



Minska datasäkerhetsrisken
med
**85 % mindre tid
för att avaktivera
främre USB-portar**

*i iDRAC9 jämfört med leverantör
K:s BMC*



Bidra till att minska
koldioxidutsläppen med
**25 anpassningsbara
rapporter om
strömförbrukning**

*i OME jämfört med 0
rapporter i leverantör K:s
företagshanteringskonsol*



Schemalägg automatiskt
**uppdateringar av
fast mjukvara på
bara 41 sekunder**

*i APEX AIOps Infrastructure
Observability (tidigare CloudIQ)*

Dells serverhanteringsverktyg kan bidra till att förbättra säkerhet, hållbarhet och hanteringseffektivitet

jämfört med jämförbara serverhanteringsverktyg från leverantör K

I takt med att datacenter fortsätter att växa, växer även administratörernas arbetsuppgifter. Infrastruktur som erbjuder inbyggda robusta hanterings- och övervakningsverktyg med automatisering kan göra skydd och hantering av datacentret enklare för administratörer som ofta är överbelastade. Vi jämförde funktionerna i hanteringsportföljerna från Dell och en konkurrent som vi kallar leverantör K:

Tabell 1: Hanteringsverktygen vi testade.

	Dell	Leverantör K
Inbyggd/fjärrstyrd serverhantering	Dell Technologies Integrated Dell Remote Access Controller 9 (iDRAC9)	Leverantör K Baseboard Management Controller (BMC)
Enhets- och konsolhantering för en-till-många	Dell Technologies OpenManage™ Enterprise (OME) APEX AIOps Infrastructure Observability (tidigare CloudIQ)	Leverantör K:s företagshanteringskonsol

Vi såg att iDRAC9, OME och APEX AIOps Infrastructure Observability (tidigare CloudIQ) erbjöd en stark uppsättning hanteringsverktyg som kunde förbättra säkerheten, hjälpa till med hållbarhetsåtgärder och göra dagliga administratörsuppgifter enklare jämfört med att använda liknande verktyg från leverantör K.

Stärka säkerheten i datacentret

För organisationer som lagrar känsliga kunddata kräver det ständiga hotet om cyberattacker starka heltäckande säkerhetsfunktioner för att säkerställa att data inte hamnar i fel händer. Faktum är att upp till "83 % av organisationerna utsattes för mer än en dataläcka under 2022"¹ och denna statistik visar hur viktigt det är att vidta försiktighetsåtgärder för kunddata för att öka konsumenternas förtroende.

I syfte att skydda din organisation och dess data från kostsamma cyberattacker erbjuder Dells hanteringsverktyg starka säkerhetsfunktioner som både finns inbäddade i servern via iDRAC9 och i övergripande konsol- och molnhanteringsmjukvara. Nedan utforskar vi några av de viktigaste säkerhetsfunktionerna som Dells verktyg använder för att skydda ditt system och jämför dem med motsvarande erbjudanden från leverantör K.

Inbyggd säkerhet

I alla Dell PowerEdge-serverar finns säkerhetsfunktioner inbyggda via iDRAC9 för att förhindra att illvilliga aktörer får åtkomst till data. Tre sådana viktiga funktioner är:

- **Dynamisk systemlåsning:** Systemlåsning förhindrar att oavsiktlig eller skadlig aktivitet ändrar system-BIOS, iDRAC och inställningar för fast mjukvara. Dynamisk avser möjligheten att konfigurera dessa funktioner en gång och sedan verkställa efter behov. (Obs! Den här funktionen är tillgänglig med iDRAC9 Enterprise- och Datacenter-licenser.)
- **Multifaktorautentisering (MFA):** MFA uppmanar administratörer att ange en lösenkod utöver sina inloggningsuppgifter för att förbättra säkerheten.
- **Aktivering/avaktivering av dynamisk USB-port:** Med avaktivering och aktivering av USB-portar får administratörer kontroll över åtkomsten till servern via en USB-port. Dynamisk avser möjligheten att aktivera och avaktivera dessa USB-portar utan att starta om servern eller operativsystemet. Innan administratören har gett åtkomst kan ingen ansluta en minnessticka eller ett tangentbord för att ändra några konfigurationsinställningar för systemet, operativsystemet eller BIOS.

Som tabell 2 visar erbjuder leverantör K inte dynamisk systemlåsning eller MFA, och dess dynamiska USB-funktioner kräver driftavbrott i systemet (vilket kan bli dyrt för organisationerna), vilket gör det mindre användbart och dyrare än Dell-lösningen.

Tabell 2: Jämförelse av inbyggda säkerhetsfunktioner som serverhanteringsverktygen erbjuder. Källa: Principled Technologies.

	iDRAC9	Leverantör K:s BMC
Dynamisk systemlåsning	✓	✗
MFA	✓	✗
Dynamisk USB	✓	✓*

* Kräver driftavbrott i systemet

Om Dell Technologies Integrated Dell Remote Access Controller 9

Dell PowerEdge™-serverar omfattar iDRAC9 med Dell Lifecycle Controller för att tillhandahålla systemadministrationsfunktioner som ger systemvarningar och fjärrhanteringsfunktioner. Enligt Dell omfattar de viktigaste fördelarna med iDRAC9:

- Skalbar automatisering. Standardbaserade API:er som Redfish och robusta skriptverktyg som RedHat Ansible, Python, PowerShell och Terraform gör att du kan hantera tusentals serverar.
- Inbyggd support som ger en vy över serverhälsa och statusövervakning för tusentals parametrar
- Starka säkerhetsfunktioner och alternativ²

Mer information om de funktioner iDRAC9 tillhandahåller finns på <https://www.dell.com/en-us/lp/dt/open-manage-idrac>.

