Riduci la vulnerabilit→ dei dati con

l'85% di tempo in meno per disabilitare le porte USB anteriori

in iDRAC9 rispetto al Vendor K BMC

Contribuisci alla riduzione delle emissioni di carbonio con

25 report sul consumo energetico personalizzabili

in OME rispetto a 0 report nella console di gestione aziendale del Vendor K

Pianifica

gli aggiornamenti automatici del firmware in soli 41 secondi

in APEX AIOps Infrastructure Observability (in precedenza CloudIQ)

Gli strumenti di gestione dei server Dell migliorano la sicurezza, la sostenibilità e l'efficienza di gestione

rispetto a strumenti analoghi di gestione dei server del Vendor K

Con la continua crescita dei data center, aumentano anche i compiti degli amministratori. L'infrastruttura che offre solidi strumenti nativi di gestione e monitoraggio con automazione può rendere la protezione e la gestione del data center un'attività più semplice per gli amministratori spesso oberati di lavoro. Abbiamo confrontato le caratteristiche e le funzionalità dei portafogli di gestione Dell e di un concorrente che chiameremo Vendor K:

Tabella 1: Gli strumenti di gestione che abbiamo testato.

	Dell	Vendor K
Gestione integrata/ remota dei server	Dell Technologies Integrated Dell Remote Access Controller 9 (iDRAC9)	Baseboard Management Controller (BMC) del Vendor K
Gestione della console e dei dispositivi one-to-many	Dell Technologies OpenManage™ Enterprise (OME) APEX AIOps Infrastructure Observability (in precedenza CloudIQ)	Console di gestione aziendale del Vendor K

Abbiamo rilevato che iDRAC9, OME e APEX AIOps Infrastructure Observability (in precedenza CloudIQ) offrono una solida famiglia di strumenti di gestione in grado di migliorare la sicurezza, supportare le misure di sostenibilità e semplificare le attività di amministrazione quotidiane rispetto a strumenti simili del Vendor K.

Rafforzamento della sicurezza del data center

Per le organizzazioni che archiviano dati sensibili dei clienti, la minaccia persistente degli attacchi informatici rende necessarie solide funzionalità di sicurezza end-to-end per garantire che i dati non finiscano nelle mani sbagliate. Infatti, "fino all'83% delle organizzazioni ha subito più di una violazione dei dati nel 2022",[1] un dato che sottolinea quanto sia importante adottare le giuste precauzioni con i dati dei clienti per accrescere la fiducia dei consumatori.

Per proteggere la tua organizzazione e i dati da costosi attacchi informatici, gli strumenti di gestione Dell offrono solide funzionalità di sicurezza integrate nel server tramite iDRAC9 e nel software generale di gestione del cloud e della console. Di seguito, esaminiamo alcune delle principali funzionalità di sicurezza utilizzate dagli strumenti Dell per proteggere il sistema e le confrontiamo con le offerte corrispondenti del Vendor K.

Sicurezza integrata

In ogni server Dell PowerEdge sono integrate tramite iDRAC9 delle funzionalità di protezione che impediscono agli utenti malintenzionati di accedere ai dati. Tre di queste importanti funzionalità sono:

- **Blocco dinamico del sistema:** il blocco del sistema impedisce ad attività impreviste o malevole di modificare le impostazioni del BIOS di sistema, dell'iDRAC e del firmware. Il termine "dinamico" fa riferimento alla possibilità di configurare queste funzionalità una sola volta e applicarle quindi in base alle esigenze. (Nota: questa funzionalità è disponibile con le licenze iDRAC9 Enterprise e Datacenter).
- **Autenticazione a più fattori (MFA):** l'autenticazione a più fattori richiede agli amministratori di inserire un passcode in aggiunta alle proprie credenziali di accesso per rafforzare la sicurezza.
- **Abilitazione/disabilitazione dinamica delle porte USB:** l'abilitazione e la disabilitazione delle porte USB garantiscono agli amministratori il controllo sull'accesso al server tramite una porta USB. Il termine "dinamico" fa riferimento alla possibilità di abilitare e disabilitare queste porte USB senza riavviare il server o il sistema operativo. Fino a quando l'amministratore non fornisce l'accesso, nessuno può collegare una scheda di memoria o una tastiera per modificare le impostazioni di configurazione del sistema, del sistema operativo o del BIOS.

Come mostrato nella tabella 2, il Vendor K non offre il blocco dinamico del sistema o la MFA e le sue funzionalità USB dinamiche richiedono il downtime del sistema (che può essere molto dispendioso per le organizzazioni), fattore che lo rende meno utile e più costoso rispetto alla soluzione Dell.

Tabella 2: Confronto delle funzionalità di sicurezza integrate offerte dagli strumenti di gestione dei server. Fonte: Principled Technologies.

	iDRAC9	Vendor K BMC
Blocco dinamico del sistema	✓	✗
MFA	✓	✗
Dynamic USB	✓	✓*

**Richiede il downtime del sistema*

Informazioni su Dell Technologies Integrated Dell Remote Access Controller 9

I server Dell PowerEdge™ includono iDRAC9 con Dell Lifecycle Controller per fornire funzioni di amministrazione dei sistemi che includono avvisi di sistema e funzionalità di gestione remota. Secondo Dell, i vantaggi principali di iDRAC9 includono:

- Automazione scalabile. API basate su standard come Redfish e solidi strumenti di scripting come RedHat Ansible, Python, PowerShell e Terraform, con cui è possibile gestire migliaia di server.
- Supporto integrato, che offre la panoramica dell'integrità e dello stato del server, con il monitoraggio di migliaia di parametri
- Funzionalità e opzioni di protezione avanzate[2]

Per ulteriori informazioni sulle funzionalità offerte da iDRAC9, visita il sito https://www.dell.com/en-us/lp/dt/open-manage-idrac.

