergelijking van de geïntegreerde beveiligingsfuncties die de serverbeheertools bieden. Bron: Principled Technologies.

	iDRAC9	BMC van leverancier K
Dynamische systeemvergrendeling	✓	✗
MFA	✓	✗
Dynamisch USB	✓	✓*

*Vereist downtime van het systeem

Over Dell Technologies Integrated Dell Remote Access Controller 9

Dell PowerEdge™ servers bevatten iDRAC9 met Dell Lifecycle Controller om systeembeheerfuncties te bieden, waaronder systeemwaarschuwingen en mogelijkheden voor extern beheer. Volgens Dell zijn de belangrijkste voordelen van iDRAC9:

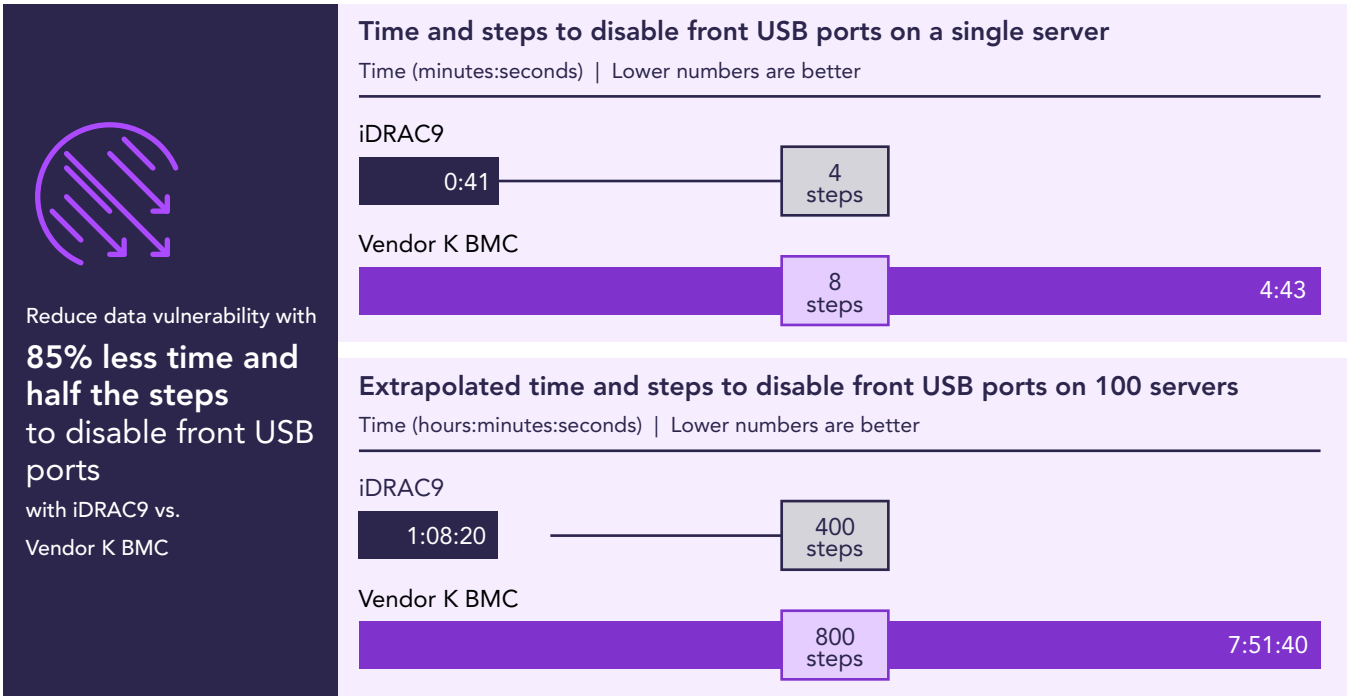
- Schaalbare automatisering. Met op standaarden gebaseerde API's zoals Redfish en robuuste scriptingtools zoals RedHat Ansible, Python, PowerShell, Terraform kunt u duizenden servers beheren.
- Geïntegreerde support, met een weergave van de serverstatus en statusbewaking met duizenden parameters
- Krachtige beveiligingsfuncties en -opties²

Ga naar <https://www.dell.com/en-us/lp/dt/open-manage-idrac> voor meer informatie over de functies die iDRAC9 biedt.

Afbeelding 1 toont de resultaten van onze praktische vergelijking tussen iDRAC9 en Vendor K BMC om USB-poorten dynamisch uit te schakelen.

Met behulp van iDRAC9 vonden we dat beheerders USB-poorten aan de voorzijde op één server konden uitschakelen in slechts 41 seconden en 4 stappen. In vergelijking met de leverancier K van BMC zou hetzelfde proces 4 minuten 43 seconden en 8 stappen per server in beslag nemen. Dit betekent dat per server **de Dell oplossing 85 procent minder tijd en de helft van de stappen kost om USB-poorten aan de voorzijde uit te schakelen.**³ Wanneer u deze stappen in een datacenter uitvoert, levert dat een flinke tijdsbesparing op. Voor een implementatie van 100 servers kunnen beheerders met iDRAC9 6 uur en 43 minuten besparen vergeleken met BMC van leverancier K.

