



Réduisez la vulnérabilité des données

en diminuant de **85 %** le temps nécessaire → la désactivation des ports USB frontaux

dans iDRAC9, par rapport au BMC du fournisseur K



Réduisez les émissions de carbone avec

25 rapports de consommation électrique personnalisables

dans OME, contre 0 dans la console de gestion d'entreprise du fournisseur K



Planifiez des mises → jour automatiques

du firmware en seulement 41 secondes

dans APEX AIOps Infrastructure Observability (anciennement CloudIQ)

Les outils de gestion des serveurs Dell peuvent vous aider à améliorer la sécurité, le développement durable et l'efficacité de la gestion

par rapport aux outils de gestion de serveurs comparables du fournisseur K

À mesure que les datacenters continuent de croître, les tâches de l'administrateur évoluent également. Une infrastructure qui offre des outils de gestion et de surveillance natifs robustes et automatisés peut faciliter la sécurisation et la gestion du datacenter pour les administrateurs souvent surchargés. Nous avons comparé les caractéristiques et les capacités des portefeuilles de gestion provenant de Dell et d'un concurrent que nous appellerons le fournisseur K :

Tableau 1 : Les outils de gestion que nous avons testés.

	Dell	Fournisseur K
Gestion des serveurs intégrée/à distance	Dell Technologies Integrated Dell Remote Access Controller 9 (iDRAC9)	Baseboard Management Controller (BMC) du fournisseur K
Console de gestion des appareils un-à-plusieurs	Dell Technologies OpenManage™ Enterprise (OME) APEX AIOps Infrastructure Observability (anciennement CloudIQ)	Console de gestion d'entreprise du fournisseur K

Nous avons constaté que iDRAC9, OME et APEX AIOps Infrastructure Observability (anciennement CloudIQ) offraient une gamme solide d'outils de gestion qui pouvaient améliorer la sécurité, faciliter les mesures de développement durable et faciliter les tâches d'administration quotidiennes par rapport à l'utilisation d'outils similaires du fournisseur K.

Renforcer la sécurité du datacenter

Pour les organisations qui stockent des données clients sensibles, la menace persistante des cyberattaques exige de puissantes fonctionnalités de sécurité de bout en bout pour s'assurer que les données ne finissent pas entre de mauvaises mains. En fait, jusqu'à « 83 % des organisations ont subi au moins une violation de données en 2022 »,¹ une statistique qui montre à quel point il est important de gérer les données des clients avec précaution pour renforcer la confiance des consommateurs.

Pour protéger votre organisation et ses données contre de coûteuses cyberattaques, les outils de gestion Dell offrent de puissantes fonctionnalités de sécurité intégrées au serveur via iDRAC9 et dans la console globale et le logiciel de gestion Cloud. Ci-dessous, nous explorons certaines des principales fonctionnalités de sécurité utilisées par les outils Dell pour protéger votre système et les comparons aux offres correspondantes du fournisseur K.

Sécurité intégrée

Des fonctionnalités de sécurité intégrées à chaque serveur Dell PowerEdge via iDRAC9 empêchent les acteurs malveillants d'accéder aux données. Voici trois de ces importantes fonctionnalités :

- **Verrouillage dynamique du système** : le verrouillage du système empêche toute activité involontaire ou malveillante de modifier les paramètres du BIOS du système, de l'iDRAC et du firmware. Le terme « dynamique » fait référence à la capacité de mettre en place ces capacités une seule fois, puis de les activer au besoin. (Remarque : Cette fonctionnalité est disponible avec les licences iDRAC9 Enterprise et Datacenter.)
- **Authentification multifacteur (MFA)** : la MFA invite les administrateurs à saisir un code secret en plus de leurs informations d'identification de connexion pour renforcer la sécurité.
- **Activation/désactivation de port USB dynamique** : l'activation/la désactivation de port USB dynamique permet aux administrateurs de contrôler l'accès au serveur via un port USB. Le terme « dynamique » renvoie à la possibilité d'activer et de désactiver ces ports USB sans redémarrer le serveur ou le système d'exploitation. Tant que l'administrateur ne fournit pas l'accès, personne ne peut brancher une clé USB ou un clavier pour modifier les paramètres de configuration du système, du système d'exploitation ou du BIOS.

Comme le montre le Tableau 2, le fournisseur K n'offre ni verrouillage dynamique du système ni authentification multifacteur, et ses fonctionnalités USB dynamiques nécessitent une interruption du système (qui peut s'avérer très coûteuse pour les organisations), ce qui rend cette solution moins utile et plus coûteuse que la solution Dell.

Tableau 2 : Comparaison des fonctionnalités de sécurité intégrées offertes par les outils de gestion des serveurs. Source : Principled Technologies.

	iDRAC9	Fournisseur K BMC
Verrouillage dynamique du système	✓	✗
MFA	✓	✗
Dynamic USB	✓	✓*

*Nécessite une interruption du système

À propos de Dell Technologies Integrated Dell Remote Access Controller 9

Les serveurs Dell PowerEdge™ comprennent iDRAC9 avec Dell Lifecycle Controller pour fournir des fonctions d'administration de systèmes qui incluent des alertes système et des fonctionnalités de gestion à distance. Selon Dell, les principaux avantages de iDRAC9 sont les suivants :

- Automatisation évolutive. Des API basées sur des normes telles que Redfish et des outils de script robustes tels que RedHat Ansible, Python, PowerShell et Terraform vous permettent de gérer des milliers de serveurs.
- Prise en charge intégrée, offrant une vue de l'intégrité et de l'état des serveurs avec une surveillance de plusieurs milliers de paramètres
- Puissantes fonctionnalités et options de sécurité²

Pour en savoir plus sur les fonctionnalités fournies par iDRAC9, rendez-vous sur <https://www.dell.com/en-us/lp/dt/open-manage-idrac>.