La Figura 1 mostra i risultati del nostro confronto pratico nell'utilizzo di iDRAC9 e del BMC del Vendor K per disabilitare dinamicamente le porte USB.

Utilizzando iDRAC9, abbiamo rilevato che gli amministratori potevano disabilitare le porte USB anteriori su un singolo server in soli 41 secondi e 4 passaggi. Con il BMC del Vendor K lo stesso processo richiederebbe invece 4 minuti, 43 secondi e 8 passaggi per server. Ciò significa che per ogni server, **la soluzione Dell impiega l'85% di tempo in meno e la metà dei passaggi per disabilitare le porte USB anteriori**.[3] Quando valuti il completamento di questi passaggi in un data center, il risparmio di tempo aumenta; per il deployment di 100 server, gli amministratori potrebbero risparmiare 6 ore e 43 minuti con iDRAC9 rispetto al BMC del Vendor K.

Non solo l'accesso a queste funzioni è più semplice e veloce con iDRAC9 rispetto al BMC del Vendor K, ma con iDRAC9 gli amministratori possono mantenere i server in produzione (senza downtime) abilitando o disabilitando al contempo queste funzionalità. Il metodo del Vendor K richiede del downtime, che può comportare costi significativi, e la configurazione del sistema cambia ogni volta.

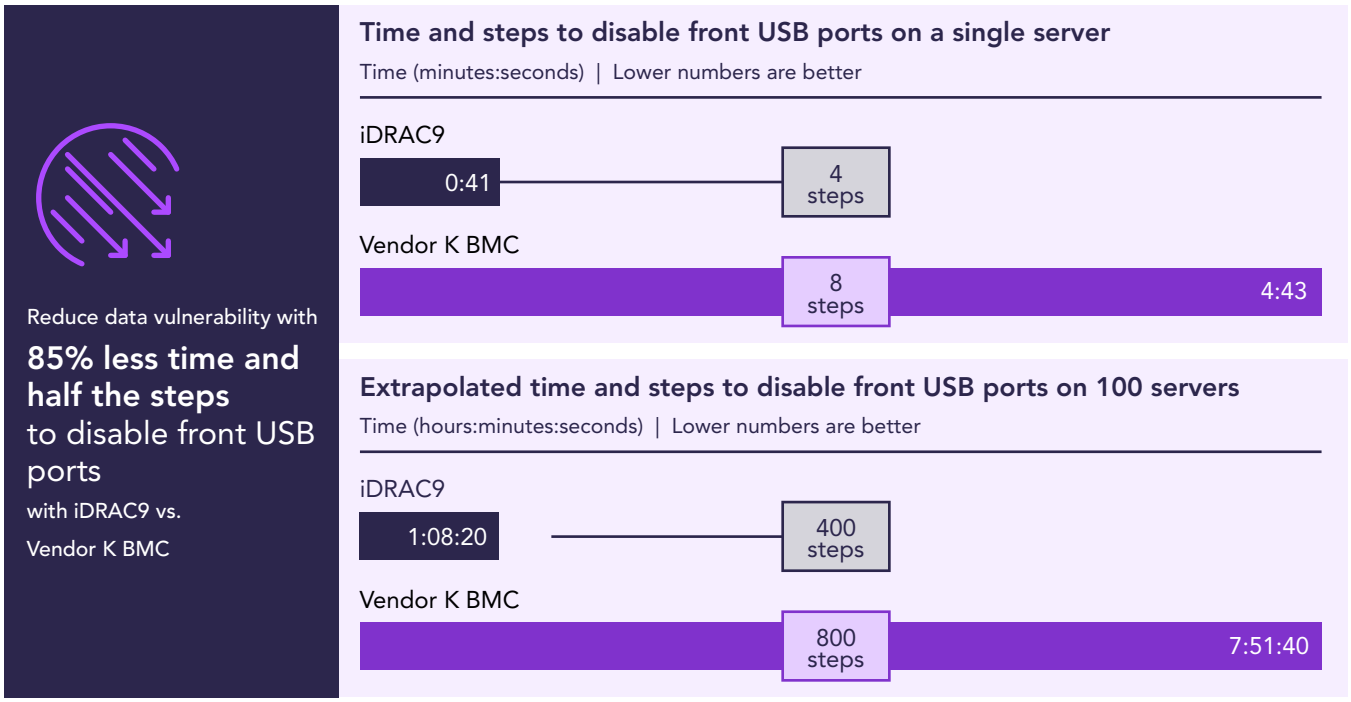

Figura 1. Tempo per disabilitare le porte USB anteriori per un singolo server e tempo estrapolato per disabilitare le porte USB anteriori per 100 server. Meno tempo e meno passaggi sono l'opzione migliore. Fonte: Principled Technologies.

Sicurezza garantita con una gestione semplificata delle credenziali in OME

OME offre agli amministratori un modo semplice per gestire la rotazione delle password di iDRAC9. Anziché richiedere un account amministratore statico e noto, OME gestisce gli iDRAC tramite un account di servizio in cui i clienti selezionano la policy richiesta di rotazione delle password, per la quale la password non viene mai divulgata, oppure gli amministratori possono effettuare la gestione esternamente con terze parti. **La console di gestione aziendale del Vendor K non dispone di funzionalità interne di rotazione delle password e ciò costringe gli amministratori a fare affidamento su terze parti se desiderano questa funzionalità.** Abbiamo confermato che i server gestiti da iDRAC9 sono integrati con l'account OME con privilegi di amministratore completi per una gestione più semplice delle credenziali.

Nota: i grafici in questo report utilizzano scale diverse. È necessario tenere presente l'intervallo di dati di ciascun grafico nell'effettuare il confronto.