Niet alleen zijn deze functies eenvoudiger en sneller toegankelijk met iDRAC9 dan met BMC van leverancier K, maar met iDRAC9 kunnen beheerders de servers in productie houden (geen downtime) terwijl ze deze functies in- of uitschakelen. Bij de methode van leverancier K is er sprake van downtime, wat aanzienlijke kosten met zich mee kan brengen. Bovendien moet u telkens wijzigingen in de configuratie van de systeeminstellingen doorvoeren.



Afbeelding 1: Tijd om USB-poorten aan de voorzijde uit te schakelen voor één server en geëxtrapoleerde tijd om USB-poorten aan de voorzijde uit te schakelen voor 100 servers. Minder tijd en minder stappen zijn beter. Bron: Principled Technologies.

Veilig blijven met eenvoudiger aanmeldingsbeheer in OME

OME biedt beheerders een eenvoudige manier om iDRAC9-wachtwoordrotatie te beheren. In plaats van een statisch, bekend beheerdersaccount te vereisen, beheert OME iDRAC's via een serviceaccount waarin klanten het vereiste wachtwoordrotatiebeleid selecteren (waarvoor het wachtwoord nooit wordt vrijgegeven). Beheerders kunnen het ook extern beheren met een derde partij. **De Enterprise Management Console van leverancier K heeft geen interne wachtwoordrotatiecapaciteiten, waardoor beheerders moeten vertrouwen op een derde partij als ze deze functionaliteit willen.** We hebben bevestigd dat door iDRAC9 beheerde servers zijn geïntegreerd met het OME-account met volledige beheerdersrechten voor eenvoudiger aanmeldingsbeheer.

Duurzaamheidsdoelstellingen behalen

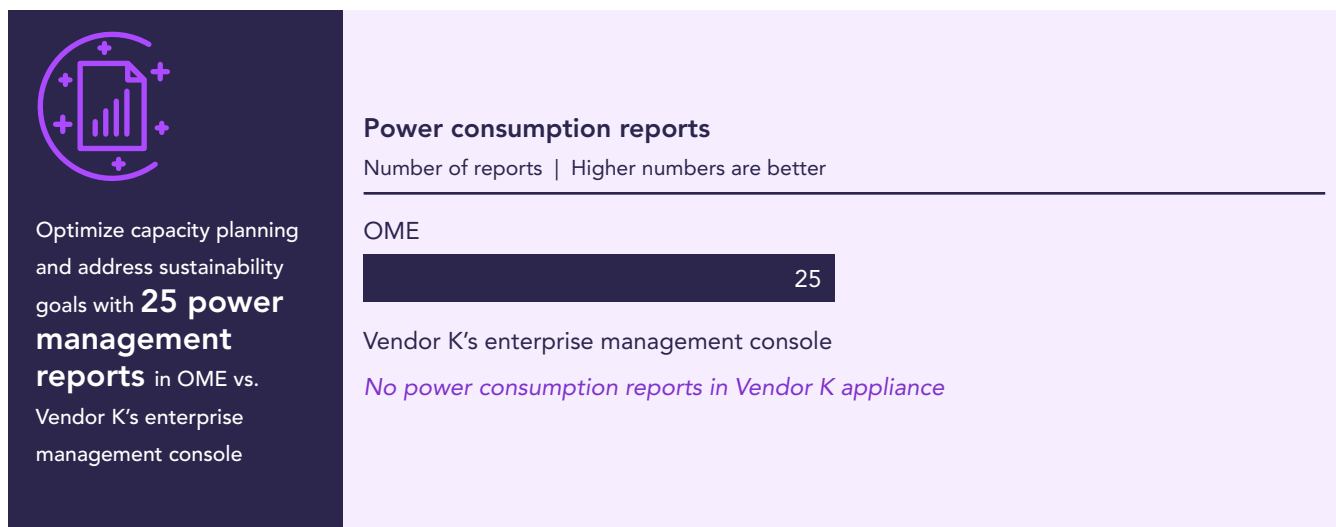
Volgens het Amerikaanse Department of Energy: "datacenters zijn verantwoordelijk voor ongeveer 2% van het totale elektriciteitsverbruik in de VS, terwijl koeling van datacenters verantwoordelijk kan zijn voor maximaal 40% van het totale energieverbruik van datacenters."⁴ Naarmate data blijven groeien, zullen deze aantallen alleen maar toenemen, waardoor thermisch en energiebeheer van vitaal belang is om de kosten van datacenters laag te houden en duurzaamheidsdoelstellingen te behalen om de CO2-uitstoot te helpen beperken. Om organisaties te helpen het energieverbruik te verminderen, bevat OME verschillende functies voor het bewaken en beheren van het energieverbruik. Tabel 3 toont de belangrijkste voordelen van deze functies, die we hieronder in meer detail beschrijven.

Tabel 3: Overzicht van belangrijke duurzaamheidsfuncties die beschikbaar zijn in OME versus de Enterprise Management Console van leverancier K.
Bron: Principled Technologies.

