



Reduza a vulnerabilidade de dados, gastando **85% menos tempo para desativar as portas USB frontais**

no iDRAC9 em comparação com o BMC do Fornecedor K



Ajude a reduzir as emissões de carbono com **25 relatórios personalizáveis de consumo de energia**

no OME, enquanto o console de gerenciamento empresarial do Fornecedor K tem 0 relatórios



Agende atualizações **automáticas de firmware em apenas 41 segundos**

no APEX AIOps Infrastructure Observability (anteriormente, CloudIQ)

As ferramentas de gerenciamento de servidores da Dell podem ajudar a melhorar a segurança, a sustentabilidade e a eficiência do gerenciamento

em comparação com as ferramentas de gerenciamento de servidores do Fornecedor K

À medida que os data centers continuam crescendo, o mesmo acontece com as tarefas dos administradores. Uma infraestrutura que oferece sólidas ferramentas nativas de gerenciamento e monitoramento com automação pode tornar a proteção e o gerenciamento do data center uma tarefa mais fácil para os administradores muitas vezes sobrecarregados. Nós comparamos os recursos e as capacidades dos portfólios de gerenciamento da Dell e de um concorrente, ao qual nos referiremos como Fornecedor K:

Tabela 1: As ferramentas de gerenciamento que testamos.

	Dell	Fornecedor K
Gerenciamento remoto/integrado de servidores	Dell Technologies Integrated Dell Remote Access Controller 9 (iDRAC9)	Baseboard Management Controller (BMC) do Fornecedor K
Gerenciamento de consoles e dispositivos de um para muitos	Dell Technologies OpenManage™ Enterprise (OME) APEX AIOps Infrastructure Observability (anteriormente, CloudIQ)	Console de gerenciamento empresarial do Fornecedor K

Nós constatamos que o iDRAC9, o OME e o APEX AIOps Infrastructure Observability (anteriormente, CloudIQ) oferecem uma sólida família de ferramentas de gerenciamento que podem aumentar a segurança, auxiliar em medidas de sustentabilidade e facilitar as tarefas administrativas diárias, em comparação com o uso de ferramentas semelhantes do Fornecedor K.

Fortalecendo a segurança do data center

Para organizações que armazenam dados confidenciais de clientes, a ameaça persistente de ataques cibernéticos exige recursos de segurança ponta a ponta para garantir que os dados não acabem nas mãos erradas. De fato, até "83% das organizações sofreram mais de uma violação de dados em 2022",¹ uma estatística que acentua a importância de tomar precauções acerca dos dados de clientes para aumentar a confiança dos consumidores.

Para proteger sua organização e seus dados contra os caros ataques cibernéticos, as ferramentas de gerenciamento da Dell oferecem sólidos recursos de segurança, tanto integrados ao servidor por meio do iDRAC9 quanto em um software abrangente de gerenciamento de nuvem e console. Abaixo, nós exploramos alguns dos principais recursos de segurança que as ferramentas da Dell usam para proteger seu sistema e os comparamos com as ofertas correspondentes do Fornecedor K.

Segurança integrada

Há recursos de segurança integrados a todos os servidores Dell PowerEdge por meio do iDRAC9 que funcionam para impedir que agentes mal-intencionados obtenham acesso aos dados. Três desses recursos importantes são:

- **Bloqueio dinâmico do sistema:** o bloqueio do sistema impede que atividades não intencionais ou mal-intencionadas alterem as configurações do firmware, do iDRAC e do BIOS do sistema. O termo "dinâmico" se refere à capacidade de configurar esses recursos uma vez e, em seguida, implementá-los conforme necessário. (Nota: esse recurso está disponível com licenças iDRAC9 Enterprise e Datacenter.)
- **Autenticação baseada em vários fatores (MFA):** a MFA solicita aos administradores uma senha, além de suas credenciais de log-in, para reforçar a segurança.
- **Ativação/desativação dinâmica de portas USB:** desativar e ativar as portas USB permite que os administradores controlem o acesso ao servidor por meio de uma porta USB. O termo "dinâmico" se refere à capacidade de ativar e desativar essas portas USB sem reinicializar o servidor nem o SO. Até que o administrador conceda acesso, ninguém poderá conectar um pen drive nem um teclado para modificar qualquer configuração do sistema, do SO ou do BIOS.

Como mostra a Tabela 2, o Fornecedor K não oferece bloqueio dinâmico do sistema nem MFA, e seus recursos dinâmicos de USB exigem tempo de inatividade do sistema (que pode ser muito caro para as organizações), o que os torna menos úteis e mais dispendiosos do que a solução da Dell.

Tabela 2: Comparação dos recursos integrados de segurança que as ferramentas de gerenciamento de servidores oferecem. Fonte: Principled Technologies.

	iDRAC9	BMC do fornecedor K
Bloqueio dinâmico do sistema	✓	✗
MFA	✓	✗
USB dinâmico	✓	✓*

*Requer tempo de inatividade do sistema

Sobre o Dell Technologies Integrated Dell Remote Access Controller 9

Os servidores Dell PowerEdge™ incluem o iDRAC9 com Dell Lifecycle Controller para oferecer funções de administração de sistemas que incluem alertas do sistema e recursos de gerenciamento remoto. De acordo com a Dell, os principais benefícios do iDRAC9 são:

- Automação escalável. APIs com base em padrões, como Redfish, e sólidas ferramentas de script, como RedHat Ansible, Python, PowerShell e Terraform, permitem gerenciar milhares de servidores.
- Suporte integrado, apresentando uma exibição da integridade do servidor e monitorando o status de milhares de parâmetros
- Sólidos recursos e opções de segurança²

Para saber mais sobre os recursos que o iDRAC9 oferece, acesse <https://www.dell.com/pt-br/lp/dt/open-manage-idrac>.