Raggiungimento degli obiettivi di sostenibilità

Secondo il Dipartimento dell'energia degli Stati Uniti, "i data center rappresentano circa il 2% del consumo totale di elettricità degli Stati Uniti, mentre il raffreddamento può costituire fino al 40% del consumo energetico complessivo del data center".[4] Con il continuo proliferare dei dati, questi numeri non fanno che aumentare, rendendo la gestione termica e dell'alimentazione fondamentale per mantenere bassi i costi dei data center e raggiungere gli obiettivi di sostenibilità per contribuire a ridurre le emissioni di carbonio. Per fare in modo che le organizzazioni possano ridurre il consumo energetico, OME incorpora diverse funzionalità per il monitoraggio e la gestione del consumo energetico. La Tabella 3 evidenzia i vantaggi principali di queste funzionalità, che descriviamo più nel dettaglio di seguito.

Tabella 3: Panoramica delle principali funzionalità di sostenibilità disponibili in OME rispetto alla console di gestione aziendale del Vendor K. Fonte: Principled Technologies.

Funzione	Vantaggi principali degli strumenti di gestione Dell	Svantaggio degli strumenti di gestione del Vendor K
Calcolatore dell'utilizzo delle emissioni di anidride carbonica e strumento di pianificazione della capacità	Possibilità di effettuare la stima delle **emissioni di gas serra** con valori personalizzabili per raggiungere gli obiettivi di sostenibilità	La console di gestione aziendale del Vendor K **non offre funzionalità analoghe**
Policy sui limiti di alimentazione	Il plug-in OME Power Manager **può gestire i limiti di alimentazione** per dispositivi o gruppi di dispositivi che applicano limiti di alimentazione quando è abilitato	La console di gestione aziendale del Vendor K **non offre funzionalità analoghe**
Gestione termica e dell'alimentazione automatizzata	Opzioni di **policy attivate in base all'alimentazione e alla temperatura** con l'opzione di attivarsi quando il server supera una certa soglia di consumo energetico o della temperatura	La console di gestione aziendale del Vendor K **non offre funzionalità analoghe**
Dashboard per il consumo energetico	**Il dashboard del plug-in OME Power Manager fornisce accesso rapido** ai dati di Power Manager, **offrendo metriche 2,75 volte superiori, per un totale di 11 metriche**	La console di gestione aziendale del Vendor K offre **solo 4 metriche** sul dashboard
Report sul consumo energetico	Il plug-in OME Power Manager fornisce **25 diversi report predefiniti e personalizzabili aggiuntivi**	La console di gestione aziendale del Vendor K **non fornisce report sulla gestione dell'alimentazione**
Metriche della gestione dell'alimentazione	Fino al **triplo di metriche**, che offrono informazioni più granulari sulla gestione del consumo energetico, per un totale di **21 metriche**	La console di gestione aziendale del Vendor K offre **solo 7 metriche** relative alla gestione dell'alimentazione

Gestione termica e dell'alimentazione automatizzata

OME Power Manager offre la gestione automatizzata dell'alimentazione e della temperatura tramite opzioni di policy sia statiche sia attivate in base alla temperatura, con cui gli amministratori possono impostare i limiti per il consumo energetico o le soglie della temperatura per diminuire i costi di raffreddamento, supportare strategie di riduzione dell'alimentazione e rispondere agli eventi termici. Al contrario, **il Vendor K non offre alcuna funzione di gestione automatizzata dell'alimentazione e termica**. Senza la possibilità di impostare limiti basati sulla temperatura, il consumo energetico potrebbe superare le aspettative e rendere difficile effettuare la pianificazione tenendo conto della sostenibilità. L'ottimizzazione del consumo energetico rappresenta una strategia importante per raggiungere gli obiettivi di sostenibilità. Il plug-in OME Power Manager offre **25 report predefiniti e/o personalizzabili relativi a Power Manager** (17 nei dispositivi Power Manager e altri 8 nei gruppi Power Manager) con cui gli amministratori possono ottimizzare la pianificazione della capacità e gestire l'alimentazione per aumentare l'efficienza. **La console di gestione aziendale del Vendor K non offre report simili sulla gestione dell'alimentazione** (v. la Figura 2).