La Figure 1 illustre les résultats de notre comparaison pratique lors de l'utilisation d'iDRAC9 et du BMC du fournisseur K pour désactiver dynamiquement les ports USB.

Avec iDRAC9, nous avons constaté que les administrateurs pouvaient désactiver les ports USB frontaux sur un seul serveur en seulement 41 secondes, moyennant 4 étapes. En comparaison, avec le BMC du fournisseur K, le même processus prendrait 4 minutes 43 secondes et 8 étapes par serveur. Autrement dit, pour chaque serveur, **il faut 85 % de temps en moins et deux fois moins d'étapes pour désactiver les ports USB frontaux avec la solution Dell.**³ À l'échelle d'un datacenter, les gains de temps s'accumulent. Pour un déploiement de 100 serveurs, les administrateurs peuvent gagner 6 heures et 43 minutes en utilisant iDRAC9, comparativement au BMC du fournisseur K.

Non seulement ces fonctionnalités sont plus faciles et plus rapides d'accès avec l'iDRAC9 qu'avec le BMC du fournisseur K, mais avec iDRAC9, les administrateurs peuvent maintenir les serveurs en production (sans interruption de service) tout en activant ou désactivant ces fonctionnalités. La méthode du fournisseur K implique des interruptions de service, qui peuvent entraîner des coûts importants, et suppose de modifier à chaque fois la configuration du système.

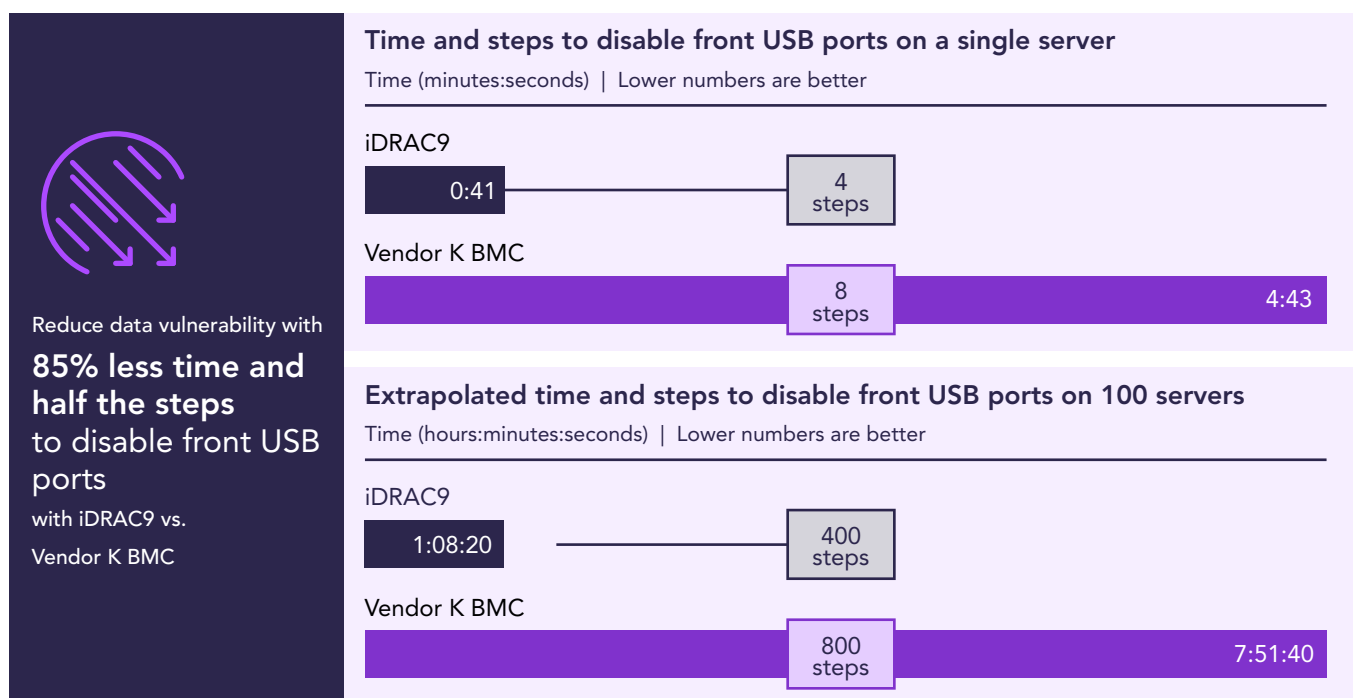


Figure 1 : Temps nécessaire pour désactiver les ports USB frontaux pour un seul serveur, avec extrapolation du délai de désactivation des ports USB frontaux pour 100 serveurs. Moins de temps et moins d'étapes pour plus d'efficacité. Source : Principled Technologies.

Maintenir la sécurité grâce à une gestion simplifiée des informations d'identification dans OME




OME fournit aux administrateurs un moyen simple de gérer la rotation des mots de passe d'iDRAC9. Plutôt que d'exiger un compte administrateur statique et connu, OME gère les iDRAC via un compte de service dans lequel les clients sélectionnent la règle de rotation des mots de passe requise, dont le mot de passe n'est jamais divulgué. Les administrateurs peuvent aussi confier cette gestion à un tiers externe. **La console de gestion d'entreprise du fournisseur K ne dispose pas de fonctionnalités de rotation des mots de passe internes, ce qui oblige les administrateurs à s'appuyer sur un tiers s'ils souhaitent cette fonctionnalité.** Nous avons confirmé que les serveurs gérés par iDRAC9 étaient intégrés au compte OME avec des privilèges d'administrateur complets pour faciliter la gestion des informations d'identification.

