



Reduzca la complejidad de los datos con

**Un 85 % menos de tiempo para deshabilitar los puertos USB frontales**

en iDRAC9 frente al BMC del Proveedor K



Contribuya a mitigar las emisiones de carbono con

**25 informes de consumo de energía personalizables**

En OME frente a 0 informes en la consola de gestión empresarial del Proveedor K.



Programe automáticamente **actualizaciones de firmware en tan solo 41 segundos**

en APEX AIOps Infrastructure Observability (anteriormente CloudIQ)

## Las herramientas de gestión de servidores de Dell pueden ayudar a mejorar la seguridad, la sostenibilidad y la eficiencia de la gestión

### Frente a herramientas de gestión de servidores comparables del Proveedor K

A medida que los centros de datos siguen creciendo, también lo hacen las tareas de los administradores. La infraestructura que ofrece herramientas nativas sólidas de gestión y supervisión con automatización puede hacer que proteger y gestionar el centro de datos sea una tarea más fácil para los administradores que, a menudo, están sobrecargados. Comparamos las funciones y capacidades de las carteras de gestión de Dell y un competidor al que denominaremos Proveedor K:

Tabla 1: Las herramientas de gestión que hemos probado.

	Dell	Proveedor K
<b>Administración de servidores integrada/remota</b>	Dell Technologies Integrated Dell Remote Access Controller 9 (iDRAC9)	Controlador de gestión de la placa base (BMC) del Proveedor K
<b>Administración de dispositivos y consolas de tipo uno a muchos</b>	Dell Technologies OpenManage™ Enterprise (OME)  APEX AIOps Infrastructure Observability (anteriormente CloudIQ)	Consola de gestión empresarial del Proveedor K

Descubrimos que iDRAC9, OME y APEX AIOps Infrastructure Observability (anteriormente CloudIQ) ofrecieron una sólida familia de herramientas de gestión que mejoran la seguridad, ayudan en las medidas de sostenibilidad y facilitan las tareas administrativas diarias en comparación con el uso de herramientas similares del Proveedor K.

# Reforzamiento de la seguridad de los centros de datos

Para las organizaciones que almacenan datos confidenciales de los clientes, la amenaza persistente de los ciberataques exige unas sólidas características de seguridad integrales para garantizar que los datos no terminen en las manos equivocadas. De hecho, hasta "el 83 % de las organizaciones sufrieron más de una vulneración de datos durante 2022",<sup>1</sup> una estadística que acentúa la importancia de tomar precauciones con los datos de los clientes para aumentar la confianza de los consumidores.

Para proteger su organización y sus datos frente a ciberataques costosos, las herramientas de gestión de Dell ofrecen características de seguridad sólidas, tanto integradas en el servidor a través de iDRAC9 como en el software general de gestión de la cloud y la consola. A continuación, exploramos algunas de las características de seguridad clave que utilizan las herramientas de Dell para proteger su sistema y compararlas con las ofertas correspondientes del Proveedor K.

## Seguridad integrada

Todos los servidores Dell PowerEdge integrados a través de iDRAC9 cuentan con características de seguridad que evitan que los atacantes obtengan acceso a los datos. Tres funciones importantes:

- **Bloqueo dinámico del sistema:** el bloqueo del sistema evita que la actividad no intencionada o maliciosa cambie la configuración del BIOS, la iDRAC y el firmware del sistema. El término "dinámico" se refiere a la capacidad de establecer estas capacidades una vez y luego activarlas según sea necesario. (Nota: Esta función está disponible con licencias iDRAC9 Enterprise o Datacenter).
- **Autenticación multifactor (MFA):** MFA solicita a los administradores un código de acceso, además de sus credenciales de inicio de sesión, para mejorar la seguridad.
- **Activación/desactivación del puerto USB dinámico:** la desactivación y habilitación de los puertos USB permite a los administradores controlar el acceso al servidor a través de un puerto USB. El término "dinámico" se refiere a la capacidad de habilitar y deshabilitar estos puertos USB sin reiniciar el servidor ni el sistema operativo. Hasta que el administrador proporcione acceso, nadie puede conectar una memoria o un teclado para modificar los ajustes de configuración del sistema, el sistema operativo o el BIOS.