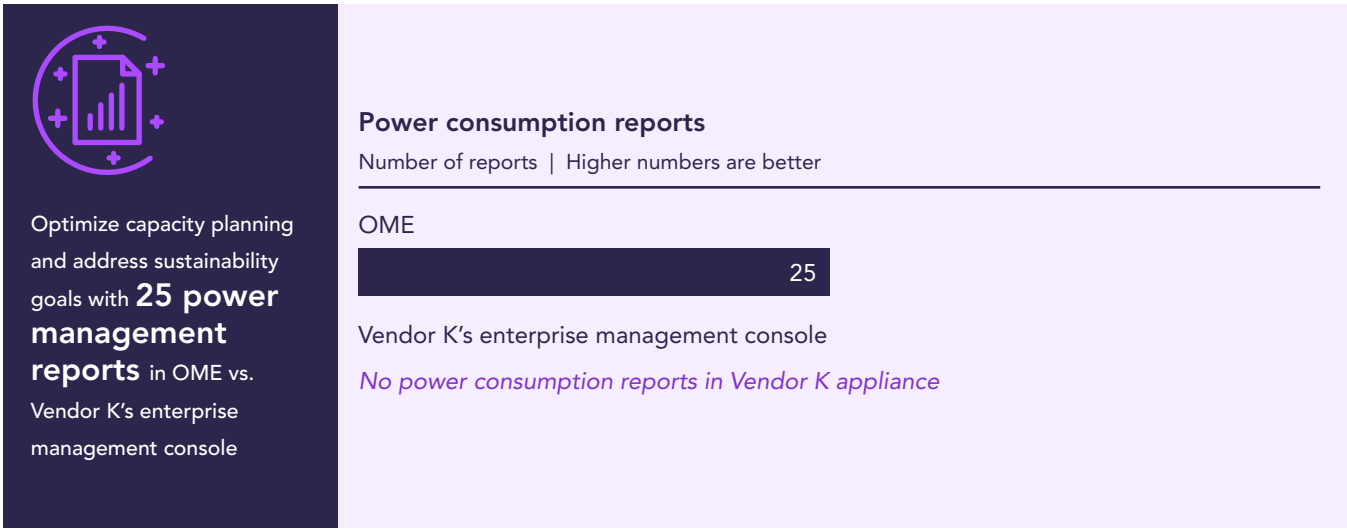

Figura 2. Confronto tra il numero di report sulla gestione dell'alimentazione disponibili in OME e nella console di gestione aziendale del Vendor K. Un numero maggiore di report è l'opzione migliore. Fonte: Principled Technologies

Per ottimizzare ulteriormente la gestione dell'alimentazione, il plug-in OME Power Manager rende possibile per gli amministratori visualizzare fino al **triplo delle metriche rispetto alla console di gestione aziendale del Vendor K** (v. la Figura 3). OME offre 21 metriche diverse, tra cui l'uso dell'alimentazione da parte dei singoli componenti, il flusso d'aria e l'utilizzo dei componenti, mentre la console di gestione aziendale del Vendor K offre soltanto 7 metriche diverse.

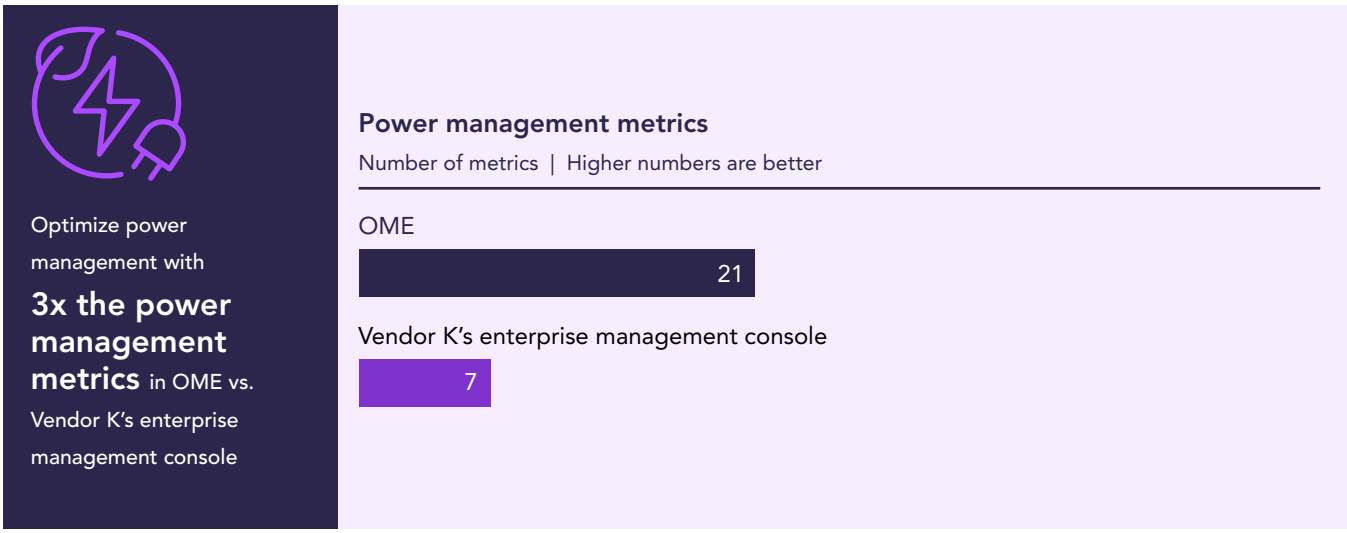

Figura 3. Confronto tra il numero di metriche di gestione dell'alimentazione disponibili in OME e nella console di gestione aziendale del Vendor K. Un numero maggiore di metriche è l'opzione migliore. Fonte: Principled Technologies.

Analisi delle emissioni e dell'impronta di carbonio

Una funzionalità fondamentale per la sostenibilità **inclusa in OME è rappresentata dal calcolatore dell'utilizzo delle emissioni di carbonio e dallo strumento di pianificazione della capacità**. Questo strumento aiuta le organizzazioni a effettuare una stima delle proprie emissioni di gas serra, fornendo valori predefiniti per i costi energetici e le emissioni di carbonio per unità di energia consumata. Questa funzione consente anche la personalizzazione, offrendo alle organizzazioni la possibilità di inserire valori per i costi energetici e le emissioni di carbonio della propria regione per i dati specifici del modello di consumo del data center.
La console di gestione aziendale del Vendor K non dispone di una funzionalità analoga, fattore che può minare la capacità di un'organizzazione di effettuare la pianificazione tenendo conto della sostenibilità.

Ridurre il carico di gestione con solide funzionalità di monitoraggio e gestione

Con la crescita dell'infrastruttura, possono aumentare anche le responsabilità degli amministratori del data center. Scegliendo strumenti di gestione dei server che automatizzino determinate attività e migliorino la gestione quotidiana, le organizzazioni possono aiutare gli amministratori a diventare più efficienti e garantire loro più tempo per pianificare il futuro. Abbiamo riscontrato che il portafoglio di gestione dei server Dell offe una serie di funzionalità che semplificano i compiti degli amministratori. La Tabella 4 fornisce un riepilogo delle principali funzioni di facilità di utilizzo disponibili nel portafoglio Dell rispetto agli strumenti di gestione del Vendor K.

Tabella 4: Panoramica delle principali funzioni di facilità di utilizzo disponibili negli strumenti di gestione Dell rispetto agli strumenti del Vendor K. Fonte: Principled Technologies.