Bild 1 visar resultaten av vår praktiska jämförelse med iDRAC9 och leverantör K:s BMC för att dynamiskt avaktivera USB-portar.

Med hjälp av iDRAC9 upptäckte vi att administratörer kunde avaktivera främre USB-portar på en enda server på bara 41 sekunder och med 4 steg. I jämförelse skulle samma process ta 4 minuter, 43 sekunder och 8 steg per server med leverantör K:s BMC. Det innebär att per server **tar Dells lösning 85 % mindre tid och hälften så många steg för att avaktivera främre USB-portar.**³ När man tänker sig att dessa steg ska utföras i ett datacenter ökar tidsbesparingarna. I en distribution med 100 servrar kan administratörer spara 6 timmar och 43 minuter med iDRAC9 jämfört med leverantör K:s BMC.

Dessa funktioner är inte bara enklare och snabbare att komma åt med iDRAC9 jämfört med leverantör K:s BMC, utan med iDRAC9 kan administratörerna bibehålla servrarna i produktion (inga driftavbrott) när de aktiverar eller avaktiverar dessa funktioner. Leverantör K:s metod kräver driftavbrott, vilket kan medföra betydande kostnader, samt ändringar av systemkonfigurationen varje gång.

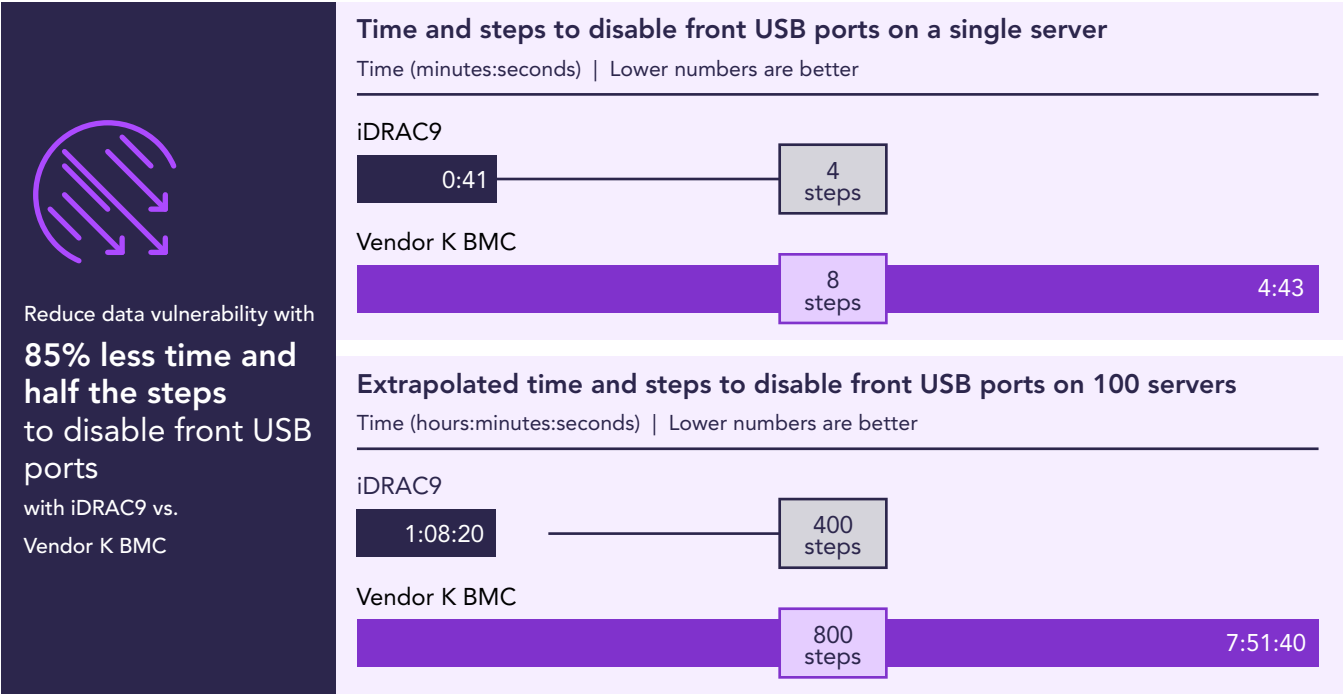


Bild 1: Tid för att avaktivera främre USB-portar för en enda server och extrapolerad tid för att avaktivera främre USB-portar för 100 servrar. Mindre tid och färre steg är bättre. Källa: Principled Technologies.

Håll dig säker med enklare hantering av inloggningsuppgifter i OME

OME ger administratörer ett enkelt sätt att hantera iDRAC9-lösenordsrotation. I stället för att kräva ett statiskt, känt administratörskonto hanterar OME iDRAC via ett tjänstkonto där kunderna väljer den policy för lösenordsrotation som krävs och som lösenordet aldrig avslöjas för. Administratörerna kan även välja att hantera externt med en tredje part. **Leverantör K:s företagshanteringskonsol har inga funktioner för intern lösenordsrotation, vilket tvingar administratörerna att förlita sig på en tredje part om de vill ha den här funktionen.** Vi bekräftade att iDRAC9-hanterade servrar integrerades med OME-kontot med fullständig administratörsbehörighet för enklare hantering av inloggningsuppgifter.