Remarque : Les graphiques de ce rapport utilisent des échelles différentes. Faites attention à la plage de données de chaque graphique lors de la comparaison.

Atteindre les objectifs de développement durable

Selon le département de l'Énergie des États-Unis, « les datacenters représentent environ 2 % de la consommation électrique totale aux États-Unis, tandis que le refroidissement du datacenter peut représenter jusqu'à 40 % de sa consommation énergétique globale ».4 À mesure que les données continuent de proliférer, ces chiffres ne feront qu'augmenter, ce qui rend la gestion thermique et de l'alimentation essentielle pour réduire les coûts du datacenter et atteindre les objectifs de développement durable, afin de réduire les émissions de carbone. Pour aider les organisations à réduire leur consommation électrique, OME intègre plusieurs fonctionnalités de surveillance et de gestion de la consommation électrique. Le Tableau 3 met en évidence les principaux avantages de ces fonctionnalités, que nous décrivons plus en détail ci-dessous.

Tableau 3 : Présentation des principales fonctionnalités de développement durable disponibles dans OME et la console de gestion d'entreprise du fournisseur K. Source : Principled Technologies.

Fonctionnalité	Avantages clés des outils de gestion Dell	Inconvénients avec les outils de gestion du fournisseur K
 Calculateur d'utilisation des émissions de carbone et outil de planification de la capacité	Estimation des émissions de gaz à effet de serre avec des valeurs personnalisables pour vous aider à atteindre vos objectifs de développement durable	La console de gestion d'entreprise du fournisseur K n'offre aucune fonctionnalité comparable
 Règles de seuil énergétique	Le plug-in OME Power Manager peut gérer les plafonds d'alimentation pour les appareils ou les groupes d'appareils qui appliquent des limites d'alimentation lorsqu'ils sont activés	La console de gestion d'entreprise du fournisseur K n'offre aucune fonctionnalité comparable
 Gestion thermique et de l'alimentation automatisée	Options de règles à déclenchement électrique et thermique , avec la possibilité de déclencher une action lorsque le serveur dépasse un seuil de consommation électrique ou de température	La console de gestion d'entreprise du fournisseur K n'offre aucune fonctionnalité comparable
 Tableau de bord de la consommation électrique	Le plug-in OME Power Manager permet d'accéder rapidement aux données de Power Manager, offrant 2,75 fois plus de mesures, avec un total de 11.	La console de gestion d'entreprise du fournisseur K ne propose que 4 mesures sur le tableau de bord
 Rapports de consommation électrique	Le plug-in OME Power Manager fournit 25 rapports personnalisables par défaut et supplémentaires	La console de gestion d'entreprise du fournisseur K ne fournit aucun rapport de gestion de l'alimentation
 Mesures de gestion de l'alimentation	Jusqu'à trois fois plus de mesures , offrant une analyse plus détaillée de la gestion de la consommation électrique avec 21 mesures.	La console de gestion d'entreprise du fournisseur K ne propose que 7 mesures liées à la gestion de l'alimentation

Gestion thermique et de l'alimentation automatisée

OME Power Manager assure une gestion automatisée de l'alimentation et de la température grâce à des options de règles statiques à déclenchement électrique et thermique, qui permettent aux administrateurs de définir des limites de consommation électrique ou des seuils de température afin de réduire les coûts de refroidissement, de soutenir les stratégies de réduction de l'alimentation et de réagir face aux événements thermiques. En revanche, le **fournisseur K n'offre aucune fonctionnalité automatisée de gestion de l'alimentation et de la température**. Sans la possibilité de définir des limites basées sur la température, la consommation d'énergie pourrait dépasser les attentes et rendre difficile la planification en tenant compte du développement durable. L'optimisation de la consommation électrique est une stratégie importante pour atteindre les objectifs de développement durable. Le plugin OME Power Manager offre **25 rapports par défaut et/ou personnalisables liés à Power Manager** (17 dans les appareils Power Manager et 8 dans les groupes Power Manager) qui permettent aux administrateurs d'optimiser la planification de la capacité et de gérer l'alimentation pour optimiser l'efficacité. **La console de gestion d'entreprise du fournisseur K ne propose aucun rapport de gestion de l'alimentation similaire** (voir Figure 2).