Funzione	Vantaggi principali degli strumenti di gestione Dell	Svantaggio degli strumenti di gestione del Vendor K
Maggiori funzionalità remote del BIOS	Gestione remota più semplice con **51 funzionalità remote del BIOS in iDRAC9**	Il BMC del Vendor K offre **soltanto 1** funzionalità remota del BIOS
Modifiche alla configurazione del BIOS più semplici	**87% di tempo in meno e metà dei passaggi** richiesti per modificare la configurazione del BIOS	Il Vendor K rende necessario **l'intervento manuale degli amministratori** per apportare modifiche all'interno delle utilità di sistema
Importazione/esportazione della configurazione completa dei server	**Configurazione più rapida di vari server identici** con la possibilità di esportare/importare le impostazioni di configurazione per server completamente configurati	Il Vendor K offre **soltanto il backup e il ripristino del BMC per ogni singolo server**
Aggiornamenti pianificati automatizzati	IDRAC9 offre agli amministratori la possibilità di **pianificare aggiornamenti automatizzati** da un repository durante una finestra di manutenzione senza ulteriori interventi da parte degli amministratori	Il BMC del Vendor K **non offre aggiornamenti automatizzati pianificati**
Panoramica completa dello stato dello storage	iDRAC9 offre una rappresentazione visiva dello stato dello storage, per **identificare rapidamente i dischi con stato di allerta**	Il BMC del Vendor K **non** fornisce una panoramica simile
Telemetria in streaming	iDRAC9 **fornisce la telemetria per il doppio di categorie di metriche, per un totale di 8 categorie**	Il BMC del Vendor K fornisce telemetria **soltanto per 4 categorie**
Visualizzazione delle connessioni	La visualizzazione delle connessioni in iDRAC9 **fornisce dettagli sulla mappatura fisica delle porte degli switch alle porte della rete del server e alle connessioni dedicate delle porte iDRAC**	Il BMC del Vendor K **non fornisce informazioni sulla connessione fisica** agli switch a monte
Scalabilità	OME **può gestire fino a 8.000 dispositivi**[5]	Il Vendor K può gestire **soltanto** un massimo di **1.000 dispositivi**

Funzione	Vantaggi principali degli strumenti di gestione Dell	Svantaggio degli strumenti di gestione del Vendor K
Azioni basate sugli avvisi	OME fornisce **il doppio di azioni basate sugli avvisi (12)** che attivano azioni in base all'input di un avviso	Il Vendor K offre soltanto **4 azioni basate sugli avvisi**
Architettura dei plug-in	OME offre la possibilità di **espandere le funzionalità con plug-in** che gli amministratori possono aggiungere alla console senza la necessità di ulteriori applicazioni da gestire	La console di gestione aziendale del Vendor K **non offre un'architettura basata sui plug-in** per l'espandibilità
Monitoraggio dei dispositivi di terze parti	OME **supporta il monitoraggio di server e dispositivi di terze parti**	La console di gestione aziendale del Vendor K **non supporta** il monitoraggio di server e dispositivi di terze parti
Reporting	OME offre agli amministratori **42 report integrati** con personalizzazione, in modo che gli amministratori possano selezionare in modo granulare i dati più importanti per i loro scopi	La console di gestione aziendale del Vendor K **non prevede la creazione di report nativi**

Gestione remota

Con iDRAC9, gli amministratori non devono accedere al data center per effettuare qualsiasi modifica. iDRAC9 offre 51 funzionalità remote del BIOS per garantire agli amministratori la libertà di apportare più modifiche dall'esterno del data center, rispetto a una sola per il BMC del Vendor K, che assicura agli amministratori un controllo notevolmente più granulare sulla configurazione del BIOS da qualsiasi luogo (v. la Figura 4).

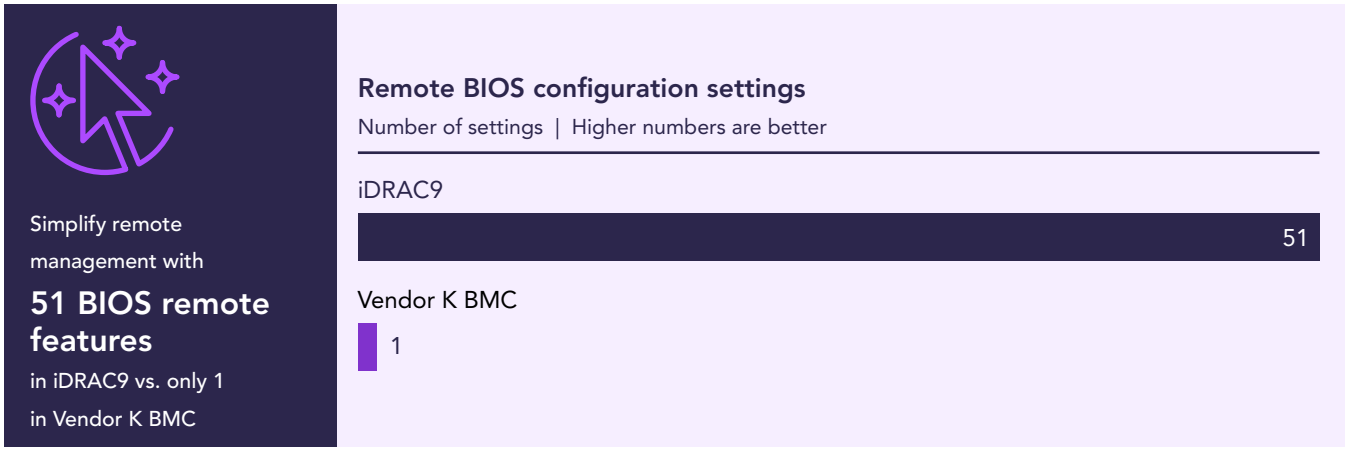

Figura 4. Confronto delle funzionalità remote del BIOS offerte da ciascun strumento di gestione. Un maggior numero di funzionalità è l'opzione migliore. Fonte: Principled Technologies.