Obs! Diagrammen i den här rapporten använder olika skalor. Tänk på varje diagrams dataintervall när du jämför.

Nå hållbarhetsmålen

Enligt amerikanska energidepartementet (Department of Energy) "står datacenter för cirka 2 % av den totala elförbrukningen i USA, medan datacenterkylning kan stå för upp till 40 % av datacentrets energiförbrukning totalt sett".⁴ I takt med att data sprids kommer dessa siffror bara att växa, vilket gör värme- och strömhantering avgörande för att hålla kostnaderna för datacenter nere samt uppfylla hållbarhetsmålen för att minska koldioxidutsläppen. OME har flera funktioner för övervakning och hantering av strömförbrukning för att hjälpa organisationer att minska strömförbrukningen. I tabell 3 beskrivs de viktigaste fördelarna med dessa funktioner, som vi beskriver mer detaljerat nedan.

Tabell 3: Översikt över viktiga hållbarhetsfunktioner som finns i OME jämfört med leverantör K:s företagshanteringskonsol. Källa: Principled Technologies.

Funktionen	Viktiga fördelar med Dells hanteringsverktyg	Nackdelar med hanteringsverktyg från leverantör K
 Kalkylator för koldioxidutsläpp och verktyg för kapacitetsplanering	Möjlighet att uppskatta utsläpp av växthusgaser med anpassningsbara värden som hjälper till att uppfylla hållbarhetsmålen	Leverantör K:s företagshanteringskonsol erbjuder ingen jämförbar funktion
 Policyer för strömbegränsning	Insticksprogrammet OME Power Manager kan hantera strömbegränsning för enheter eller grupper med enheter som tillämpar strömgränser när det är aktiverat	Leverantör K:s företagshanteringskonsol erbjuder ingen jämförbar funktion
 Automatiserad ström- och värmehantering	Ström- och temperaturaktiverade policyalternativ med möjlighet att aktivera när servern överskrider en strömförbruknings- eller temperaturtröskel	Leverantör K:s företagshanteringskonsol erbjuder ingen jämförbar funktion
 Instrumentpanel för strömförbrukning	Insticksprogrammet OME Power Manager har en instrumentpanel som ger snabb åtkomst till Power Manager-data och erbjuder 2,75 gånger fler mätvärden med 11 mätvärden	Leverantör K:s företagshanteringskonsol erbjuder bara 4 mätvärden på instrumentpanelen
 Rapporter om strömförbrukning	Insticksprogrammet OME Power Manager ger 25 olika standardrapporter och ytterligare anpassningsbara rapporter	Leverantör K:s företagshanteringskonsol tillhandahåller inga rapporter för strömhantering
 Mätvärden för strömhantering	Upp till tre gånger fler mätvärden ger mer detaljerad insikt i hantering av strömförbrukning med 21 mätvärden	Leverantör K:s företagshanteringskonsol erbjuder bara 7 mätvärden för strömhantering

Automatiserad ström- och värmehantering

OME Power Manager erbjuder automatiserad ström- och värmehantering genom både ström- och temperaturaktiverade policyalternativ som gör det möjligt för administratörer att ställa in gränser för strömförbrukning eller temperaturtröskelvärden för att minska kylningskostnaderna, främja strategier för lägre strömförbrukning och hantera värmehändelser. **Leverantör K erbjuder däremot ingen automatiserad ström- och värmehanteringsfunktion.** Utan möjligheten att ställa in temperaturbaserade gränser kan energiförbrukningen överskrida förväntningarna och göra det svårt att planera med hållbarhet i åtanke. Att optimera energiförbrukningen är en viktig strategi för att nå hållbarhetsmålen. Insticksprogrammet OME Power Manager innehåller **25 standardrapporter och/eller anpassningsbara Power Manager-relaterade rapporter** (17 i Power Manager-enheter och 8 till i Power Manager-grupper) som gör det möjligt för administratörer att optimera kapacitetsplanering och hantera ström för att maximera effektiviteten. **Leverantör K:s företagshanteringskonsol erbjuder inga liknande rapporter för strömhantering** (se bild 2).