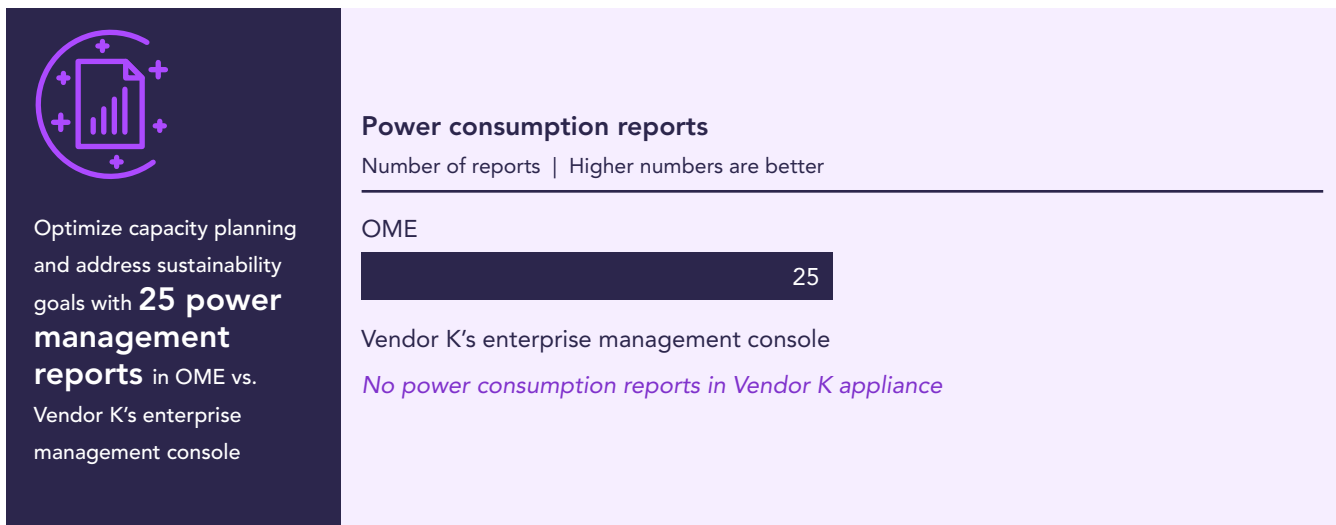


Figure 2 : Comparaison du nombre de rapports de gestion de l'alimentation disponibles dans OME et dans la console de gestion d'entreprise du fournisseur K. Des rapports plus nombreux offrent plus d'efficacité. Source : Principled Technologies

Pour optimiser davantage la gestion de l'alimentation, le plug-in OME Power Manager permet aux administrateurs d'afficher jusqu'à **3 fois plus de mesures que la console de gestion d'entreprise du fournisseur K** (voir Figure 3). OME fournit 21 mesures différentes, y compris la consommation d'énergie par composant individuel, le flux d'air et l'utilisation des composants, tandis que la console de gestion d'entreprise du fournisseur K ne fournit que 7 mesures différentes.

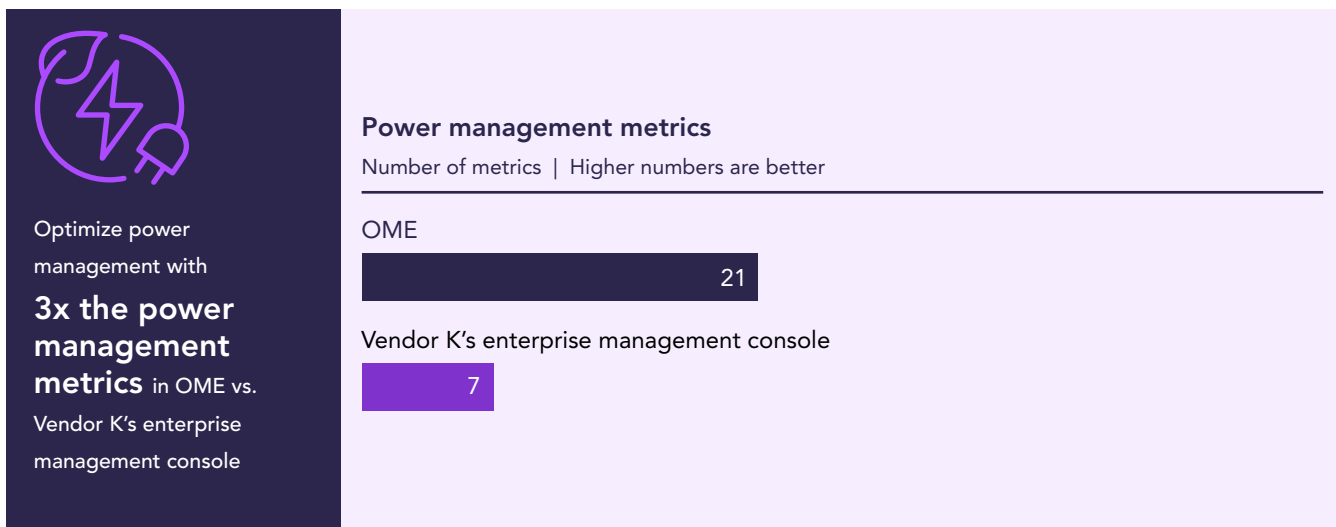


Figure 3 : Comparaison du nombre de mesures de gestion de l'alimentation disponibles dans OME et dans la console de gestion d'entreprise du fournisseur K. Un plus grand nombre de mesures offre plus d'efficacité. Source : Principled Technologies.









Émissions de carbone et analyse de l'empreinte carbone





L'une des principales fonctionnalités favorables au développement durable **d'OME est un calculateur d'utilisation des émissions de carbone et un outil de planification de la capacité**. Cet outil aide les organisations à estimer leurs émissions de gaz à effet de serre, en fournissant des valeurs par défaut pour les coûts énergétiques et les émissions de carbone par unité d'énergie consommée. Cette fonctionnalité permet également la personnalisation, ce qui offre aux organisations la possibilité de saisir des valeurs pour les coûts énergétiques et les émissions de carbone de leur propre région pour les données spécifiques au modèle de consommation de leur datacenter. **La console de gestion d'entreprise du fournisseur K ne dispose pas d'une fonctionnalité comparable**, ce qui peut entraver la capacité d'une organisation à planifier en tenant compte du développement durable.

Allégement de la charge de gestion avec des fonctionnalités de surveillance et de gestion robustes

À mesure que l'infrastructure se développe, les responsabilités de l'administrateur du datacenter évoluent également. En choisissant des outils de gestion des serveurs qui automatisent certaines tâches et améliorent la gestion quotidienne, les organisations peuvent aider les administrateurs à gagner en efficacité et leur donner plus de temps pour planifier l'avenir. La gamme de solutions de gestion de serveurs Dell propose un certain nombre de fonctionnalités qui simplifient les tâches de l'administrateur. Le Tableau 4 fournit un récapitulatif des principales fonctionnalités faciles d'utilisation disponibles dans la gamme de gestion Dell par rapport aux outils de gestion du fournisseur K.