Functie	Belangrijkste voordelen van Dell beheertools	Nadeel met beheertools van leverancier K
 Calculator voor het gebruik van koolstofemissies en capaciteitsplanningstool	Mogelijkheid om uitstoot van broeikasgassen te schatten met aanpasbare waarden om duurzaamheidsdoelstellingen te bereiken	De Enterprise Management Console van leverancier K biedt geen vergelijkbare functie
 Beleid voor stroomaftopping	OME Power Manager plug-in kan stroomaftopping beheren voor apparaten of groepen apparaten die stroomlimieten afdwingen wanneer deze zijn ingeschakeld	De Enterprise Management Console van leverancier K biedt geen vergelijkbare functie
 Geautomatiseerd energie- en thermisch beheer	Beleidsopties die worden geactiveerd door energie en temperatuur met de optie om te activeren wanneer de server een drempelwaarde voor energieverbruik of temperatuur overschrijdt	De Enterprise Management Console van leverancier K biedt geen vergelijkbare functie
 Dashboard voor energieverbruik	Het OME Power Manager plugin- dashboard biedt snelle toegang tot Power Manager-data, met 2,75x de statistieken, met 11 statistieken	De Enterprise Management Console van leverancier K biedt slechts 4 statistieken op het dashboard
 Rapporten over energieverbruik	De OME Power Manager plug-in biedt 25 verschillende standaard en aanvullende aanpasbare rapporten	De Enterprise Management Console van leverancier K biedt geen energiebeheerrapporten
 Statistieken voor energiebeheer	Tot 3x meer statistieken , met meer gedetailleerd inzicht in energieverbruiksbeheer met 21 statistieken	De Enterprise Management Console van leverancier K biedt slechts 7 statistieken met betrekking tot energiebeheer

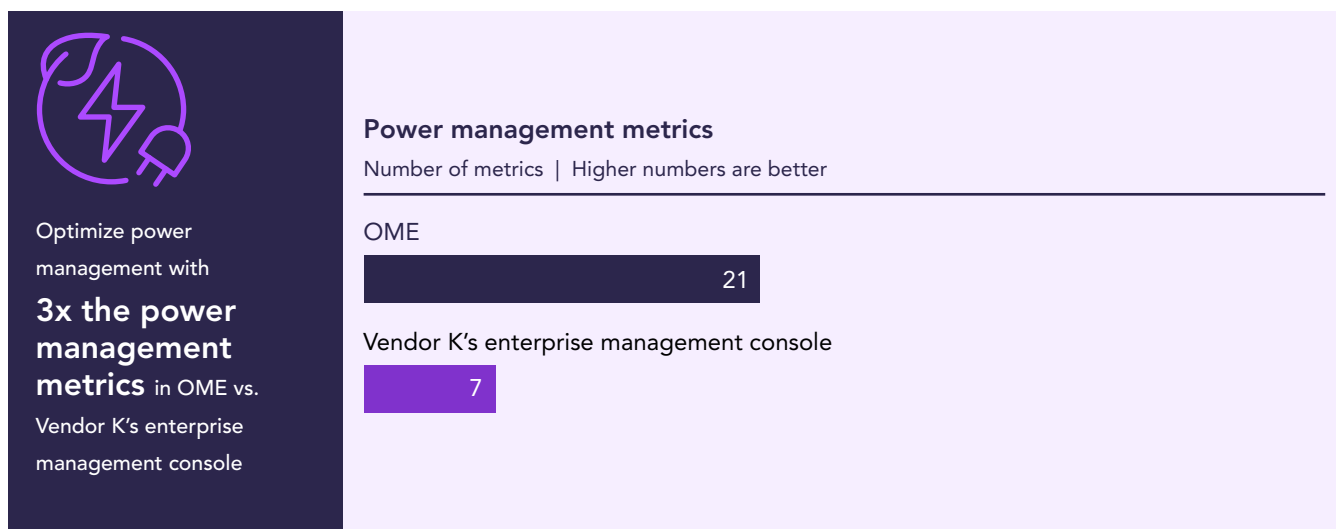
Geautomatiseerd energie- en thermisch beheer

OME Power Manager biedt geautomatiseerd energie- en thermisch beheer via zowel statische energie- als temperatuurgeactiveerde beleidsopties waarmee beheerders limieten voor energieverbruik of temperatuurdrempels kunnen instellen om de koelingskosten te verlagen, energiebesparingsstrategieën te ondersteunen en te reageren op thermische gebeurtenissen. Daarentegen **biedt Leverancier K biedt geen geautomatiseerde functie voor energie- en thermisch beheer**. Zonder de mogelijkheid om temperatuurlimieten in te stellen, kan het energieverbruik de verwachtingen overtreffen en het moeilijk maken om te plannen met duurzaamheid in gedachten. Het optimaliseren van het energieverbruik is een belangrijke strategie voor het behalen van duurzaamheidsdoelstellingen. De OME Power Manager plug-in biedt **25 standaard- en/of aanpasbare Power Manager-gerelateerde rapporten** (17 in Power Manager-apparaten en nog eens 8 in Power Manager-groepen) waarmee beheerders de capaciteitsplanning kunnen optimaliseren en het stroomverbruik kunnen beheren om de efficiëntie te maximaliseren. **De Enterprise Management Console van leverancier K biedt geen vergelijkbare energiebeheerrapporten** (zie afbeelding 2).