Como se muestra en la Tabla 2, el Proveedor K no ofreció bloqueo dinámico del sistema ni MFA, y sus capacidades USB dinámicas requieren tiempo de inactividad del sistema (que puede ser muy costoso para las organizaciones), lo que lo hace menos útil y más caro que la solución Dell.

Tabla 2: Comparación de las características de seguridad integradas que ofrecen las herramientas de gestión de servidores. Fuente: Principled Technologies.

	iDRAC9	BMC del Proveedor K
Bloqueo dinámico del sistema	✓	✗
MFA	✓	✗
USB dinámico	✓	✓*

\*Requiere tiempo de inactividad del sistema

## Acerca de Dell Technologies Integrated Dell Remote Access Controller 9

Los servidores Dell PowerEdge™ incluyen iDRAC9 con Dell Lifecycle Controller para proporcionar funciones de administración de sistemas que incluyen alertas del sistema y capacidades de gestión remota. Según Dell, las ventajas clave de iDRAC9 son:

- Automatización ampliable. Las API basadas en estándares, como Redfish y las sólidas herramientas de scripting, como RedHat Ansible, Python, PowerShell y Terraform, le permiten gestionar miles de servidores.
- Compatibilidad integrada, que ofrece una vista del estado del servidor y la supervisión del estado de miles de parámetros
- Funciones y opciones de seguridad sólidas<sup>2</sup>

Para obtener más información sobre las funciones que ofrece iDRAC9, visite <https://www.dell.com/en-us/lp/dt/open-manage-idrac>.

La Figura 1 muestra los resultados de nuestra comparación práctica utilizando iDRAC9 y el BMC del Proveedor K para desactivar dinámicamente los puertos USB.

Con iDRAC9, descubrimos que los administradores podían deshabilitar los puertos USB frontales en un solo servidor en tan solo 41 segundos y 4 pasos. En comparación, con el BMC del Proveedor K, el mismo proceso tardaría 4 minutos y 43 segundos, y 8 pasos por servidor. Esto significa que, por servidor, **la solución Dell tarda un 85 % menos de tiempo y la mitad de los pasos para desactivar puertos USB frontales.**<sup>3</sup> Si se plantea completar estos pasos en un centro de datos, el ahorro de tiempo se acumula. Para una implementación de 100 servidores, los administradores pueden ahorrar 6 horas y 43 minutos con iDRAC9 en comparación con el BMC del Proveedor K.

No solo resulta más fácil y más rápido acceder a estas funciones con iDRAC9 que con el BMC del Proveedor K, sino que con iDRAC9, los administradores pueden mantener los servidores en producción (sin tiempo de inactividad), mientras activan o desactivan estas funciones. El método del Proveedor K requiere tiempo de inactividad, lo que puede implicar costes significativos, y la configuración del sistema cambia cada vez.