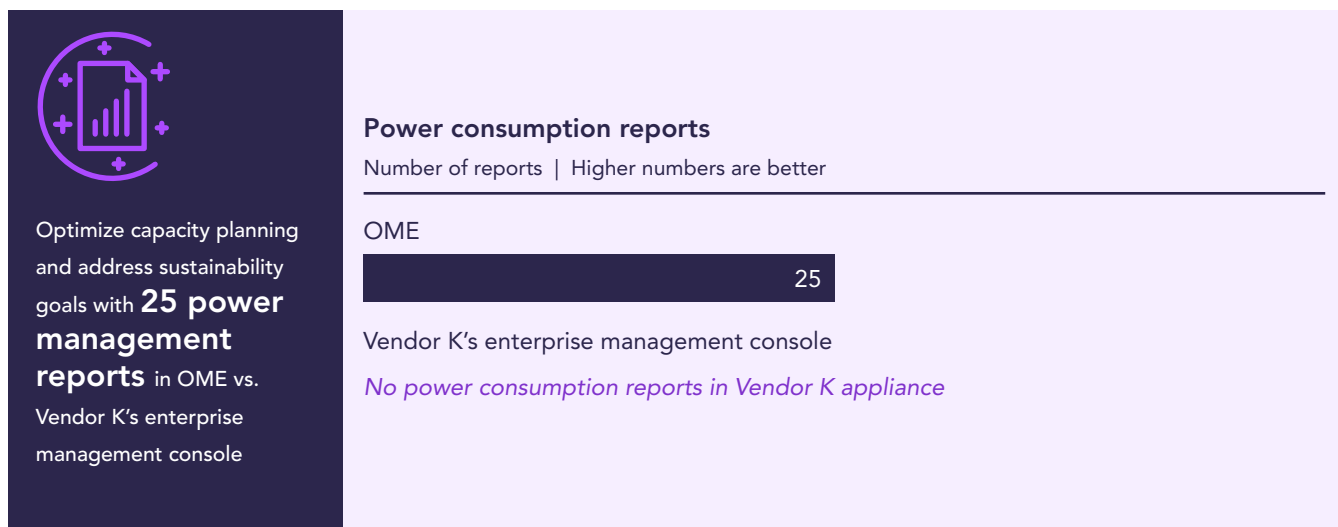


Bild 2: Jämförelse av antalet strömhanteringsrapporter som finns i OME och leverantör K:s företagshanteringskonsol. Fler rapporter är bättre. Källa: Principled Technologies

I syfte att optimera strömhanteringen ytterligare gör insticksprogrammet OME Power Manager det möjligt för administratörer att visa upp till **tre gånger fler mätvärden jämfört med leverantör K:s företagshanteringskonsol** (se bild 3). OME tillhandahåller 21 olika mätvärden, inklusive strömförbrukning för enskilda komponenter, luftflöde och komponentanvändning, medan leverantör K:s företagshanteringskonsol endast tillhandahåller 7 olika mätvärden.

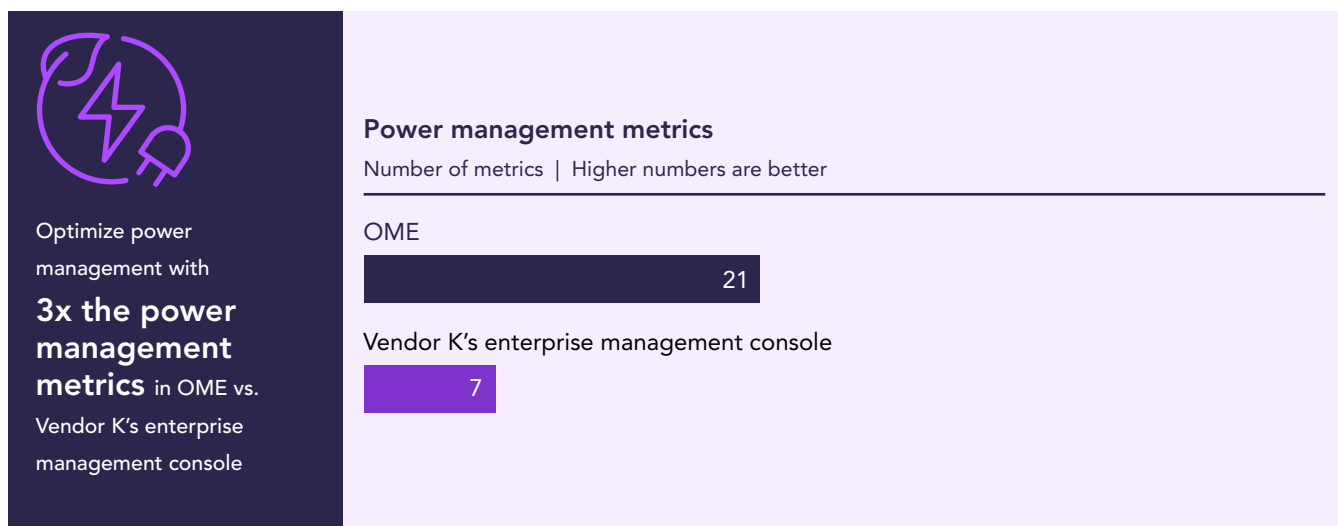


Bild 3: Jämförelse av antalet strömhanteringsmätvärden som finns i OME och leverantör K:s företagshanteringskonsol. Fler mätvärden är bättre. Källa: Principled Technologies.

Koldioxidutsläpp och analys av koldioxidutsläpp

En viktig hållbarhetsfunktion som **OME omfattar är en kalkylator för koldioxidutsläpp och ett verktyg för kapacitetsplanering**. Det här verktyget hjälper organisationer att uppskatta sina utsläpp av växthusgaser, vilket ger standardvärden för energikostnader och koldioxidutsläpp per energienhet. Den här funktionen möjliggör även anpassning, vilket ger organisationer möjlighet att ange värden för sin egen regions elkostnader och koldioxidutsläpp för data som är specifika för datacentrets förbrukningsmodell. **Leverantör K:s företagshanteringskonsol har ingen jämförbar funktion**, vilket kan begränsa en organisations förmåga att planera med hållbarhet i åtanke.

Minska hanteringsbördan med robusta övervaknings- och hanteringsfunktioner

I takt med att infrastrukturen växer kan datacenteradministratörens ansvar växa med den. Genom att välja serverhanteringsverktyg som automatiserar vissa uppgifter och förbättrar den dagliga hanteringen kan organisationer hjälpa administratörerna att bli effektivare och ge dem mer tid att planera för framtiden. Vi såg att Dells serverhanteringsportfölj erbjuder ett antal funktioner som kan förenkla administratörsuppgifter. Tabell 4 innehåller en sammanfattning av viktiga användarvänliga funktioner som finns i Dells hanteringsportfölj jämfört med leverantör K:s hanteringsverktyg.