A Figura 1 mostra os resultados de nossa comparação prática, em que usamos o iDRAC9 e o BMC do Fornecedor K para desativar as portas USB dinamicamente.

Usando o iDRAC9, nós constatamos que os administradores podem desativar as portas USB frontais de um só servidor em apenas 41 segundos e 4 etapas. Em comparação, o mesmo processo com o BMC do Fornecedor K leva 4 minutos e 43 segundos e exige 8 etapas por servidor. Isso significa que, por servidor, **a solução da Dell leva 85% menos tempo e requer metade das etapas para desativar as portas USB frontais.**³ Quando consideramos concluir essas etapas em um data center, a economia de tempo faz ainda mais sentido; em uma implementação de 100 servidores, os administradores podem economizar 6 horas e 43 minutos com o iDRAC9, em comparação com o BMC do Fornecedor K.

Além de serem mais fáceis e rápidos de acessar com o iDRAC9 do que com o BMC do Fornecedor K, esses recursos também permitem que os administradores mantenham os servidores em produção (sem tempo de inatividade) enquanto os ativam ou desativam. O método do Fornecedor K requer tempo de inatividade, o que pode incorrer em custos significativos, e alterações na configuração do sistema a cada desativação de porta.

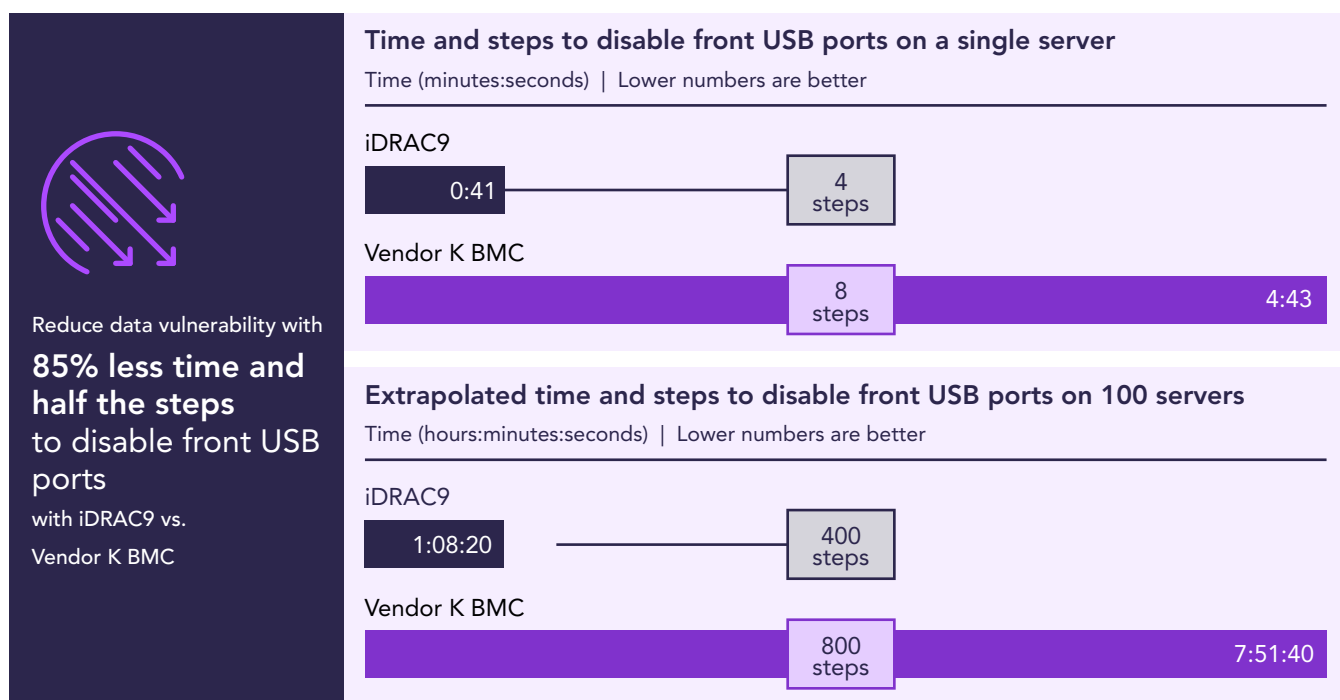


Figura 1: Tempo para desativar as portas USB frontais de um só servidor e tempo extrapolado para desativar as portas USB frontais de 100 servidores. É melhor gastar menos tempo e seguir menos etapas. Fonte: Principled Technologies.

Mantendo a segurança com o gerenciamento mais fácil de credenciais no OME







O OME oferece aos administradores uma maneira mais simples de gerenciar a rotação de senhas do iDRAC9. Em vez de exigir uma conta de administrador estática e conhecida, o OME gerencia os iDRACs por meio de uma conta de serviço em que os clientes selecionam a política necessária de rotação de senhas (pela qual a senha nunca é divulgada), ou os administradores podem gerenciá-los externamente com um terceiro. **O console de gerenciamento empresarial do Fornecedor K não tem recursos internos de rotação de senhas, o que força os administradores a recorrer a um terceiro caso queiram esse recurso.** Nós confirmamos que os servidores gerenciados pelo iDRAC9 se integram à conta do OME com privilégios totais de administrador para facilitar o gerenciamento de credenciais.

Nota: os gráficos deste relatório usam escalas diferentes. Atente-se ao intervalo de dados de cada gráfico à medida que os compara.