Tableau 4 : Présentation des principales fonctionnalités faciles d'utilisation disponibles dans les outils de gestion Dell par rapport aux outils de gestion du fournisseur K. Source : Principled Technologies.

Fonctionnalité	Avantages clés des outils de gestion Dell	Inconvénients avec les outils de gestion du fournisseur K
 Plus de fonctionnalités de BIOS distant	Gestion à distance simplifiée avec 51 fonctionnalités de BIOS distantes dans iDRAC9	Le BMC du fournisseur K offre une seule fonctionnalité de BIOS à distance.
 Modifications simplifiées de la configuration du BIOS	87 % de temps en moins et deux fois moins d'étapes pour apporter une modification à la configuration du BIOS	Le fournisseur K nécessite une intervention manuelle de l'administrateur pour apporter des modifications à partir des utilitaires système
 Importation/exportation complète de la configuration du serveur	Configuration plus rapide de plusieurs serveurs identiques avec la possibilité d'exporter/importer les paramètres de configuration pour un serveur entièrement configuré.	Le fournisseur K fournit uniquement la sauvegarde et la restauration du contrôleur BMC pour chaque serveur individuel
 Mises à jour planifiées automatisées	iDRAC9 permet aux administrateurs de planifier des mises à jour automatisées à partir d'un référentiel pendant une fenêtre de maintenance sans intervention supplémentaire de l'administrateur	Le BMC du fournisseur K ne propose pas de mises à jour automatisées planifiées
 Aperçu complet de l'état du stockage	iDRAC9 fournit une représentation visuelle de l'état du stockage, pour identifier rapidement les disques avec un état d'alerte	Le BMC du fournisseur K ne fournit pas une vue similaire
 Téléométrie en streaming	iDRAC9 fournit la téléométrie pour 2 fois plus de catégories de mesures, avec 8 catégories au total	Le BMC du fournisseur K fournit la téléométrie pour seulement 4 catégories .
 Affichage des connexions	La fonction Affichage des connexions dans iDRAC9 établit un mappage physique détaillé entre les ports du commutateur, et les ports réseau du serveur et les connexions des ports dédiés à l'iDRAC	Le BMC du fournisseur K ne fournit aucune information de connexion physique aux commutateurs en amont
 l'évolutivité	OME est capable de gérer jusqu'à 8 000 appareils³	Le fournisseur K ne peut gérer que 1 000 appareils au maximum

Fonctionnalité	Avantages clés des outils de gestion Dell	Inconvénients avec les outils de gestion du fournisseur K
 Actions basées sur des alertes	OME fournit 2 fois plus d'actions basées sur des alertes (12 au total) qui déclenchent des actions en fonction des entrées d'une alerte	Le fournisseur K propose seulement 4 actions basées sur des alertes
 Architecture de plug-ins	OME offre la possibilité d'étendre les fonctionnalités avec des plug-ins que les administrateurs peuvent ajouter à la console sans avoir besoin d'applications supplémentaires à gérer	La console de gestion d'entreprise du fournisseur K n'offre pas d'architecture basée sur des plug-ins pour plus d'évolutivité
 Surveillance des appareils tiers	OME prend en charge la surveillance des appareils et des serveurs tiers	La console de gestion d'entreprise du fournisseur K ne prend pas en charge la surveillance des appareils et des serveurs tiers
 Rapports	OME propose 42 rapports intégrés avec personnalisation aux administrateurs, ce qui leur permet de sélectionner de manière granulaire les données les plus importantes pour leurs besoins.	La console de gestion d'entreprise du fournisseur K ne propose pas de création de rapports natifs

Gestion à distance

Avec iDRAC9, les administrateurs n'ont pas besoin de se rendre physiquement dans le datacenter pour chaque modification. iDRAC9 offre 51 fonctionnalités de gestion du BIOS à distance (contre une seule pour le BMC du fournisseur K) pour permettre aux administrateurs d'effectuer librement davantage de modifications à l'extérieur du datacenter. Les administrateurs bénéficient ainsi d'un contrôle beaucoup plus granulaire sur la configuration du BIOS, partout où ils se trouvent (voir Figure 4).

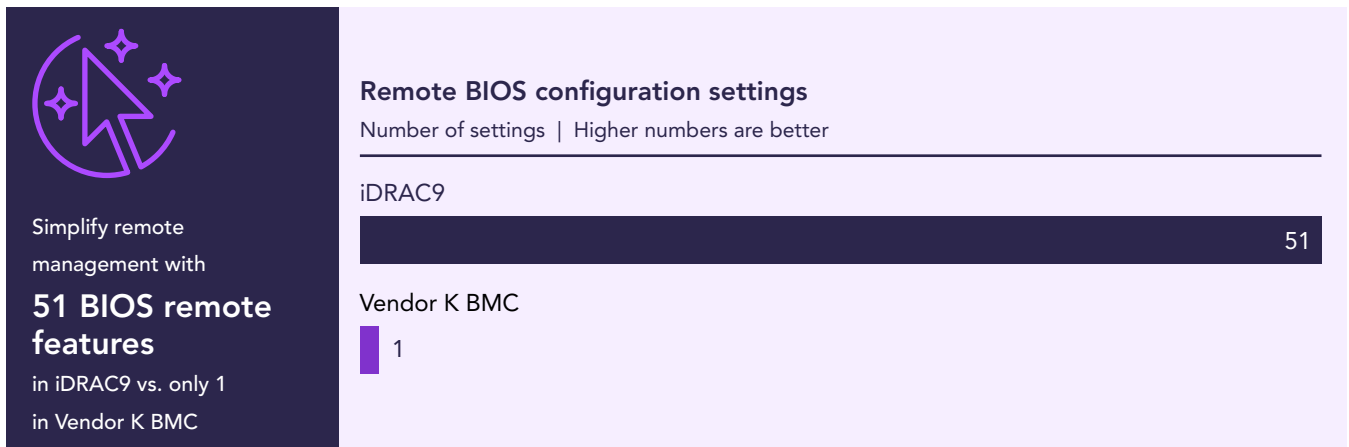


Figure 4 : Comparaison des fonctionnalités distantes du BIOS offertes par chaque outil de gestion. Un plus grand nombre de fonctionnalités offre plus d'efficacité. Source : Principled Technologies.