Tabell 4: Översikt över viktiga användarvänliga funktioner som finns i Dells hanteringsverktyg jämfört med leverantör K:s hanteringsverktyg. Källa: Principled Technologies.

Funktionen	Viktiga fördelar med Dells hanteringsverktyg	Nackdelar med hanteringsverktyg från leverantör K
 Fler fjärranslutna BIOS-funktioner	Enklare fjärrhantering med 51 fjärranslutna BIOS-funktioner i iDRAC9	Leverantör K:s BMC erbjuder endast 1 fjärransluten BIOS-funktion
 Enklare BIOS-konfigurationsändringar	87 % mindre tid och hälften så många steg för att göra en BIOS-konfigurationsändring	Leverantör K kräver manuella administratörsåtgärder för att göra ändringar inifrån systemverktygen
 Import/export av fullständig serverkonfiguration	Snabbare konfiguration av flera identiska servrar med möjlighet att exportera/importera konfigurationsinställningar för en fullt konfigurerad server	Leverantör K tillhandahåller endast säkerhetskopiering och återställning av BMC för varje enskild server
 Automatiska schemalagda uppdateringar	iDRAC9 ger administratörer möjlighet att schemalägga automatiska uppdateringar från ett datalager under ett underhållsfönster utan ytterligare administratörsåtgärder	Leverantören K BMC erbjuder inte schemalagda automatiserade uppdateringar
 Omfattande översikt över lagringsstatus	iDRAC9 ger en visuell representation av lagringsstatus för att snabbt identifiera enheter med varningsstatus	Leverantören K BMC tillhandahåller inte en liknande vy
 Telemetriströmning	iDRAC9 tillhandahåller telemetri för dubbelt så många mätvärdeskategorier, med totalt 8 kategorier	Leverantör K:s BMC tillhandahåller telemetri för endast 4 kategorier
 Anslutningsvisning	Anslutningsvyn i iDRAC9 innehåller information om den fysiska mappningen av switchportar till serverns nätverksportar och iDRAC-dedikerade portanslutningar	Leverantör K:s BMC har ingen fysisk anslutningsinformation till switchar uppströms
 Skalbarhet	OME kan hantera upp till 8 000 enheter⁵	Leverantör K kan endast hantera upp till 1 000 enheter

Funktionen	Viktiga fördelar med Dells hanteringsverktyg	Nackdelar med hanteringsverktyg från leverantör K
 Varningsbaserade åtgärder	OME tillhandahåller två gånger fler varningsbaserade åtgärder (med 12) som utlöser åtgärder baserat på indata från en varning	Leverantör K erbjuder endast 4 varningsbaserade åtgärder
 Arkitektur för insticksprogram	OME erbjuder möjligheten att utöka funktionerna med insticksprogram som administratörer kan lägga till i konsolen utan att det behövs ytterligare program att hantera	Leverantör K:s företagshanteringskonsol erbjuder inte insticksprogrambaserad arkitektur för utbyggbarhet
 Övervakning av enheter från tredje part	OME har stöd för övervakning av enheter och servrar från tredje part	Leverantör K:s företagshanteringskonsol stöder inte övervakning av tredjepartsenheter och servrar
 Rapportering	OME erbjuder administratörer 42 inbyggda rapporter med anpassning så att administratörer får ett detaljerat urval av de viktigaste data för sina ändamål	Leverantör K:s företagshanteringskonsol har ingen inbyggd rapportgenerering

Fjärrhantering

Med iDRAC9 behöver administratörerna inte öppna datacentret för varje ändring. iDRAC9 erbjuder 51 fjärbaserade BIOS-funktioner som ger administratörer friheten att göra fler ändringar utanför datacentret, jämfört med bara en för leverantör K:s BMC, vilket ger administratörerna betydligt mer detaljerad kontroll över BIOS-konfigurationen var som helst (se bild 4).

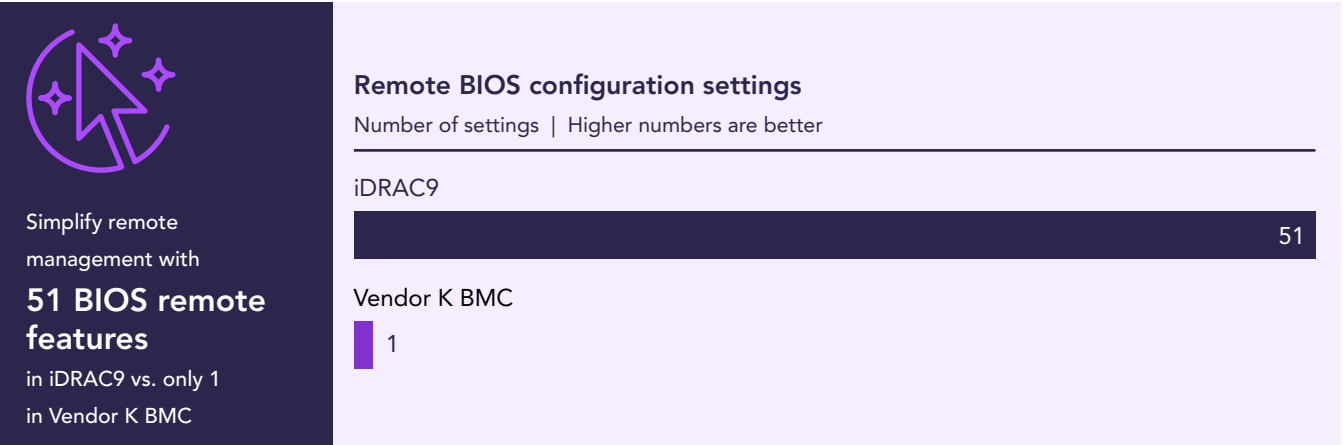


Bild 4: Jämförelse av fjärranslutna BIOS-funktioner som de olika hanteringsverktygen erbjuder. Fler funktioner är bättre. Källa: Principled Technologies.