Atingindo metas de sustentabilidade

De acordo com o Departamento de Energia dos EUA, "os data centers são responsáveis por aproximadamente 2% do consumo total de eletricidade nos EUA, enquanto o resfriamento do data center pode representar até 40% do consumo total de energia do data center".⁴ À medida que os dados continuam se proliferando, esses números só aumentarão, o que torna o gerenciamento térmico e de energia vitais para manter baixos os custos do data center e atingir as metas de sustentabilidade para ajudar a reduzir as emissões de carbono. Para ajudar as organizações a reduzir o consumo de energia, o OME incorpora vários recursos para monitoramento e gerenciamento do consumo de energia. A Tabela 3 destaca os principais benefícios desses recursos, que nós descrevemos em mais detalhes abaixo.

Tabela 3: Visão geral dos principais recursos de sustentabilidade disponíveis no OME e no console de gerenciamento empresarial do Fornecedor K.
Fonte: Principled Technologies.

Recurso	Principais benefícios das ferramentas de gerenciamento da Dell	Desvantagem das ferramentas de gerenciamento do Fornecedor K
 Ferramenta de planejamento de capacidade e calculadora de emissões de carbono	Capacidade de estimar as emissões de gases do efeito estufa com valores personalizáveis para ajudar a atingir metas de sustentabilidade	O console de gerenciamento empresarial do Fornecedor K não oferece recursos comparáveis
 Políticas de limite de consumo de energia	O plug-in OME Power Manager pode gerenciar limites de energia de dispositivos ou grupos de dispositivos que, quando ativados, impõem limites ao consumo de energia	O console de gerenciamento empresarial do Fornecedor K não oferece recursos comparáveis
 Gerenciamento automatizado de temperatura e energia	Opções de políticas acionadas por energia e temperatura , com a opção de acionamento quando o servidor ultrapassar um limite de consumo de energia ou de temperatura	O console de gerenciamento empresarial do Fornecedor K não oferece recursos comparáveis
 Painel de indicadores de consumo de energia	O painel de indicadores do plug-in OME Power Manager oferece acesso rápido aos dados do Power Manager, entregando 2,75x mais métricas, com um total de 11 métricas	O console de gerenciamento empresarial do Fornecedor K oferece apenas quatro métricas no painel de indicadores
 Relatórios de consumo de energia	O plug-in OME Power Manager disponibiliza 25 relatórios padrão e personalizáveis diferentes	O console de gerenciamento empresarial do Fornecedor K não disponibiliza relatórios de gerenciamento de energia
 Métricas de gerenciamento de energia	Até o triplo de métricas , apresentando informações mais específicas sobre o gerenciamento do consumo de energia, com um total de 21 métricas	O console de gerenciamento empresarial do Fornecedor K oferece apenas sete métricas relacionadas ao gerenciamento de energia

Gerenciamento automatizado de temperatura e energia

O OME Power Manager oferece gerenciamento automatizado de temperatura e energia por meio de opções de políticas estáticas e acionadas por energia e temperatura. Essas políticas permitem que os administradores definam limites para o consumo de energia ou limites de temperatura para ajudar a reduzir os custos de resfriamento, oferecer suporte às estratégias de energia e responder aos eventos térmicos. Por outro lado, **o Fornecedor K não oferece recursos automatizados de gerenciamento térmico e de energia**. Sem a capacidade de definir limites com base em temperatura, o uso de energia pode exceder as expectativas e dificultar o planejamento com a sustentabilidade em mente. Otimizar o consumo de energia é uma estratégia importante para atingir metas de sustentabilidade. O plug-in OME Power Manager disponibiliza **25 relatórios padrão e/ou personalizáveis relacionados ao Power Manager** (17 em dispositivos Power Manager e mais 8 em grupos do Power Manager). Eles permitem que os administradores otimizem o planejamento de capacidade e gerenciem a energia para maximizar a eficiência. **O console de gerenciamento empresarial do Fornecedor K não disponibiliza relatórios semelhantes de gerenciamento de energia** (consulte a Figura 2).