Esecuzione di modifiche alla configurazione

Con iDRAC9, gli amministratori possono modificare le impostazioni di configurazione del BIOS ed eseguire l'aggiornamento per il riavvio successivo senza che sia richiesta un'ulteriore presenza da parte degli amministratori, mentre il BMC del Vendor K rende necessario effettuare le modifiche all'interno delle utilità di sistema, nonché l'intervento manuale dell'amministratore durante la modifica. Come illustrato nella Figura 5, l'esecuzione della modifica alla configurazione del BIOS per un riavvio pianificato con iDRAC9 ha richiesto l'87% di tempo in meno e la metà dei passaggi rispetto al BMC del Vendor K. Estrapolando questi risparmi per deployment di grandi dimensioni, si riduce maggiormente il tempo di amministrazione. Ad esempio, in un deployment di 100 server, gli amministratori potrebbero risparmiare oltre 6 ore nella modifica degli elementi di configurazione del BIOS.

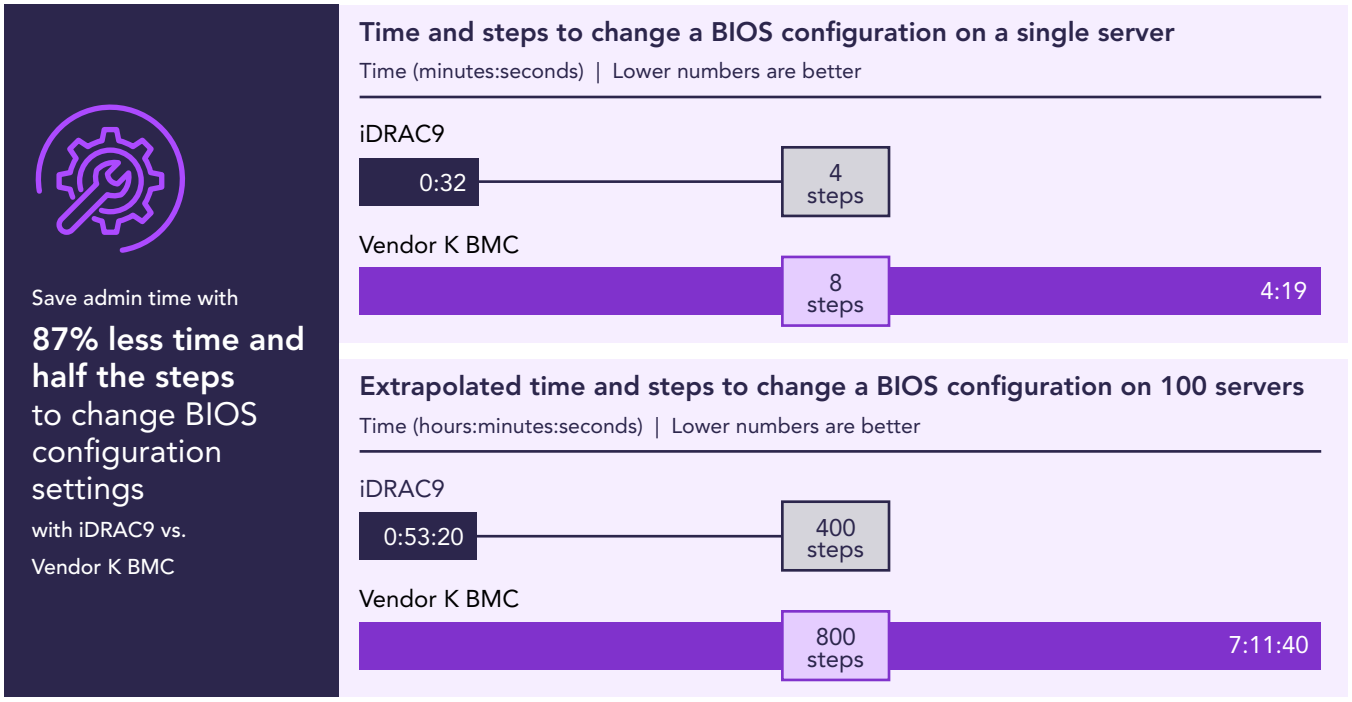

Figura 5. Tempo richiesto per modificare le impostazioni di configurazione del BIOS ed eseguire l'aggiornamento per il riavvio successivo per un singolo server e tempo estrapolato per 100 server. Meno tempo e meno passaggi sono l'opzione migliore. Fonte: Principled Technologies.

Impostazione delle azioni basate sugli avvisi

Gli amministratori possono utilizzare meglio il proprio tempo quando non sono relegati alla scrivania, monitorando lo stato dell'ambiente. Come illustrato nella Figura 6, OME offre 12 opzioni basate sulle policy per le azioni basate sugli avvisi, in modo che la mitigazione dei problemi si avvii automaticamente ogni volta che l'ambiente raggiunge determinate soglie. Al contrario, la console di gestione aziendale del Vendor K rende possibile per gli amministratori configurare solo quattro eventi basati sugli avvisi.