Göra konfigurationsändringar

Med iDRAC9 kan administratörerna ändra inställningarna för BIOS-konfigurationen och stega upp uppdateringen för en senare omstart utan att ytterligare administratörsnärvaro krävs. Leverantör K:s BMC kräver däremot ändringar från systemverktygen och manuella administratörsåtgärder under ändringen. Som bild 5 visar tog förberedelse av BIOS-konfigurationsändringen för en schemalagd omstart 87 % mindre tid och omfattade hälften så många steg med iDRAC9 jämfört med leverantör K:s BMC. När man extrapolerar dessa besparingar till stora distributioner ger det ännu större besparingar av administrationstiden. I en distribution med 100 servrar kan administratörerna till exempel spara över 6 timmar vid ändring av BIOS-konfigurationsobjekt.

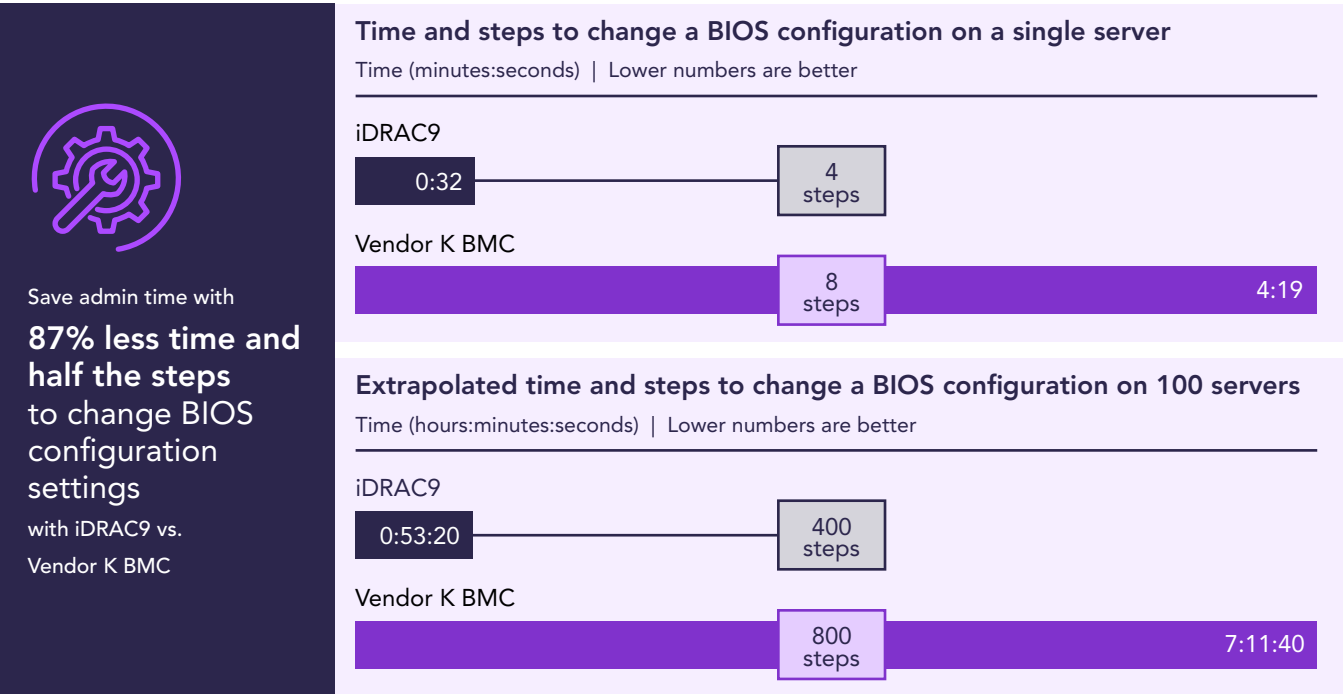


Bild 5: Tiden för att ändra BIOS-konfigurationsinställningarna och förbereda en uppdatering för en senare omstart för en enda server och extrapolerad tid för 100 servrar. Mindre tid och färre steg är bättre. Källa: Principled Technologies.

Konfigurera varningsbaserade åtgärder

Administratörerna kan använda sin tid på ett bättre sätt när de inte är bundna till ett skrivbord för att övervaka miljöns hälsa. Som bild 6 visar tillhandahåller OME 12 policydrivna alternativ för varningsbaserade åtgärder så att problemhanteringen startar automatiskt när miljön når vissa tröskelvärden. Leverantör K:s företagshanteringskonsol gör det i stället möjligt för administratörerna att konfigurera endast fyra varningsbaserade händelser.