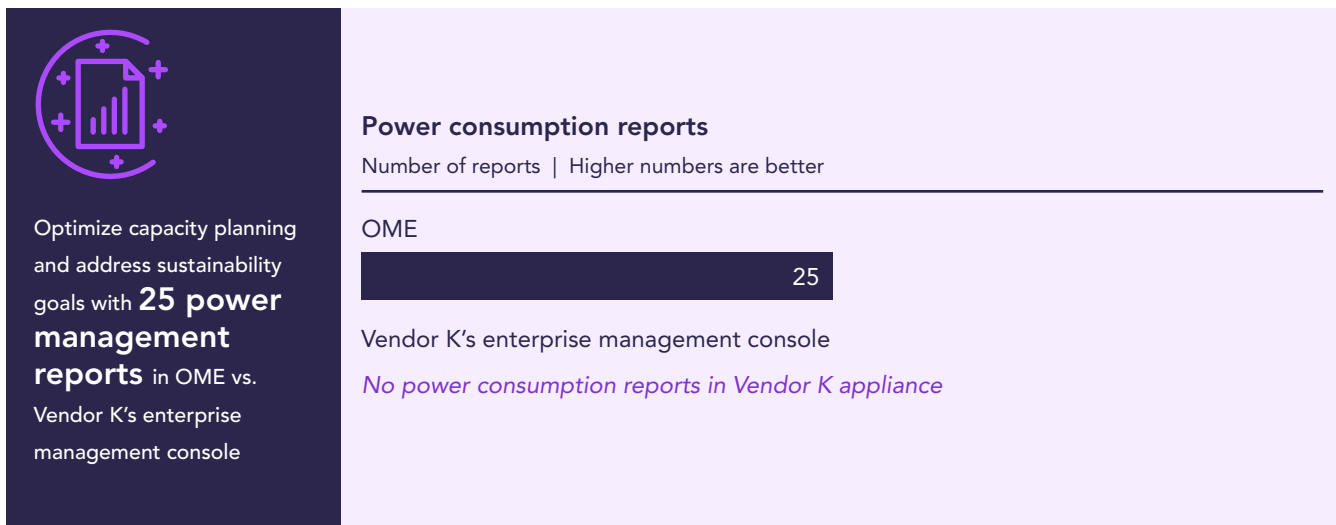


Figura 2: Comparação do número de relatórios de gerenciamento de energia disponíveis no OME e no console de gerenciamento empresarial do Fornecedor K. Quanto mais relatórios, melhor. Fonte: Principled Technologies

Para otimizar ainda mais o gerenciamento de energia, o plug-in OME Power Manager permite que os administradores visualizem até **3x mais métricas do que o console de gerenciamento empresarial do Fornecedor K** (consulte a Figura 3). O OME oferece 21 métricas diferentes, inclusive o uso de energia por componentes individuais, o fluxo de ar e a utilização de componentes, enquanto o console de gerenciamento empresarial do Fornecedor K oferece apenas 7 métricas diferentes.

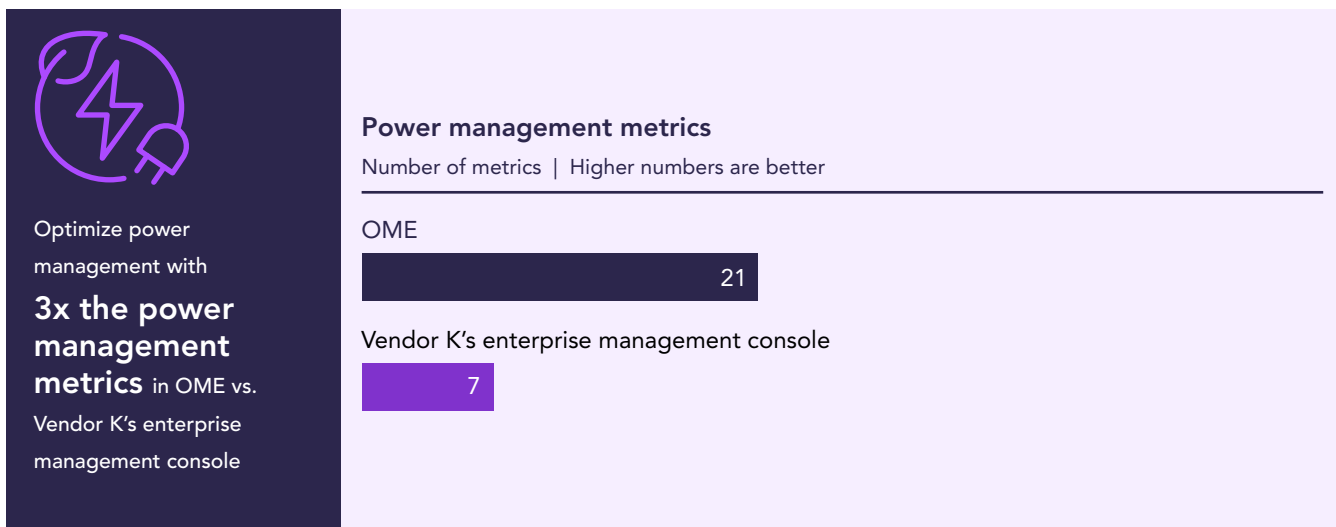


Figura 3: Comparação do número de métricas de gerenciamento de energia disponíveis no OME e no console de gerenciamento empresarial do Fornecedor K. Quanto mais métricas, melhor. Fonte: Principled Technologies.







Análise das emissões e da pegada de carbono





Um dos principais recursos de sustentabilidade que o **OME inclui é uma ferramenta de planejamento de capacidade e calculadora de emissões de carbono**. Essa ferramenta ajuda as organizações a estimar as emissões de gases do efeito estufa, informando valores padrão dos custos de energia e das emissões de carbono por unidade de energia consumida. Esse recurso também permite personalização, dando às organizações a capacidade de especificar os valores dos custos de energia e das emissões de carbono de sua própria região e, assim, gerar dados específicos ao modelo de consumo de seu data center. **O console de gerenciamento empresarial do Fornecedor K não tem um recurso comparável**, o que pode prejudicar a capacidade de uma organização de planejar com a sustentabilidade em mente.

Aliviando a carga de gerenciamento com sólidos recursos de monitoramento e gerenciamento

À medida que a infraestrutura vai aumentando, o mesmo acontece com as responsabilidades dos administradores de data center. Ao escolher ferramentas de gerenciamento de servidores que automatizam determinadas tarefas e aprimoram o gerenciamento diário, as organizações podem ajudar os administradores a se tornar mais eficientes e dar a eles mais tempo para se planejar para o futuro. Nós constatamos que o portfólio de gerenciamento de servidores da Dell viabilizou vários recursos que podem simplificar as tarefas dos administradores. A Tabela 4 apresenta um resumo comparativo entre os principais recursos fáceis de usar disponíveis no portfólio de gerenciamento da Dell e as ferramentas de gerenciamento do Fornecedor K.

Tabela 4: Visão geral dos principais recursos fáceis de usar disponíveis nas ferramentas de gerenciamento da Dell e as ferramentas de gerenciamento do Fornecedor K. Fonte: Principled Technologies.