Afbeelding 2: Vergelijking van het aantal beschikbare energiebeheerrapporten in OME en de Enterprise Management Console van leverancier K. Meer rapporten zijn beter. Bron: Principled Technologies

Om het energiebeheer verder te optimaliseren, kunnen beheerders met de OME Power Manager plug-in tot **3x meer statistieken bekijken in vergelijking met de bedrijfsbeheerconsole van leverancier K** (zie afbeelding 3). OME biedt 21 verschillende statistieken, waaronder energieverbruik per afzonderlijke componenten, luchtstroom en componentgebruik, terwijl de Enterprise Management Console van leverancier K slechts 7 verschillende statistieken biedt.



Afbeelding 3: Vergelijking van het aantal statistieken voor energiebeheer dat beschikbaar is in de bedrijfsbeheerconsole van OME en leverancier K. Meer statistieken zijn beter. Bron: Principled Technologies.

Analyse van CO2-uitstoot en CO2-voetafdruk

Een belangrijke duurzaamheidsfunctie **die OME omvat, is een calculator voor CO2-uitstoot en een tool voor capaciteitsplanning**. Deze tool helpt organisaties bij het schatten van hun uitstoot van broeikasgassen en biedt standaardwaarden voor energiekosten en koolstofuitstoot per verbruikte eenheid energie. Deze functie maakt ook aanpassing mogelijk, zodat organisaties waarden kunnen invoeren voor de energiekosten en CO2-uitstoot van hun eigen regio voor data die specifiek zijn voor het verbruiksmodel van hun datacenter. **De Enterprise Management Console van leverancier K heeft geen vergelijkbare functie**, wat het vermogen van een organisatie om te plannen met duurzaamheid in gedachten kan belemmeren.

Verminder de beheerlast met robuuste bewakings- en beheerfuncties

Naarmate de infrastructuur groeit, kunnen de verantwoordelijkheden van de beheerder van het datacenter ook toenemen. Door te kiezen voor serverbeheertools die bepaalde taken automatiseren en het dagelijkse beheer verbeteren, kunnen organisaties beheerders helpen efficiënter te worden en hen meer tijd geven om te plannen voor de toekomst. We hebben vastgesteld dat het Dell serverbeheerportfolio een aantal functies bood die beheerderstaken kunnen vereenvoudigen. Tabel 4 bevat een overzicht van de belangrijkste gebruiksvriendelijke functies die beschikbaar zijn in het Dell beheerportfolio versus de beheertools van leverancier K.

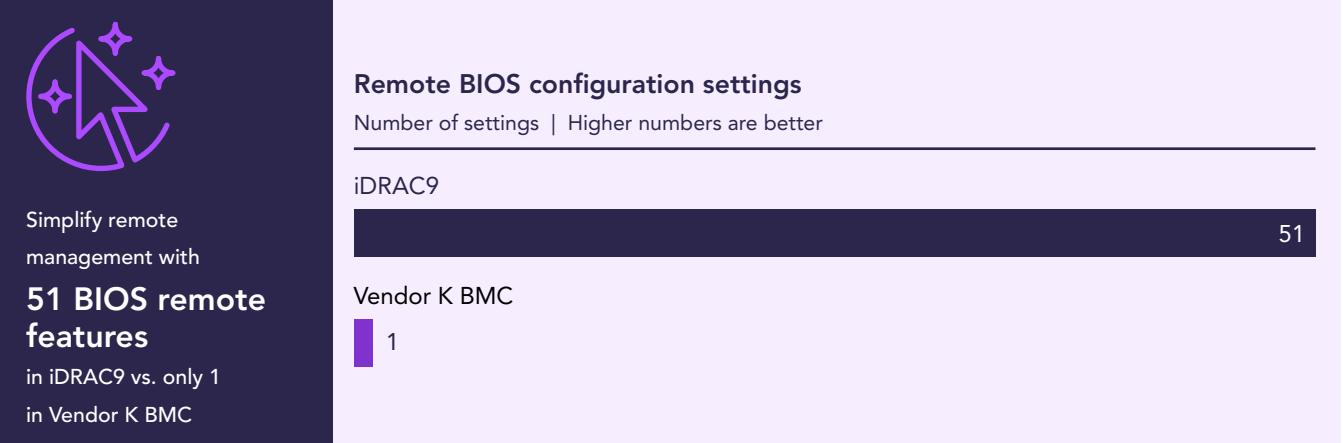
Tabel 4: Overzicht van de belangrijkste gebruiksvriendelijke functies die beschikbaar zijn in de beheertools van Dell versus de beheertools van leverancier K. Bron: Principled Technologies.