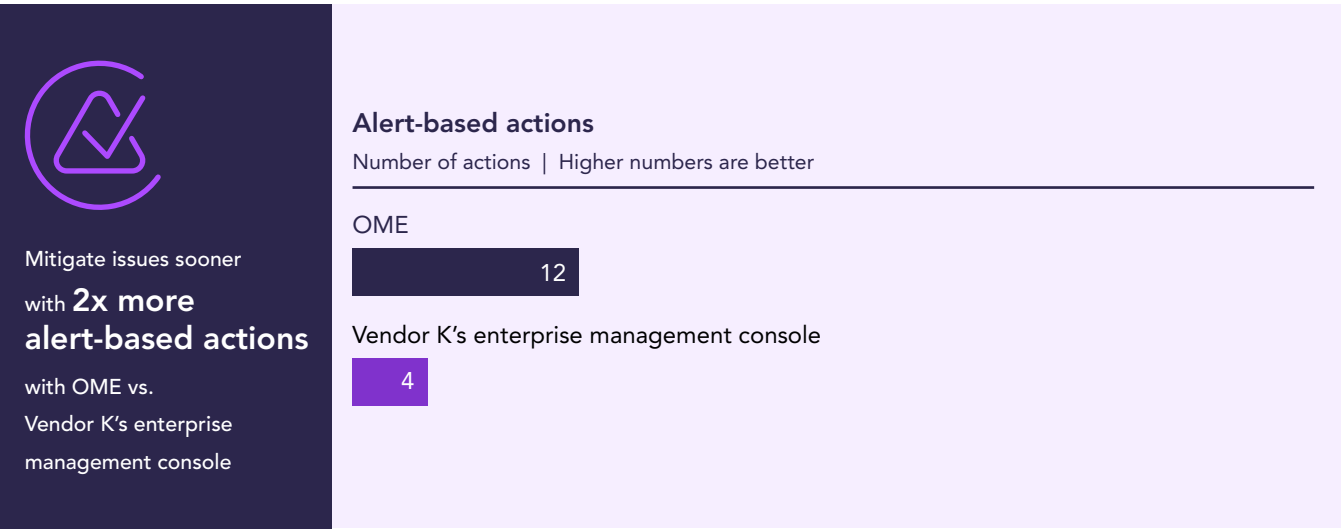


Bild 6: Jämförelse av de varningsbaserade åtgärder som de olika hanteringsverktygen erbjuder. Fler åtgärder är bättre. Källa: Principled Technologies.

Om Dell Technologies OpenManage Enterprise

OME är en en-till-många-systemhanteringskonsol för datacentret. Konsolen har ett modernt grafiskt HTML5-användargränssnitt och installeras som en virtuell enhet för miljöer med VMware ESXi™, Microsoft Hyper-V och KVM (Kernel-based Virtual Machine). OME kan upptäcka och inventera IPV4- och IPV6-nätverk för upp till 8 000 enheter, inklusive Dell-rackservrar, Dell-tornservrar och Dell-blad och -chassin.⁶ I en PT-studie som utfördes nyligen såg vi att en Dell-miljö med OME och OpenManage Enterprise Modular (OME-M) kan spara tid på att göra ändringar i VLAN och hjälpa till att undvika åtgärder under schemalagda uppdateringar av fast mjukvara.⁷

Läs mer om OME på <https://www.dell.com/en-us/lp/dt/open-manage-enterprise>.

Molnbaserad hantering med APEX AIOps Infrastructure Observability (tidigare CloudIQ)

Inbäddade verktyg och företagshanteringskonsoler är inte de enda verktygen i Dells serverhanteringsportfölj. Med APEX AIOps Infrastructure Observability (tidigare CloudIQ) får administratörer ytterligare ett användarvänligt automatiserat sätt att hålla koll på infrastrukturens hälsa och säkerhet – den här gången från molnet.

Ytterligare säkerhetsfunktioner är tillgängliga i APEX AIOps Infrastructure Observability (tidigare CloudIQ)

APEX AIOps Infrastructure Observability (tidigare CloudIQ) erbjuder flera säkerhetsfunktioner som kan stärka organisationen ytterligare mot attacker. I tabell 5 beskrivs några av dessa viktiga säkerhetsfunktioner.

Tabell 5: Översikt över viktiga säkerhetsfunktioner som är tillgängliga i APEX AIOps Infrastructure Observability (tidigare CloudIQ). Källa: Principled Technologies.

Funktionen		Så fungerar APEX AIOps Infrastructure Observability (tidigare CloudIQ) för att skydda din miljö
	Varningar på cybersäkerhetsrisknivå	Tillhandahåller automatiserade insikter för cybersäkerhet med specifika varningar på säkerhetsrisknivå så att administratörer kan reagera snabbare och åtgärda problem snabbt för att skydda data
	Policybaserad säkerhetskfiguration	Erbjuder policybaserade inställningar för säkerhetskfiguration och lättanvända mallar som gör det möjligt för en administratör att säkerställa att inställningar för bästa säkerhetspraxis finns på plats och skyddar PowerEdge-miljön
	Rådgivning om cybersäkerhet	Tillhandahåller relevant rapportering av säkerhetsrekommendationer , med specifik sårbarhetsinformation och förslag på åtgärder, vilket möjliggör snabba insatser för att åtgärda säkerhetsluckor

Om APEX AIOps Infrastructure Observability (tidigare CloudIQ)

APEX AIOps Infrastructure Observability (tidigare CloudIQ) är ett molnbaserat AIOps-verktyg som erbjuder "proaktiv övervakning, maskininlärning och prediktiv analys" för ett stort antal produkter och tjänster från Dell, inklusive servrar, lagring, dataskyddsenheter och hyperkonvergerad infrastruktur.⁸ I en studie från Principled Technologies 2022 såg vi att CloudIQ hade försumbar inverkan på nätverksbandbredden samtidigt som vi kunde övervaka telemetri, hälsostatus, varningar och lager från en enda konsol.⁹

Läs mer om APEX AIOps Infrastructure Observability (tidigare CloudIQ) på <https://www.dell.com/en-us/dt/apex/aiops.htm>.