Recurso	Principais benefícios das ferramentas de gerenciamento da Dell	Desvantagem das ferramentas de gerenciamento do Fornecedor K
 Mais recursos remotos de BIOS	Gerenciamento remoto mais fácil com 51 recursos remotos de BIOS no iDRAC9	O BMC do Fornecedor K oferece apenas um recurso remoto de BIOS
 Alterações mais fáceis na configuração do BIOS	87% menos tempo e metade das etapas para fazer uma alteração na configuração do BIOS	O Fornecedor K exige intervenção manual do administrador para fazer alterações a partir dos utilitários do sistema
 Importação/exportação da configuração completa do servidor	Configuração mais rápida de vários servidores idênticos com a capacidade de exportar/importar definições para um servidor totalmente configurado	O Fornecedor K oferece apenas backup e restauração do BMC para cada servidor individual
 Atualizações automatizadas agendadas	O iDRAC9 dá aos administradores a capacidade de agendar atualizações automatizadas de um repositório durante uma janela de manutenção, sem intervenção adicional do administrador	O BMC do Fornecedor K não oferece atualizações automatizadas agendadas
 Visão geral abrangente do status do armazenamento	O iDRAC9 oferece uma representação visual do status do armazenamento, para identificar rapidamente unidades com status de alerta	O BMC do Fornecedor K não apresenta uma exibição semelhante
 Streaming de telemetria	O iDRAC9 oferece telemetria para 2x mais categorias de métricas, com um total de 8 categorias	O BMC do Fornecedor K oferece telemetria para apenas quatro categorias
 Connection View	O Connection View do iDRAC9 apresenta detalhes do mapeamento físico das portas de switch às conexões dedicadas de porta do iDRAC e às portas de rede do servidor	O BMC do Fornecedor K não tem informações de conexão física para switches upstream
 Dimensionamento	O OME pode gerenciar até oito mil dispositivos ⁵	O Fornecedor K pode gerenciar apenas até 1.000 dispositivos

Recurso	Principais benefícios das ferramentas de gerenciamento da Dell	Desvantagem das ferramentas de gerenciamento do Fornecedor K
 Ações com base em alertas	O OME oferece 2x mais ações com base em alertas (oferecendo 12 ações) que desencadeiam ações com base na entrada de um alerta	O Fornecedor K oferece apenas quatro ações com base em alertas
 Arquitetura de plug-ins	O OME oferece a capacidade de expandir a funcionalidade com plug-ins , que os administradores podem adicionar ao console sem a necessidade de aplicativos adicionais para gerenciar	O console de gerenciamento empresarial do Fornecedor K não oferece uma arquitetura com base em plug-ins para proporcionar capacidade de expansão
 Monitoramento de dispositivos de terceiros	O OME oferece suporte ao monitoramento de dispositivos e servidores de terceiros	O console de gerenciamento empresarial do Fornecedor K não oferece suporte ao monitoramento de dispositivos e servidores de terceiros
 Relatórios	O OME disponibiliza aos administradores 42 relatórios integrados com personalização, para que eles possam selecionar especificamente os dados mais importantes para seus propósitos	O console de gerenciamento empresarial do Fornecedor K não tem criação nativa de relatórios

Gerenciamento remoto

Com o iDRAC9, os administradores não precisam entrar no data center a cada alteração. O iDRAC9 oferece 51 recursos remotos de BIOS para dar aos administradores a liberdade de fazer mais alterações de fora do data center. Em comparação, o BMC do Fornecedor K oferece apenas um recurso desse tipo. Sendo assim, o iDRAC9 oferece aos administradores um controle significativamente mais específico sobre a configuração do BIOS de qualquer lugar (consulte a Figura 4).

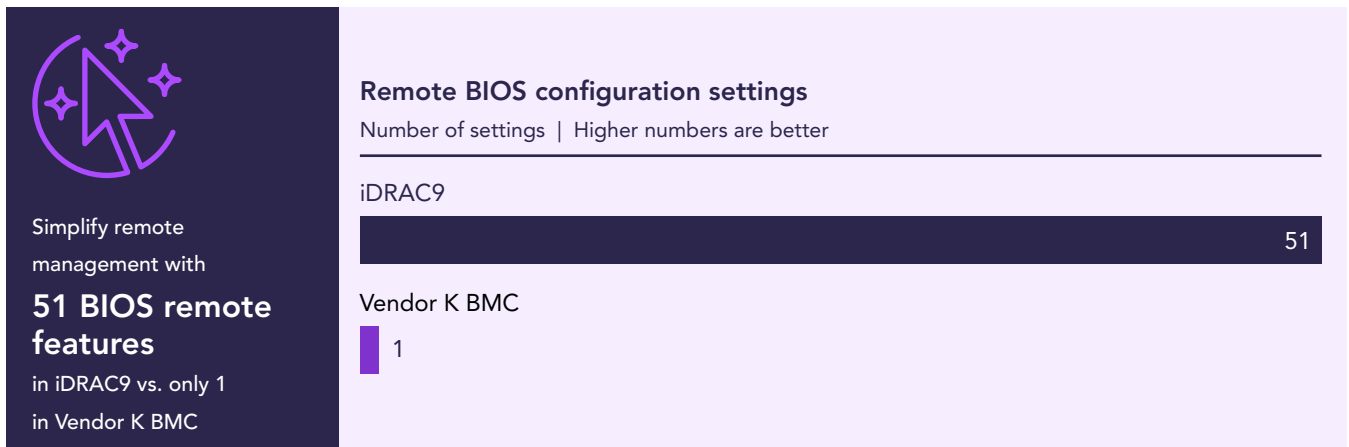


Figura 4: Comparação dos recursos remotos de BIOS que cada ferramenta de gerenciamento oferece. Quanto mais recursos, melhor. Fonte: Principled Technologies.