Effectuer des modifications de configuration

Avec iDRAC9, les administrateurs peuvent modifier les paramètres de configuration du BIOS et organiser la mise à jour en vue d'un redémarrage ultérieur sans la présence d'un administrateur supplémentaire. À l'inverse, le BMC du fournisseur K impose de passer par des utilitaires système pour introduire des modifications et nécessite une intervention manuelle de l'administrateur pendant la modification. Comme le montre la Figure 5, la préparation de la modification de la configuration du BIOS pour un redémarrage planifié a pris 87 % de temps en moins et deux fois moins d'étapes avec iDRAC9 qu'avec le BMC du fournisseur K. En extrapolant ces économies à des déploiements de grande envergure, les gains de temps d'administration augmentent. Par exemple, dans un déploiement de 100 serveurs, les administrateurs peuvent gagner plus de 6 heures en modifiant les éléments de configuration du BIOS.

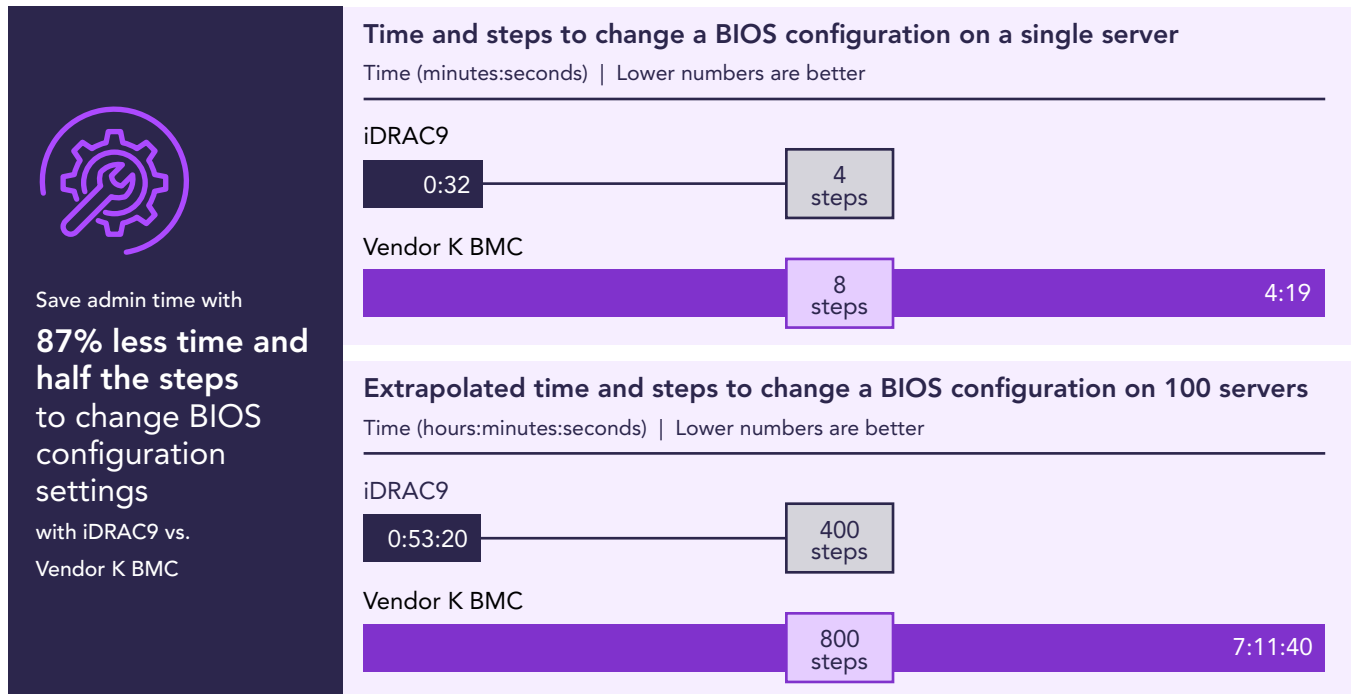


Figure 5 : Temps nécessaire pour modifier les paramètres de configuration du BIOS et organiser la mise à jour en vue d'un redémarrage ultérieur pour un seul serveur, avec extrapolation de la durée nécessaire pour 100 serveurs. Moins de temps et moins d'étapes pour plus d'efficacité. Source : Principled Technologies.

Configuration d'actions basées sur des alertes

Les administrateurs peuvent mettre mieux à profit le temps dont ils disposent lorsqu'ils ne se trouvent pas pieds et poings liés à un bureau pour surveiller l'intégrité de l'environnement. Comme le montre la Figure 6, OME fournit 12 options d'actions basées sur des alertes, qui sont pilotées par des règles, afin que la mitigation des problèmes commence automatiquement dès que l'environnement atteint certains seuils. En revanche, la console de gestion d'entreprise du fournisseur K permet aux administrateurs de configurer uniquement quatre événements basés sur des alertes.