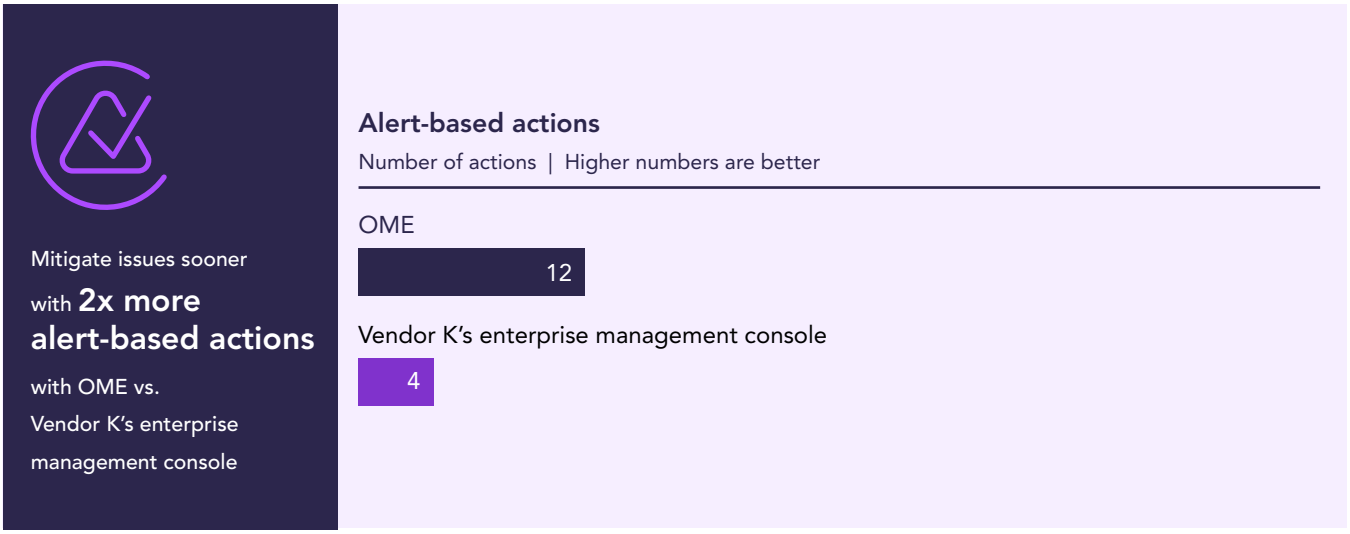

Figura 6. Confronto dell'azione basata su avvisi offerta da ogni strumento di gestione. Un maggior numero di azioni è l'opzione migliore. Fonte: Principled Technologies.

Informazioni su Dell Technologies OpenManage Enterprise

OME è una console per la gestione dei sistemi di tipo one-to-many per il data center. La console offre un'interfaccia grafica utente HTML5 moderna e viene implementata come Virtual Appliance per ambienti VMware ESXi™, Microsoft Hyper-V e KVM (Kernel-Based Virtual Machine). OME è in grado di rilevare e inventariare le reti IPV4 e IPV6 per un massimo di 8.000 dispositivi, tra cui server rack Dell, server tower Dell e server blade e chassis Dell.[6] In un recente studio di PT, abbiamo rilevato che un ambiente Dell con OME e OpenManage Enterprise Modular (OME-M) può ridurre il tempo necessario per apportare modifiche alle VLAN ed evitare interventi durante gli aggiornamenti pianificati del firmware.[7]

Ulteriori informazioni su OME sono disponibili all'indirizzo https://www.dell.com/en-us/lp/dt/open-manage-enterprise.

Gestione basata sul cloud con APEX AIOps Infrastructure Observability (in precedenza CloudIQ)

Gli strumenti integrati e le console di gestione aziendale non sono gli unici strumenti presenti nel portafoglio di gestione dei server Dell. Con APEX AIOps Infrastructure Observability (in precedenza CloudIQ), gli amministratori dispongono di un altro strumento automatizzato e di facile utilizzo con cui tenere sotto controllo l'integrità e la sicurezza dell'infrastruttura, questa volta dal cloud.

Funzionalità di sicurezza aggiuntive disponibili in APEX AIOps Infrastructure Observability (in precedenza CloudIQ)

APEX AIOps Infrastructure Observability (in precedenza CloudIQ) offre diverse funzionalità di sicurezza che possono rafforzare ulteriormente l'organizzazione per far fronte gli attacchi. La Tabella 5 evidenzia alcune delle principali funzionalità di sicurezza.

Tabella 5: Panoramica delle principali funzionalità di sicurezza disponibili in APEX AIOps Infrastructure Observability (in precedenza CloudIQ). Fonte: Principled Technologies.

Funzione	Come funziona APEX AIOps Infrastructure Observability (in precedenza CloudIQ) per la protezione dell'ambiente
Avvisi sul livello di rischio per la sicurezza informatica	Fornisce informazioni automatizzate per la sicurezza informatica con **avvisi specifici sul livello di rischio per la sicurezza**, in modo che gli amministratori possano reagire più rapidamente e risolvere velocemente i problemi per mantenere i dati al sicuro
Configurazione della sicurezza basata sulle policy	Offre **impostazioni di configurazione della sicurezza basate sulle policy e modelli facili da applicare** con cui l'amministratore può garantire che vengano implementate le impostazioni delle best practice per la sicurezza, proteggendo l'ambiente PowerEdge
Consulenza sulla sicurezza informatica	Fornisce **report sugli avvisi di sicurezza pertinenti**, offrendo dettagli specifici sulle vulnerabilità e suggerimenti per la correzione, grazie ai quali è possibile agire rapidamente per colmare eventuali lacune della sicurezza

Informazioni su APEX AIOps Infrastructure Observability (in precedenza CloudIQ)

APEX AIOps Infrastructure Observability (in precedenza CloudIQ) è uno strumento AIOps basato sul cloud che offre "monitoraggio proattivo, apprendimento automatico e analisi predittiva" per un elevato numero di prodotti e servizi Dell, tra cui server, storage, appliance di protezione dei dati e infrastruttura iperconvergente.[8] In uno studio di Principled Technologies del 2022, abbiamo rilevato che CloudIQ ha avuto un impatto trascurabile sulla larghezza di banda della rete, ma al contempo ha reso possibile monitorare la telemetria, lo stato di integrità, gli avvisi e l'inventario da un'unica console.[9]

Ulteriori informazioni su APEX AIOps Infrastructure Observability (in precedenza CloudIQ) sono disponibili all'indirizzo https://www.dell.com/en-us/dt/apex/aiops.htm.