Functie	Belangrijkste voordelen van Dell beheertools	Nadeel met beheertools van leverancier K
 Meer externe BIOS-functies	Eenvoudiger extern beheer met 51 externe BIOS-functies in iDRAC9	Leverancier K BMC biedt slechts 1 externe BIOS-functie
 Eenvoudigere BIOS-configuratiewijzigingen	87% minder tijd en de helft van de stappen om een BIOS-configuratiewijziging aan te brengen	Leverancier K vereist handmatige beheerinterventie om wijzigingen aan te brengen vanuit de systeemhulpprogramma's
 Volledige serverconfiguratie importeren/exporteren	Snellere configuratie van meerdere identieke servers met de mogelijkheid om configuratie-instellingen voor een volledig geconfigureerde server te exporteren/importeren	Leverancier K biedt alleen back-up en herstel van de BMC voor elke afzonderlijke server
 Geautomatiseerde geplande updates	iDRAC9 biedt beheerders de mogelijkheid om geautomatiseerde updates vanuit een repository te plannen tijdens een onderhoudsvenster zonder extra tussenkomst van de beheerder	BMC van leverancier K biedt geen geplande geautomatiseerde updates
 Uitgebreid overzicht van storagestatus	iDRAC9 biedt een visuele weergave van de storagestatus, voor het snel identificeren van schijven met een waarschuwingsstatus	BMC van leverancier K biedt geen vergelijkbare weergave
 Telemetriestreaming	iDRAC9 biedt telemetrie voor 2x zoveel metrische categorieën, met in totaal 8 categorieën	BMC van leverancier K biedt telemetrie voor slechts 4 categorieën
 Connection View	Connection View in iDRAC9 biedt details over de fysieke toewijzing van switchpoorten aan netwerkpoorten van de server en aan speciale iDRAC-poortverbindingen	BMC van leverancier K heeft geen informatie over fysieke verbindingen naar upstream switches
 Schaalbaarheid	OME kan tot 8.000 apparaten beheren ⁵	Leverancier K kan maximaal 1.000 apparaten beheren

Functie	Belangrijkste voordelen van Dell beheertools	Nadeel met beheertools van leverancier K
 Acties op basis van waarschuwingen	OME biedt 2x meer op waarschuwingen gebaseerde acties (met 12) die acties activeren op basis van invoer van een waarschuwing	Leverancier K biedt slechts 4 op waarschuwingen gebaseerde acties
 Plug-inarchitectuur	OME biedt de mogelijkheid om functionaliteit uit te breiden met plug-ins die beheerders aan de console kunnen toevoegen zonder dat er extra applicaties hoeven te worden beheerd	De Enterprise Management Console van leverancier K biedt geen plug-inarchitectuur voor uitbreidbaarheid
 Bewaking van apparaten van derden	OME ondersteunt apparaat- en serverbewaking van derden	De Enterprise Management Console van leverancier K biedt geen ondersteuning voor apparaat- en serverbewaking van derden
 Rapportage	OME biedt beheerders 42 geïntegreerde rapporten met aanpassingen, zodat beheerders gedetailleerder de belangrijkste data voor hun doeleinden kunnen selecteren	De Enterprise Management Console van leverancier K heeft geen systeemeigen rapportage-aanmaakfunctie

Extern beheer

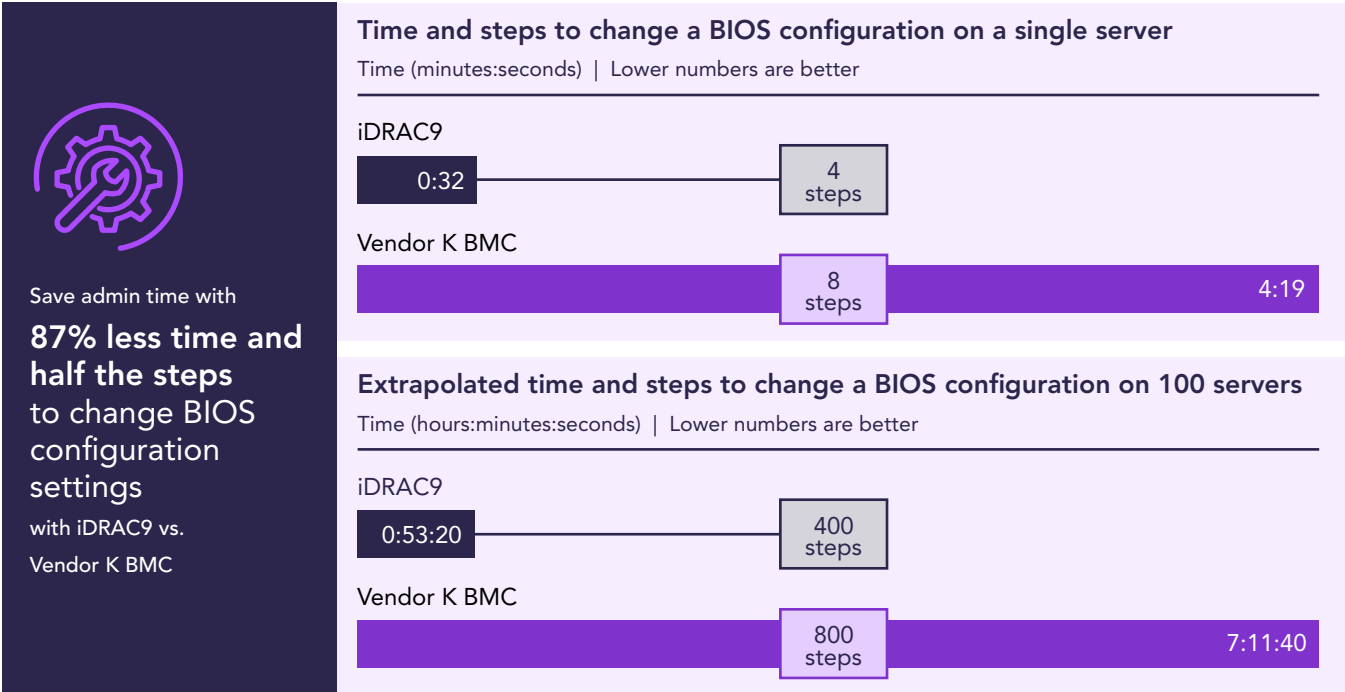
Met iDRAC9 hoeven beheerders niet bij elke wijziging het datacenter binnen te komen. IDRAC9 biedt 51 externe BIOS-functies om beheerders de vrijheid te geven om meer wijzigingen van buiten het datacenter aan te brengen, vergeleken met slechts één voor BMC van leverancier K, waardoor beheerders vanaf elke locatie aanzienlijk meer gedetailleerde controle over de BIOS-configuratie krijgen (zie afbeelding 4).