Fazendo alterações de configuração

Com o iDRAC9, os administradores podem alterar as configurações do BIOS e preparar a atualização para uma reinicialização posterior sem a necessidade de presença adicional do administrador. Já o BMC do Fornecedor K requer alterações a partir dos utilitários do sistema e intervenção manual do administrador durante a alteração. Como mostra a Figura 5, a preparação da alteração de configurações do BIOS para uma reinicialização agendada levou 87% menos tempo e exigiu metade das etapas com o iDRAC9 do que com o BMC do Fornecedor K. Quando extrapolamos essas economias para grandes implementações, a economia de tempo dos administradores aumenta ainda mais. Por exemplo, em uma implementação de 100 servidores, os administradores podem economizar mais de 6 horas para alterar itens de configuração do BIOS.

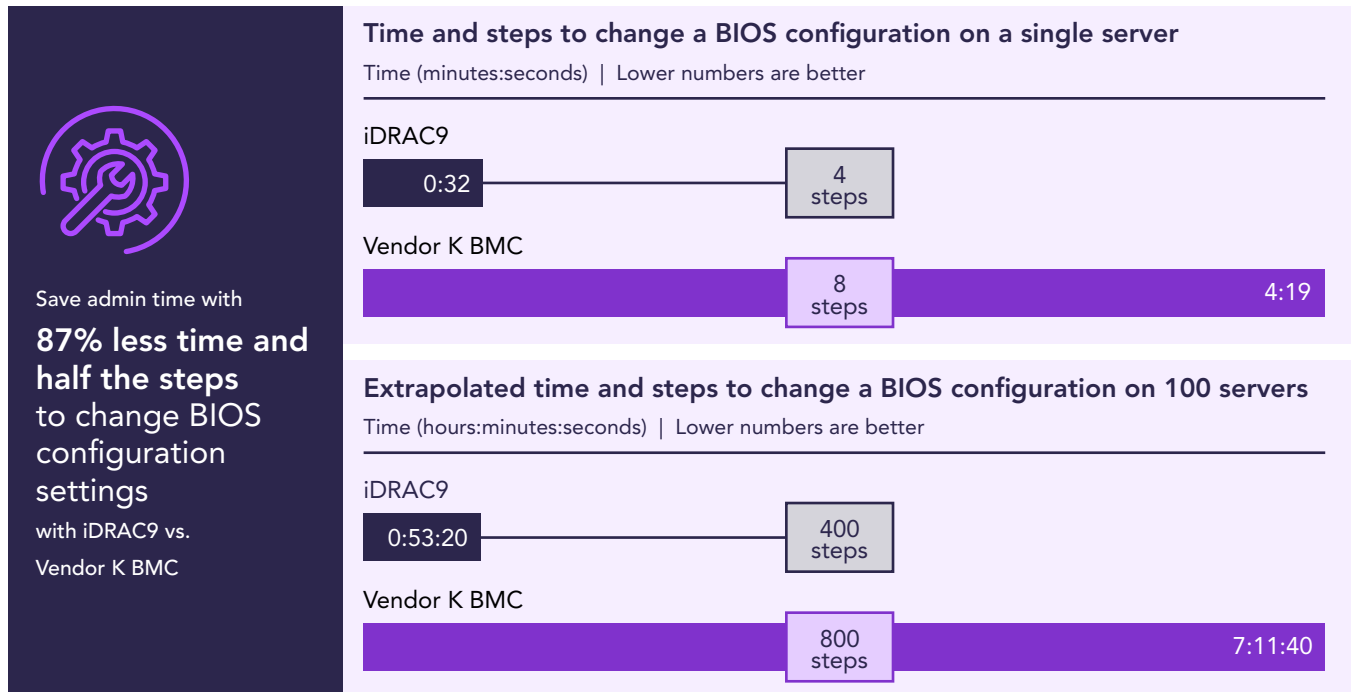


Figura 5: Tempo para alterar as configurações do BIOS e preparar a atualização para uma reinicialização posterior de um só servidor e tempo extrapolado para 100 servidores. É melhor gastar menos tempo e seguir menos etapas. Fonte: Principled Technologies.

Configurando ações com base em alertas

Os administradores podem usar melhor o seu tempo quando não estão presos a uma mesa, monitorando a integridade do ambiente. Como mostra a Figura 6, o OME oferece 12 opções orientadas por políticas para ações com base em alertas. Assim, a redução de problemas inicia automaticamente sempre que o ambiente atinge determinados limites. Por outro lado, o console de gerenciamento empresarial do Fornecedor K permite que os administradores configurem apenas quatro eventos com base em alertas.