Ytterligare funktioner för hållbarhet och effektivitet finns i APEX AIOps Infrastructure Observability (tidigare CloudIQ)

APEX AIOps Infrastructure Observability (tidigare CloudIQ) tillhandahåller även funktioner som förbättrar hållbarhet och effektivitet. De kan integreras med iDRAC9 och OME för att göra det lättare för administratörer att övervaka PowerEdge-miljöns hälsa. I tabell 6 beskrivs några av dessa funktioner.

Tabell 6: Översikt över hållbarhet och användarvänliga hanteringsfunktioner som finns i APEX AIOps Infrastructure Observability (tidigare CloudIQ). Källa: Principled Technologies.

Funktionen		Viktiga fördelar med APEX AIOps Infrastructure Observability (tidigare CloudIQ)
	Analys av koldioxidutsläpp	Det här verktyget finns i övervakningsavsnittet och ger en bild av utsläppen på högre nivå och kan förutse koldioxidutsläpp i olika miljöer
	Prestandavyer	Tillhandahåller prestandavyer och diagram för avvikelser och användning för att varna administratörer vid första tecken på problem
	Anpassade efterlevnadsrapporter	Ger användarna möjlighet att skapa anpassade efterlevnadsrapporter för utvalda enheter
	Anpassningsbara prestanda- och inventeringsrapporter	Tillhandahåller anpassade rapporteringsalternativ för serverprestanda och lagerdata, vilket ger administratörer mer kontroll över de prestanda- och enhetsmätvärden som de är intresserade av att spåra
	Schemalägga energiåtgärder	Utför energiåtgärder som strömbegränsning på flera övervakade Dell PowerEdge-servrar på bara 35 sekunder och med 6 steg
	Schemalägga uppdateringar av fast mjukvara	Schemalägg uppdateringar av fast PowerEdge-mjukvara för flera övervakade servrar på bara 41 sekunder och med 9 steg

Sammanfattning

I vår jämförelse av säkerhets-, hållbarhets- och hanterings-/övervakningsfunktioner såg vi att Dells portfölj med serverhanteringsverktyg innehöll mer robusta hanterings- och övervakningsfunktioner än leverantör K:s portfölj. När det gäller säkerhet erbjöd iDRAC9 fler funktioner, inklusive dynamisk systemlåsning och multifaktorautentisering, som leverantör K inte erbjöd alls. Dessutom minskade iDRAC9 avsevärt tiden för att avaktivera USB-portar för att minska datasårbarheten.

Tack vare analys av koldioxidutsläpp och robusta verktyg för strömhantering såg vi att OME bättre kunde hjälpa organisationer att planera för att nå hållbarhetsmål än med leverantör K:s företagshanteringskonsol. Dessutom såg vi att Dells serverhanteringsportfölj erbjöd mer automatisering och fler alternativ för fjärrhantering, vilket minskade administratörernas tid och arbete för vissa rutinövervaknings- och underhållsuppgifter. Dessa vinster inom säkerhet, hållbarhet och hantering/övervakning gör Dells serverhanteringsportfölj till ett attraktivt alternativ för organisationer som vill ha ett effektivare och säkrare datacenter.

1. Harvard Business Review, "The Devastating Business Impacts of a Cyber Breach", läst 10 april 2024, <https://hbr.org/2023/05/the-devastating-business-impacts-of-a-cyber-breach>.
2. Dell, "Integrated Dell Remote Access Controller (iDRAC)", läst 17 maj 2024, <https://www.dell.com/en-us/lp/dt/open-manage-idrac>.
3. Obs! Leverantör K:s avaktivering av USB-port kan anpassas, men det innebär att administratörer måste välja varje port för avaktivering, i stället för per grupp.
4. DOE, "DOE Announces \$40 Million for More Efficient Cooling for Data Centers", läst 20 maj 2024, <https://www.energy.gov/articles/doe-announces-40-million-more-efficient-cooling-data-centers>.
5. Dell, "OpenManage Enterprise Support Matrix", läst 21 maj 2024, <https://www.dell.com/support/kbdoc/en-us/article/lkbprint?ArticleNumber=000217909&AccessLevel=10&Lang=en>.
6. Dell, "OpenManage Enterprise", läst 17 maj 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 easier for administrators", läst 17 maj 2024, <https://www.principledtechnologies.com/Dell/PowerEdge-MX-OME-OME-M-0124.pdf>.
8. Dell, "APEX AIOps: Tame IT complexity in your digital business", läst 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", läst 9 april 2024, <https://www.principledtechnologies.com/dell/CloudIQ-network-0422.pdf>.

Läs vetenskapen bakom rapporten ►

► Se den ursprungliga, engelska versionen av den här rapporten

Det här projektet har beställts av Dell Technologies.



Facts matter.®

Principled Technologies är ett registrerat varumärke som tillhör Principled Technologies, Inc. Alla andra produktnamn är varumärken som tillhör respektive ägare. Granska vetenskapen bakom denna rapport om du vill ha mer information.