Afbeelding 4: Vergelijking van externe BIOS-functies die elke beheertool biedt. Meer functies zijn beter. Bron: Principled Technologies.

Configuratiewijzigingen aanbrengen

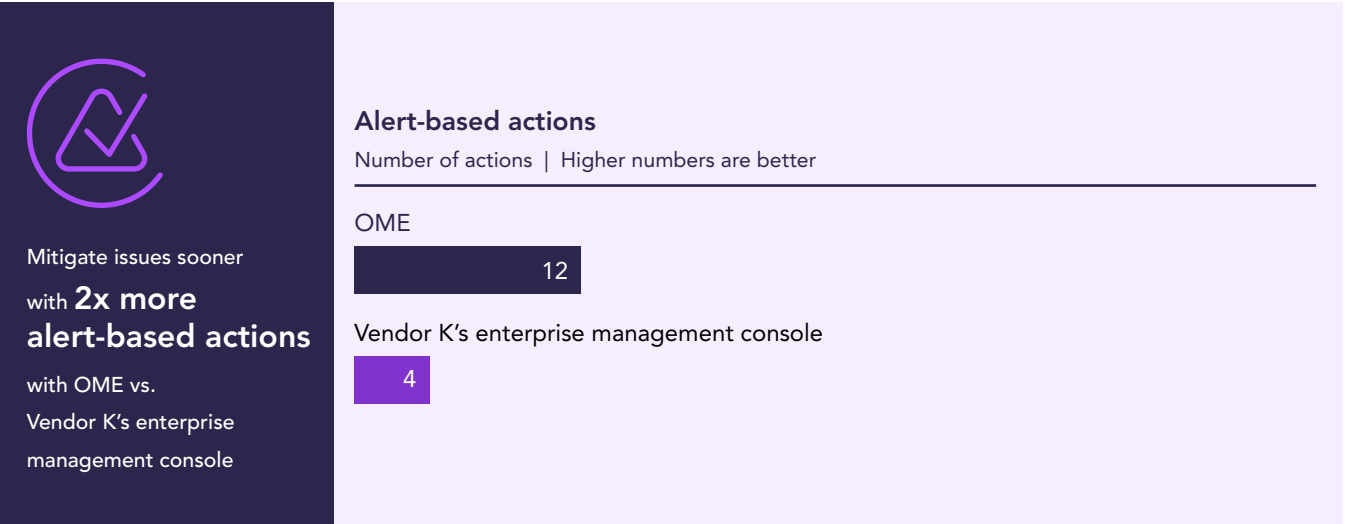
Met iDRAC9 kunnen beheerders BIOS-configuratie-instellingen wijzigen en de update voor een latere herstart voorbereiden zonder dat er extra beheerdersaanwezigheid nodig is, terwijl BMC van leverancier K wijzigingen vereist vanuit de systeemhulpprogramma's en handmatige beheerdersinterventie tijdens de wijziging. Zoals afbeelding 5 laat zien, nam het faseren van de BIOS-configuratiewijziging voor een geplande herstart met iDRAC9 87 procent minder tijd in beslag dan met BMC van leverancier K. Wanneer u deze besparingen extrapoleert naar grote implementaties, neemt de tijdsbesparing voor beheerders toe. In een implementatie van 100 servers kunnen beheerders bijvoorbeeld meer dan 6 uur besparen bij het wijzigen van BIOS-configuratie-items.



Afbeelding 5: Tijd om de BIOS-configuratie-instellingen te wijzigen en de update te faseren voor een latere herstart van een enkele server en geëxtrapoleerde tijd voor 100 servers. Minder tijd en minder stappen zijn beter. Bron: Principled Technologies.