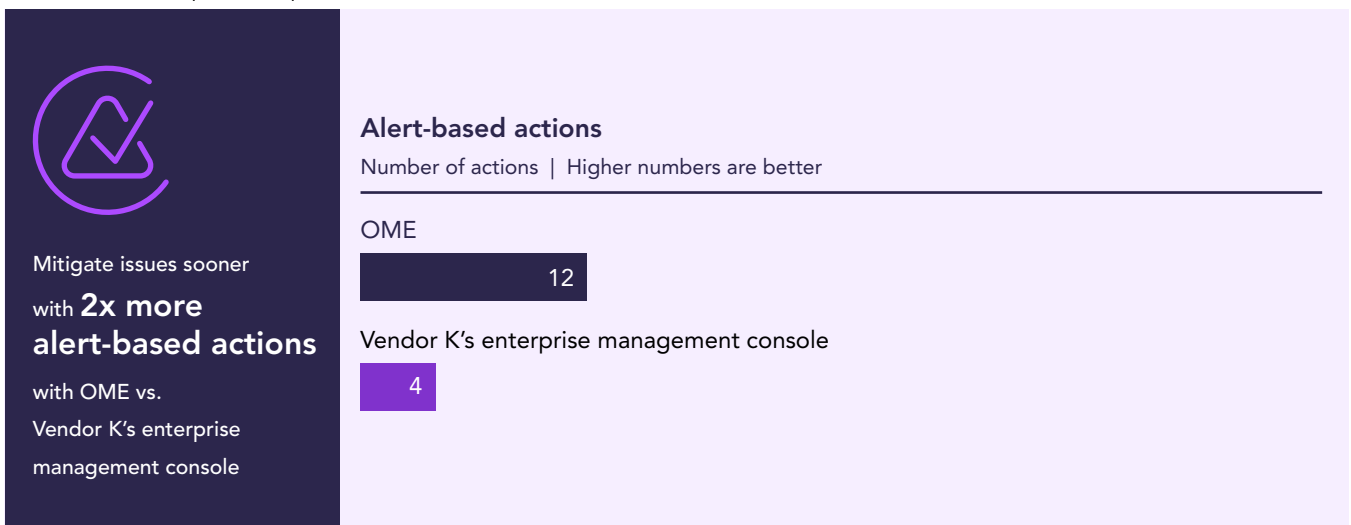


Figure 6 : Comparaison de l'action basée sur les alertes proposée par chaque outil de gestion. Plus d'actions signifient plus d'efficacité. Source : Principled Technologies.

À propos de Dell Technologies OpenManage Enterprise

OME est une console de gestion de systèmes « un-à-plusieurs » conçue pour le datacenter. La console offre une interface utilisateur graphique HTML5 moderne et se déploie en tant qu'appliance virtuelle pour les environnements VMware ESXi™, Microsoft Hyper-V et de machine virtuelle basée sur le noyau (KVM). OME est capable de détecter et d'inventorier jusqu'à 8 000 appareils sur les réseaux IPv4 et IPv6, notamment les serveurs rack Dell, les serveurs tour Dell, ainsi que les serveurs lames et boîtiers Dell.⁶ Dans une récente étude PT, nous avons constaté qu'un environnement Dell avec OME et OpenManage Enterprise Modular (OME-M) peut faire gagner du temps lors de la modification des VLAN et éviter les interventions lors des mises à jour planifiées du firmware.⁷

Pour en savoir plus sur OME, accédez à <https://www.dell.com/en-us/lp/dt/open-manage-enterprise>.




Gestion basée sur le Cloud avec APEX AIOps Infrastructure Observability (anciennement CloudIQ)

Les outils intégrés et les consoles de gestion d'entreprise ne sont pas les seuls outils de la gamme de gestion de serveurs Dell. Avec APEX AIOps Infrastructure Observability (anciennement CloudIQ), les administrateurs disposent d'un autre moyen simple d'utilisation et automatisé de contrôler l'intégrité et la sécurité de leur infrastructure, cette fois-ci à partir du Cloud.

Fonctionnalités de sécurité supplémentaires disponibles dans APEX AIOps Infrastructure Observability (anciennement CloudIQ)

Apex AIOps Infrastructure Observability (anciennement CloudIQ) offre plusieurs fonctionnalités de sécurité qui peuvent renforcer votre organisation contre les attaques. Le Tableau 5 met en évidence certaines de ces fonctionnalités de sécurité clés.

Tableau 5 : Présentation des principales fonctionnalités de sécurité disponibles dans APEX AIOps Infrastructure Observability (anciennement CloudIQ). Source : Principled Technologies.

Fonctionnalité	Comment fonctionne APEX AIOps Infrastructure Observability (anciennement CloudIQ) pour sécuriser votre environnement ?
 Alertes de niveaux de risque de cybersécurité	Fournit des informations de cybersécurité automatisées avec des alertes sur des niveaux de risque de sécurité spécifiques afin que les administrateurs puissent réagir et résoudre les problèmes plus rapidement pour sécuriser les données
 Configuration de la sécurité basée sur des règles	Propose des paramètres de configuration de la sécurité basés sur des règles et des modèles faciles à appliquer qui permettent à l'administrateur de s'assurer que les paramètres des pratiques d'excellence en matière de sécurité sont appliqués, protégeant ainsi l'environnement PowerEdge
 Conseils en cybersécurité	Fournit des rapports de conseils de sécurité pertinents , offrant des détails spécifiques sur les failles de sécurité et des suggestions de mesures correctives, ce qui permet d'agir rapidement pour combler les failles de sécurité

À propos d'APEX AIOps Infrastructure Observability (anciennement CloudIQ)







Apex AIOps Infrastructure Observability (anciennement CloudIQ) est un outil AIOps basé sur le Cloud offrant une surveillance proactive, un apprentissage automatique et une analytique prédictive pour un grand nombre de produits et services Dell, y compris les serveurs, le stockage, les appliances de protection des données et l'infrastructure hyperconvergée.⁸ Une étude réalisée en 2022 par Principled technologies a montré que CloudIQ avait un impact négligeable sur la bande passante réseau, tout en permettant de surveiller la télémétrie, l'état d'intégrité, les alertes et l'inventaire à partir d'une seule et même console.⁹

Pour en savoir plus sur APEX AIOps Infrastructure Observability (anciennement CloudIQ), accédez à <https://www.dell.com/en-us/dt/apex/aiops.htm>.