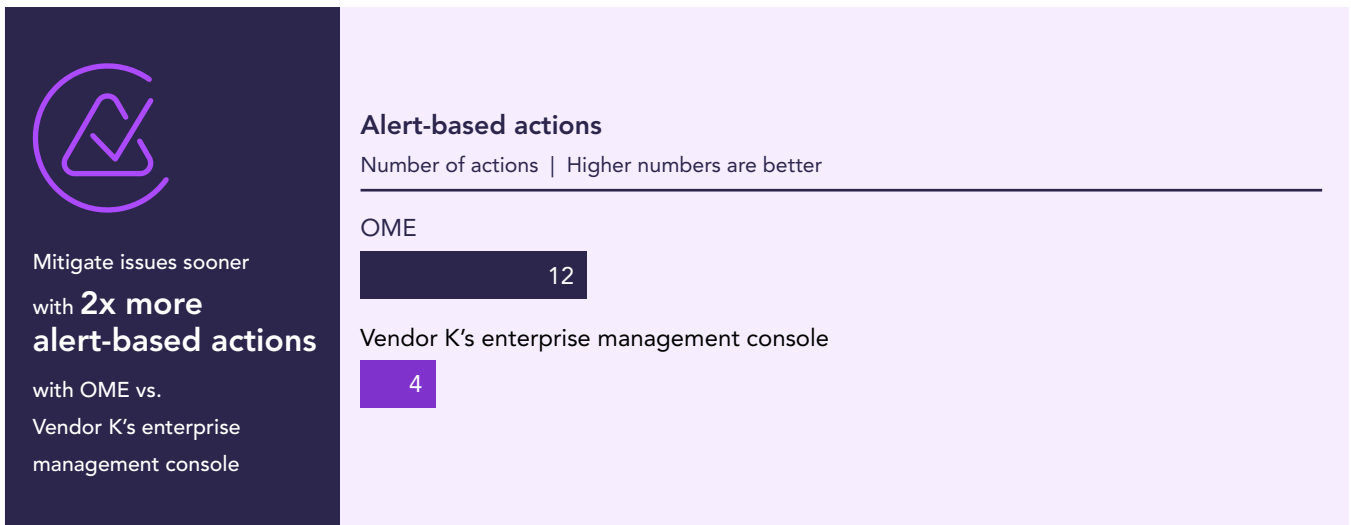


Figura 6: Comparação das ações com base em alertas que cada ferramenta de gerenciamento oferece. Quanto mais ações, melhor. Fonte: Principled Technologies.

Sobre o Dell Technologies OpenManage Enterprise

O OME é um console de gerenciamento de sistemas de um para muitos, voltado para o data center. O console oferece uma moderna interface gráfica do usuário HTML5 e é implementado como um Virtual Appliance para ambientes VMware ESXi™, Microsoft Hyper-V e de máquinas virtuais com base em Kernel (KVM). O OME pode detectar e inventariar até oito mil dispositivos em redes IPv4 e IPv6, inclusive servidores em rack Dell, servidores em torre Dell e blades e chassis Dell.⁶ Em um recente estudo da PT, nós constatamos que um ambiente Dell com OME e o OpenManage Enterprise Modular (OME-M) pode economizar tempo na realização de alterações nas VLANs e evitar intervenções durante atualizações agendadas de firmware.⁷

Saiba mais sobre o OME em <https://www.dell.com/pt-br/lp/dt/open-manage-enterprise>.




Gerenciamento em nuvem com o APEX AIOps Infrastructure Observability (anteriormente, CloudIQ)

As ferramentas integradas e os consoles de gerenciamento empresarial não são as únicas ferramentas no portfólio de gerenciamento de servidores da Dell. Com o APEX AIOps Infrastructure Observability (anteriormente, CloudIQ), os administradores obtêm outra maneira automatizada e fácil de usar para manter sob controle a integridade e a segurança da infraestrutura — desta vez, na nuvem.

Recursos adicionais de segurança disponíveis no APEX AIOps Infrastructure Observability (anteriormente, CloudIQ)

O APEX AIOps Infrastructure Observability (anteriormente, CloudIQ) oferece vários recursos de segurança que podem fortalecer ainda mais sua organização contra ataques. A Tabela 5 destaca alguns desses principais recursos de segurança.

Tabela 5: Visão geral dos principais recursos de segurança disponíveis no APEX AIOps Infrastructure Observability (anteriormente, CloudIQ). Fonte: Principled Technologies.

Recurso	Como o APEX AIOps Infrastructure Observability (anteriormente, CloudIQ) funciona para proteger seu ambiente
 Alertas em nível de risco de segurança cibernética	Apresenta informações automatizadas sobre segurança cibernética, com alertas específicos de nível de risco de segurança para que os administradores possam reagir mais rapidamente e resolver problemas com agilidade para manter os dados seguros
 Configuração de segurança com base em políticas	Oferece configurações de segurança com base em políticas e modelos fáceis de aplicar que permitem que os administradores garantam que as práticas recomendadas de configurações de segurança estejam em vigor, protegendo o ambiente PowerEdge
 Recomendações sobre segurança cibernética	Oferece relatórios relevantes de recomendações sobre segurança , apresentando detalhes específicos de vulnerabilidades e sugestões de correção, o que permite ações rápidas para eliminar as brechas de segurança

Sobre o APEX AIOps Infrastructure Observability (anteriormente, CloudIQ)







APEX AIOps Infrastructure Observability (anteriormente, CloudIQ) é uma ferramenta de AIOps em nuvem que oferece "monitoramento proativo, aprendizado de máquina e análise preditiva" a muitos produtos e serviços da Dell, inclusive servidores, armazenamento, equipamentos de proteção de dados e infraestrutura hiperconvergente.⁸ Em um estudo da Principled Technologies de 2022, nós constatamos que o CloudIQ causava um impacto insignificante sobre a largura de banda da rede e, ao mesmo tempo, nos permitia monitorar a telemetria, o status de integridade, os alertas e o inventário em um só console.⁹

Saiba mais sobre o APEX AIOps Infrastructure Observability (anteriormente, CloudIQ) em <https://www.dell.com/pt-br/dt/apex/aiops.htm#tab0=0>.