Ulteriori funzionalità di sostenibilità ed efficienza disponibili in APEX AIOps Infrastructure Observability (in precedenza CloudIQ)

APEX AIOps Infrastructure Observability (in precedenza CloudIQ) offre inoltre funzionalità che aumentano la sostenibilità e l'efficienza e si integrano con iDRAC9 e OME per semplificare il monitoraggio dello stato dell'ambiente PowerEdge da parte degli amministratori. La Tabella 6 mette in evidenza alcune di queste funzionalità.

Tabella 6: Panoramica delle funzioni di gestione della sostenibilità e di facilità di utilizzo disponibili in APEX AIOps Infrastructure Observability (in precedenza CloudIQ). Fonte: Principled Technologies.

Funzione	Vantaggi principali con APEX AIOps Infrastructure Observability (in precedenza CloudIQ)
Analisi dell'impronta di carbonio	Disponibile nella sezione Monitoraggio, questo strumento offre una visualizzazione più ampia e **può prevedere le emissioni di carbonio** in diversi ambienti
Visualizzazioni delle prestazioni	Fornisce visualizzazioni delle prestazioni e grafici delle anomalie e dell'utilizzo per **avvisare gli amministratori al primo segnale di problemi**
Report sulla conformità personalizzati	Offre agli utenti la possibilità di **creare report di conformità personalizzati** per i dispositivi selezionati
Report personalizzabili sulle prestazioni e sull'inventario	Fornisce **opzioni di creazione di report personalizzati** per le prestazioni dei server e i dati di inventario, offrendo agli amministratori un maggiore controllo sulle metriche delle prestazioni e dei dispositivi che sono interessati a monitorare
Pianificazione dei job di azioni di alimentazione	Esegui azioni di alimentazione, come il Power Capping su più server Dell PowerEdge monitorati in **soli 35 secondi e 6 passaggi**
Pianificazione degli aggiornamenti del firmware	Pianifica gli aggiornamenti del firmware PowerEdge per più server monitorati in **soli 41 secondi e 9 passaggi**

Conclusioni

Nel nostro confronto tra funzionalità di sicurezza, sostenibilità e gestione/monitoraggio, abbiamo riscontrato che il portafoglio di strumenti di gestione dei server Dell fornisce funzionalità di gestione e monitoraggio più solide rispetto al portafoglio del Vendor K. Nell'ambito della sicurezza, iDRAC9 offre più funzionalità, tra cui il blocco dinamico del sistema e l'autenticazione a più fattori, che il Vendor K non offre affatto. Inoltre, iDRAC9 riduce significativamente il tempo necessario per disabilitare le porte USB per ridurre la vulnerabilità dei dati.

Grazie all'analisi dell'impronta di carbonio e a solidi strumenti di gestione dell'alimentazione, abbiamo rilevato che con OME le organizzazioni possono pianificare meglio il raggiungimento degli obiettivi di sostenibilità rispetto a quanto possono fare utilizzando la console di gestione aziendale del Vendor K. Abbiamo inoltre riscontrato che il portafoglio di gestione dei server Dell offre maggiore automazione e più opzioni di gestione remota, riducendo il tempo e l'impegno richiesti agli amministratori per determinati compiti di monitoraggio e manutenzione di routine. Questi vantaggi in termini di funzionalità di sicurezza, sostenibilità e gestione/monitoraggio rendono il portafoglio di gestione dei server Dell un'opzione interessante per le organizzazioni che sono alla ricerca di un data center più efficiente e sicuro.

---

1. Harvard Business Review, "The Devastating Business Impact of a Cyber Breach", consultato il 10 aprile 2024, https://hbr.org/2023/05/the-devastating-business-impacts-of-a-cyber-breach.
2. Dell, "Integrated Dell Remote Access Controller (iDRAC)", consultato il 17 maggio 2024, https://www.dell.com/en-us/lp/dt/open-manage-idrac.
3. Nota: la disabilitazione delle porte USB del Vendor K è personalizzabile, anche se ciò significa che gli amministratori devono selezionare ciascuna porta da disabilitare, anziché il gruppo.
4. DOE, "DOE Announces $40 Million for More Efficient Cooling for Data Centers", consultato il 20 maggio 2024, https://www.energy.gov/articles/doe-announces-40-million-more-efficient-cooling-data-centers.
5. Dell, "OpenManage Enterprise Support Matrix", consultato il 21 maggio 2024, https://www.dell.com/support/kbdoc/en-us/article/lkbprint?ArticleNumber=000217909&AccessLevel=10&Lang=en.
6. Dell, "OpenManage Enterprise", consultato il 17 maggio 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", consultato il 17 maggio 2024, https://www.principledtechnologies.com/Dell/PowerEdge-MX-OME-OME-M-0124.pdf.
8. Dell, "APEX AIOps: Tame IT complexity in your digital business", consultato l'11 giugno 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", consultato il 9 aprile 2024, https://www.principledtechnologies.com/dell/CloudIQ-network-0422.pdf.

Leggi le basi scientifiche di questo report

Visualizza la versione originale in inglese di questo report

Questo progetto è stato commissionato da Dell Technologies.

Principled Technologies®

Facts matter.®

Principled Technologies è un marchio registrato di Principled Technologies, Inc.
Tutti gli altri nomi di prodotto sono marchi dei rispettivi proprietari. Per ulteriori informazioni, consultare le basi scientifiche di questo report.