Acties op basis van waarschuwingen instellen

Beheerders kunnen hun tijd beter benutten wanneer ze niet aan een bureau gebonden zijn, en de status van de omgeving bewaken. Zoals afbeelding 6 laat zien, biedt OME 12 beleidsgestuurde opties voor op waarschuwingen gebaseerde acties, zodat probleembeperving automatisch wordt gestart wanneer de omgeving bepaalde drempels bereikt. In tegenstelling hiermee kunnen beheerders met de Enterprise Management Console van leverancier K slechts vier gebeurtenissen op basis van waarschuwingen configureren.



Afbeelding 6: Vergelijking van de op waarschuwingen gebaseerde actie die elke beheertool biedt. Meer acties zijn beter. Bron: Principled Technologies.

Over Dell Technologies OpenManage Enterprise

OME is een één-naar-veel systeembeheerconsole voor het datacenter. De console biedt een moderne grafische HTML5-gebruikersinterface en kan worden geïmplementeerd als een virtueel apparaat voor VMware ESXi™-, Microsoft Hyper-V- en Kernel-based Virtual Machine (KVM)-omgevingen. OME kan IPV4- en IPV6-netwerken detecteren en inventariseren voor maximaal 8.000 apparaten, waaronder Dell rackservers, Dell towerservers en Dell blades en chassis.⁶ In een recent PT-onderzoek hebben we vastgesteld dat een Dell omgeving met OME en OpenManage Enterprise Modular (OME-M) tijd kan besparen bij het aanbrengen van wijzigingen in VLAN's en interventies tijdens geplande firmware-updates kan helpen voorkomen.⁷

Meer informatie over OME vindt u op <https://www.dell.com/en-us/lp/dt/open-manage-enterprise>.

Cloudgebaseerd beheer met APEX AIOps Infrastructure Observability (voorheen CloudIQ)

Geïntegreerde tools en bedrijfsbeheerconsole's zijn niet de enige tools in het Dell serverbeheerportfolio. Met APEX AIOps Infrastructure Observability (voorheen CloudIQ) krijgen beheerders een andere gebruiksvriendelijke, geautomatiseerde manier om de status en beveiliging van hun infrastructuur onder controle te houden, dit keer vanuit de cloud.

Aanvullende beveiligingsfuncties beschikbaar in APEX AIOps Infrastructure Observability (voorheen CloudIQ)

APEX AIOps Infrastructure Observability (voorheen CloudIQ) biedt verschillende beveiligingsfuncties die uw organisatie verder kunnen versterken tegen aanvallen. Tabel 5 geeft een aantal van deze belangrijke beveiligingsfuncties weer.

Tabel 5: Overzicht van de belangrijkste beveiligingsfuncties die beschikbaar zijn in APEX AIOps Infrastructure Observability (voorheen CloudIQ). Bron: Principled Technologies.

Functie		Hoe APEX AIOps Infrastructure Observability (voorheen CloudIQ) werkt om uw omgeving te beveiligen
	Waarschuwingen voor cyberbeveiligingsrisico's	Biedt geautomatiseerde inzichten voor cyberbeveiliging met specifieke waarschuwingen voor beveiligingsrisico's , zodat beheerders sneller kunnen reageren en problemen snel kunnen aanpakken om data veilig te houden
	Op beleid gebaseerde beveiligingsconfiguratie	Biedt op beleid gebaseerde beveiligingsconfiguratie-instellingen en eenvoudig toe te passen sjablonen waarmee een beheerder kan zorgen voor best practices voor beveiliging, waardoor de PowerEdge omgeving wordt beschermd
	Cyberbeveiligingsadvies	Biedt relevante rapporten over beveiligingsadviezen , met specifieke informatie over beveiligingslekken en suggesties voor herstel, zodat u snel actie kunt ondernemen om eventuele beveiligingslekken te dichten

Over APEX AIOps Infrastructure Observability (voorheen CloudIQ)

APEX AIOps Infrastructure Observability (voorheen CloudIQ) is een cloudgebaseerde AIOps-tool die 'proactieve bewaking, machine learning en voorspellende analyses' biedt voor een groot aantal Dell producten en services, waaronder servers, storage, databeschermingsapparaten en hyperconverged infrastructuur.⁸ In een onderzoek van Principled Technologies uit 2022 ontdekten we dat CloudIQ een verwaarloosbare impact had op de netwerkbandbreedte, terwijl we telemetrie, status, waarschuwingen en inventaris konden bewaken vanaf één console.⁹

Meer informatie over APEX AIOps Infrastructure Observability (voorheen CloudIQ) vindt u op <https://www.dell.com/en-us/dt/apex/aiops.htm>.

Aanvullende duurzaamheids- en efficiëntiefuncties beschikbaar in APEX AIOps Infrastructure Observability (voorheen CloudIQ)

APEX AIOps Infrastructure Observability (voorheen CloudIQ) biedt ook functies die duurzaamheid en efficiëntie versterken en integreren met iDRAC9 en OME om het voor beheerders gemakkelijker te maken om de status van hun PowerEdge omgeving te bewaken. Tabel 6 geeft een aantal van deze functies weer.

Tabel 6: Overzicht van duurzaamheids- en gebruiksbeheerfuncties die beschikbaar zijn in APEX AIOps Infrastructure Observability (voorheen CloudIQ). Bron: Principled Technologies.