Recursos adicionais de sustentabilidade e eficiência disponíveis no APEX AIOps Infrastructure Observability (anteriormente, CloudIQ)

O APEX AIOps Infrastructure Observability (anteriormente, CloudIQ) também oferece recursos que reforçam a sustentabilidade e a eficiência e se integram ao iDRAC9 e ao OME para facilitar para os administradores o monitoramento da integridade do ambiente PowerEdge. A Tabela 6 destaca alguns desses recursos.

Tabela 6: Visão geral dos recursos fáceis de usar de sustentabilidade e gerenciamento disponíveis no APEX AIOps Infrastructure Observability (anteriormente, CloudIQ). Fonte: Principled Technologies.

Recurso	Principais benefícios do APEX AIOps Infrastructure Observability (anteriormente, CloudIQ)
 Análise da pegada de carbono	Localizada na seção "Monitoring", essa ferramenta apresenta uma visão mais abrangente e previsões das emissões de carbono em todos os ambientes
 Exibições de desempenho	Apresenta exibições de desempenho e gráficos de anomalias e utilização para alertar os administradores ao primeiro sinal de problemas
 Relatórios personalizados de conformidade	Oferece aos usuários a capacidade de criar relatórios personalizados de conformidade para dispositivos selecionados
 Relatórios personalizáveis de desempenho e inventário	Disponibiliza opções personalizadas de relatórios de dados de inventário e desempenho do servidor, proporcionando aos administradores mais controle sobre as métricas de desempenho e de dispositivos que eles têm interesse em rastrear
 Agendando trabalhos de ações de energia	Realize ações de energia, como definir limites de energia em vários servidores Dell PowerEdge monitorados, em apenas 35 segundos e 6 etapas
 Agendando atualizações de firmware	Agende atualizações de firmware do PowerEdge para vários servidores monitorados em apenas 41 segundos e 9 etapas

Conclusão

Em nossa comparação de recursos de segurança, sustentabilidade e gerenciamento/monitoramento, nós constatamos que o portfólio de ferramentas de gerenciamento de servidores da Dell oferece recursos mais sólidos de gerenciamento e monitoramento do que o portfólio do Fornecedor K. Em termos de segurança, o iDRAC9 oferece mais recursos, inclusive bloqueio dinâmico do sistema e autenticação baseada em vários fatores, que o Fornecedor K não disponibiliza. Além disso, o iDRAC9 reduz significativamente o tempo para desativar portas USB, diminuindo a vulnerabilidade de dados.

Com a análise da pegada de carbono e sólidas ferramentas de gerenciamento de energia, nós confirmamos que o OME pode ajudar melhor as organizações a planejar o cumprimento das metas de sustentabilidade do que o console de gerenciamento empresarial do Fornecedor K. Além disso, constatamos que o portfólio de gerenciamento de servidores da Dell oferece mais automação e mais opções de gerenciamento remoto, reduzindo o tempo e o esforço dos administradores em determinadas tarefas rotineiras de monitoramento e manutenção. Esses ganhos em recursos de segurança, sustentabilidade e gerenciamento/monitoramento tornam o portfólio de gerenciamento de servidores da Dell uma opção atrativa para as organizações que buscam um data center mais seguro e eficiente.

1. Harvard Business Review, "The Devastating Business Impacts of a Cyber Breach", acessado em 10 de abril de 2024, <https://hbr.org/2023/05/the-devastating-business-impacts-of-a-cyber-breach>.
2. Dell, "Integrated Dell Remote Access Controller (iDRAC)", acessado em 17 de maio de 2024, <https://www.dell.com/pt-br/lp/dt/open-manage-idrac>.
3. Nota: a desativação de portas USB do Fornecedor K é personalizável, embora isso signifique que os administradores precisam selecionar cada porta para desativação, e não um grupo delas.
4. DOE, "DOE Announces \$40 Million for More Efficient Cooling for Data Centers", acessado em 20 de maio de 2024, <https://www.energy.gov/articles/doe-announces-40-million-more-efficient-cooling-data-centers>.
5. Dell, "Matriz de suporte do OpenManage Enterprise", acessado em 21 de maio de 2024, <https://www.dell.com/support/kbdoc/pt-br/article/lkbprint?ArticleNumber=000217909&AccessLevel=10&Lang=pt>.
6. Dell, "OpenManage Enterprise", acessado em 17 de maio de 2024, <https://www.dell.com/pt-br/lp/dt/open-manage-enterprise?dgc=SM&cid=243908&lid=spr3470526067&linkId=92952834>.
7. Principled Technologies, "A Dell PowerEdge MX environment using OpenManage Enterprise and OpenManage Enterprise Modular can make life easier for administrators", acessado em 17 de maio de 2024, <https://www.principledtechnologies.com/Dell/PowerEdge-MX-OME-OME-M-0124.pdf>.
8. Dell, "APEX AIOps: controle a complexidade da TI em seus negócios digitais", acessado em 11 de junho de 2024, <https://www.dell.com/pt-br/dt/apex/aiops.htm#tab0=0>.
9. Principled Technologies, "Dell CloudIQ provides a single console for proactive monitoring and had negligible impact on network bandwidth in our tests", acessado em 9 de abril de 2024, <https://www.principledtechnologies.com/dell/CloudIQ-network-0422.pdf>.

Veja a ciência que respalda este relatório ►

► Consulte a versão original em inglês deste relatório



Facts matter.®

Este projeto foi encomendado por Dell Technologies.

Principled Technologies é uma marca registrada da Principled Technologies, Inc. Todos os outros nomes de produtos são marcas comerciais de seus respectivos proprietários. Para obter mais informações, consulte a ciência por trás desse relatório.