Fonctionnalités supplémentaires de développement durable et d'efficacité disponibles dans APEX AIOps Infrastructure Observability (anciennement CloudIQ)

APEX AIOps Infrastructure Observability (anciennement CloudIQ) offre également des fonctionnalités qui favorisent le développement durable et l'efficacité, et qui s'intègrent à iDRAC9 et OME pour permettre aux administrateurs de surveiller plus facilement l'intégrité de leur environnement PowerEdge. Le Tableau 6 met en évidence certaines de ces fonctionnalités.

Tableau 6 : Aperçu des fonctionnalités de gestion faciles d'utilisation relatives au développement durable disponibles dans APEX AIOps Infrastructure Observability (anciennement CloudIQ). Source : Principled Technologies.

Fonctionnalité	Avantages clés avec APEX AIOps Infrastructure Observability (anciennement CloudIQ)
 Analyse de l'empreinte carbone	Situé dans la section Monitoring, cet outil offre une vue plus précise des émissions de carbone et peut les prévoir dans tous les environnements
 Vues des performances	Offre des vues de performances et des graphiques d'anomalies et d'utilisation pour alerter les administrateurs dès les premiers signes de problèmes.
 Rapports de conformité personnalisés	Offre aux utilisateurs la possibilité de créer des rapports de conformité personnalisés pour les appareils sélectionnés
 Rapports d'inventaire et de performances personnalisables	Fournit des options de création de rapports personnalisés pour les données de performances et d'inventaire des serveurs, ce qui permet aux administrateurs de mieux contrôler les mesures relatives aux performances et aux appareils qu'ils souhaitent suivre
 Planification des mesures relatives à l'alimentation	Effectuez des actions d'alimentation telles que le plafonnement de l'alimentation sur plusieurs serveurs Dell PowerEdge surveillés en seulement 35 secondes et 6 étapes
 Planification des mises à jour de firmware	Planifiez les mises à jour de firmware PowerEdge pour plusieurs serveurs surveillés en seulement 41 secondes et 9 étapes

Conclusion

En comparant les fonctionnalités relatives à la sécurité, au développement durable et à la gestion/surveillance, nous avons constaté que la gamme d'outils de gestion des serveurs Dell offrait des fonctionnalités de gestion et de surveillance plus robustes que la gamme du fournisseur K. Dans le domaine de la sécurité, iDRAC9 offrait davantage de fonctionnalités, notamment le verrouillage dynamique du système et l'authentification multifacteur, que le fournisseur K ne proposait pas du tout. De plus, iDRAC9 a considérablement réduit le temps de désactivation des ports USB afin de réduire la vulnérabilité des données.

Grâce à une analyse de l'empreinte carbone et à de solides outils de gestion de l'alimentation, OME peut aider les organisations à atteindre leurs objectifs de développement durable mieux qu'en utilisant la console de gestion d'entreprise du fournisseur K. En outre, nous avons constaté que la gamme de solutions de gestion de serveurs Dell offrait davantage d'automatisation et d'options de gestion à distance, réduisant ainsi le temps et les efforts de l'administrateur pour certaines tâches de surveillance et de maintenance de routine. Ces atouts en matière de sécurité, de développement durable et de gestion/surveillance font de la gamme de gestion de serveurs Dell une option intéressante pour les organisations à la recherche d'un datacenter plus efficace et sécurisé.

1. Harvard Business Review, « The Devastating Business Impacts of a Cyber Breach », consulté le 10 avril 2024, <https://hbr.org/2023/05/the-devastating-business-impacts-of-a-cyber-breach>.
2. Dell, « Integrated Dell Remote Access Controller (iDRAC) », consulté le 17 mai 2024, <https://www.dell.com/en-us/lp/dt/open-manage-idrac>.
3. Remarque : La désactivation du port USB du fournisseur K est personnalisable, mais cela signifie que les administrateurs doivent sélectionner chaque port pour la désactivation, plutôt que de le faire par groupe.
4. DOE, « DOE Announces \$40 Million for More Efficient Cooling for Data Centers », consulté le 20 mai 2024, <https://www.energy.gov/articles/doe-announces-40-million-more-efficient-cooling-data-centers>.
5. Dell, « OpenManage Enterprise support Matrix », consulté le 21 mai 2024, <https://www.dell.com/support/kbdoc/en-us/article/lkbprint?ArticleNumber=000217909&AccessLevel=10&Lang=en>.
6. Dell, « OpenManage Enterprise », consulté le 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 easier for administrators », consulté le 17 mai 2024, <https://www.principledtechnologies.com/Dell/PowerEdge-MX-OME-OME-M-0124.pdf>.
8. Dell, « APEX AIOps: Tame IT Complexity in your digital business », consulté le 11 juin 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 », consulté le 9 avril 2024, <https://www.principledtechnologies.com/dell/CloudIQ-network-0422.pdf>.

Consultez les données scientifiques qui sous-tendent ce rapport

► Consultez la version originale en anglais de ce rapport



Facts matter.®

Ce projet a été réalisé à la demande de Dell Technologies.

Principled Technologies est une marque déposée de Principled Technologies, Inc. Tous les autres noms de produit sont des marques déposées par leurs propriétaires respectifs. Pour plus d'informations, consultez les données scientifiques qui sous-tendent ce rapport.