Functie	Belangrijkste voordelen van APEX AIOps Infrastructure Observability (voorheen CloudIQ)
 Analyse van de CO2-voetafdruk	Deze tool bevindt zich in het gedeelte Monitoring en biedt een hoger overzicht van en kan de CO2-uitstoot in alle omgevingen voorspellen
 Prestatieweergaven	Biedt prestatieweergaven en anomalieën en gebruiksgrafieken om beheerders te waarschuwen bij de eerste tekenen van problemen
 Aangepaste nalevingsrapporten	Biedt gebruikers de mogelijkheid om aangepaste nalevingsrapporten te maken voor geselecteerde apparaten
 Aanpasbare prestatie- en inventarisrapporten	Biedt aangepaste rapportageopties voor serverprestaties en inventarisdata, waardoor beheerders meer controle krijgen over de prestaties en apparaatstatistieken die ze willen bijhouden
 Energiebeheertaken plannen	Voer in slechts 35 seconden en 6 stappen energiebeheeracties uit, zoals energiebegrenzing op meerdere bewaakte Dell PowerEdge servers
 Firmware-updates plannen	Plan PowerEdge firmware-updates voor meerdere bewaakte servers in slechts 41 seconden en 9 stappen

Conclusie

In onze vergelijking van beveiligings-, duurzaamheids- en beheer-/bewakingsfuncties hebben we vastgesteld dat het portfolio van Dell serverbeheertools robuustere beheer- en bewakingsfuncties bood dan het portfolio van leverancier K. Op het gebied van beveiliging bood iDRAC9 meer functies, waaronder dynamische systeemvergrendeling en meervoudige verificatie, die leverancier K helemaal niet bood. Bovendien heeft iDRAC9 de tijd om USB-poorten uit te schakelen aanzienlijk verkort om de kwetsbaarheid van data te verminderen.

Met analyse van de CO2-voetafdruk en robuuste energiebeheertools hebben we ontdekt dat OME organisaties beter kan helpen bij het plannen om duurzaamheidsdoelstellingen te behalen dan met behulp van de bedrijfsbeheerconsole van leverancier K. Bovendien hebben we vastgesteld dat het Dell serverbeheerportfolio meer automatisering en meer opties voor extern beheer bood, waardoor de tijd en moeite van beheerders voor bepaalde routinematige bewakings- en onderhoudstaken werden verminderd. Deze voordelen op het gebied van beveiliging, duurzaamheid en beheer-/bewakingsfuncties maken het Dell serverbeheerportfolio een aantrekkelijke optie voor organisaties die op zoek zijn naar een efficiënter en veiliger datacenter.

1. Harvard Business Review, 'The Devastating Business Impact of a Cyber Breach', geraadpleegd op 10 april 2024, <https://hbr.org/2023/05/the-devastating-business-impacts-of-a-cyber-breach>.
2. Dell, "Integrated Dell Remote Access Controller (iDRAC)", geraadpleegd op 17 mei 2024, <https://www.dell.com/en-us/lp/dt/open-manage-idrac>.
3. Opmerking: De uitschakeling van USB-poorten van leverancier K is aanpasbaar, hoewel dit betekent dat beheerders elke poort moeten selecteren voor uitschakeling, in plaats van per groep.
4. DOE, "DOE kondigt \$ 40 miljoen aan voor meer efficiënte koeling voor datacenters", geraadpleegd op 20 mei 2024, <https://www.energy.gov/articles/doe-announces-40-million-more-efficient-cooling-data-centers>.
5. Dell, "OpenManage Enterprise Support Matrix", geraadpleegd op 21 mei 2024, <https://www.dell.com/support/kbdoc/en-us/article/lkbprint?ArticleNumber=000217909&AccessLevel=10&Lang=en>.
6. Dell, "OpenManage Enterprise", geraadpleegd op 17 mei 2024, <https://www.dell.com/en-us/work/learn/openmanage-enterprise>.
7. Principled Technologies, "Een Dell PowerEdge MX omgeving die gebruik maakt van OpenManage Enterprise en OpenManage Enterprise Modular kan het leven van beheerders een stuk gemakkelijker maken", geraadpleegd op 17 mei 2024, <https://www.principledtechnologies.com/Dell/PowerEdge-MX-OME-OME-M-0124.pdf>.
8. Dell, "APEX AIOps: Tame IT Complexity in Your digital business", geraadpleegd op 11 juni 2024, <https://www.dell.com/en-us/dt/apex/aiops.htm>.
9. Principled Technologies, "Dell CloudIQ biedt één enkele console voor proactieve monitoring en had verwaarloosbare gevolgen voor de netwerkbandbreedte in onze tests", geraadpleegd op 9 april 2024, <https://www.principledtechnologies.com/dell/CloudIQ-network-0422.pdf>.

Lees de wetenschap achter dit rapport ►

► Bekijk de oorspronkelijke, Engelse versie van dit rapport op



Facts matter.®

Principled Technologies is een geregistreerd handelsmerk van Principled Technologies, Inc. Alle andere productnamen zijn de handelsmerken van hun respectieve eigenaren. Bekijk voor aanvullende informatie de wetenschap achter dit rapport.

Dit project is uitgevoerd in opdracht van Dell Technologies.