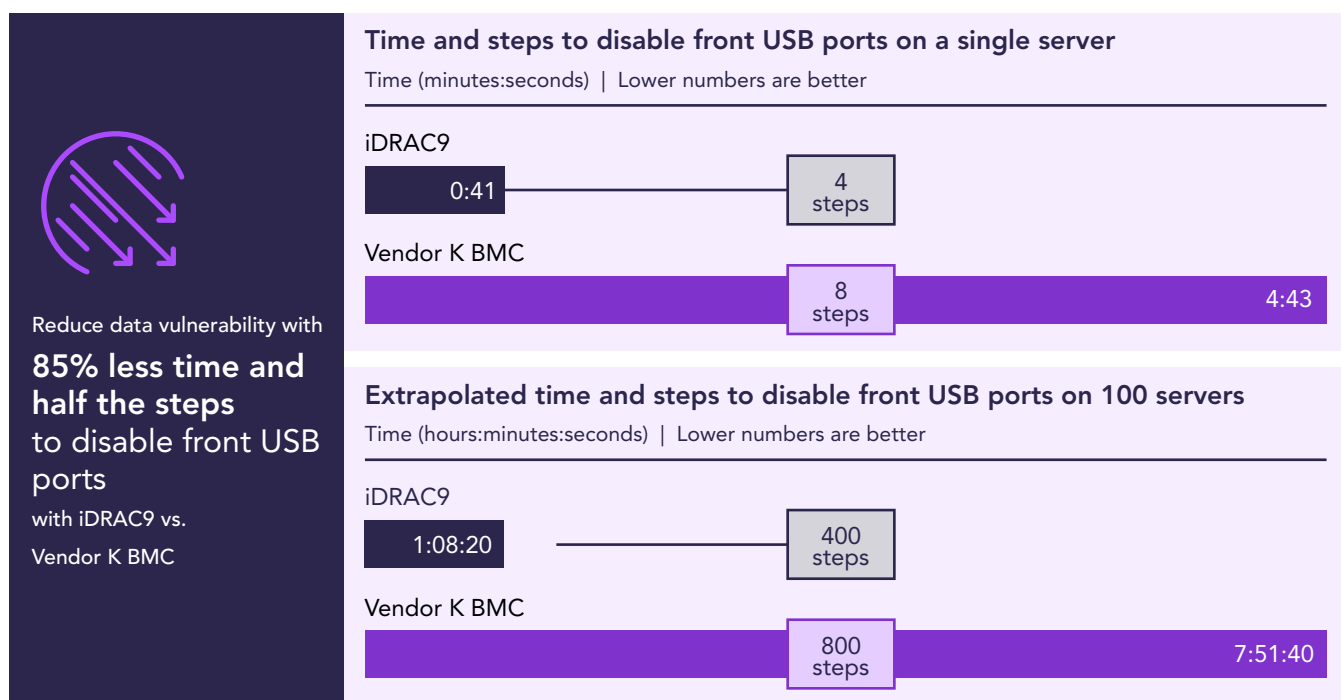


Figura 1: Tiempo para deshabilitar los puertos USB frontales para un solo servidor y tiempo extrapolado para deshabilitar los puertos USB frontales para 100 servidores. Menos tiempo y menos pasos: todo ventajas. Fuente: Principled Technologies.

## Mantener la seguridad con una gestión de credenciales más sencilla en OME







OME proporciona a los administradores una forma muy directa de gestionar la rotación de contraseñas de iDRAC9. En lugar de requerir una cuenta de administrador estática y conocida, OME gestiona los iDRAC a través de una cuenta de servicio en la que los clientes seleccionan la directiva de rotación de contraseñas requerida (para la que nunca se divulga la contraseña) o los administradores pueden gestionar externamente con un tercero. **La consola de gestión empresarial del Proveedor K no tiene capacidades internas de rotación de contraseñas, lo que obliga a los administradores a depender de terceros si desean esta capacidad.** Hemos confirmado que los servidores gestionados por iDRAC9 se integran con la cuenta OME con privilegios de administrador completos para facilitar la gestión de credenciales.

*Nota: Los gráficos de este informe utilizan escalas diferentes. Tenga en cuenta el rango de datos de cada gráfico a medida que compara.*

## Cumplimiento de los objetivos de sostenibilidad

Según el Departamento de Energía de EE. UU., "los centros de datos representan aproximadamente el 2 % del consumo total de electricidad de EE. UU., mientras que la refrigeración del centro de datos puede representar hasta el 40 % del uso de energía del centro de datos en general".<sup>4</sup> A medida que los datos continúan proliferando, estas cifras solo aumentarán, lo que hace que la gestión térmica y de la energía sea vital para reducir los costes del centro de datos y cumplir los objetivos de sostenibilidad para ayudar a mitigar las emisiones de carbono. Para ayudar a las organizaciones a reducir el uso de energía, OME incorpora varias funciones para supervisar y gestionar el consumo de energía. En la tabla 3 se destacan las ventajas clave de estas funciones, que describimos con mayor detalle a continuación.

Tabla 3: Descripción general de las funciones clave de sostenibilidad disponibles en OME frente a la consola de gestión empresarial del Proveedor K. Fuente: Principled Technologies.

Característica	Ventajas clave de las herramientas de gestión de Dell	Desventaja con las herramientas de gestión del Proveedor K
 <b>Calculadora de uso de emisiones de carbono y herramienta de planificación de la capacidad</b>	Capacidad para estimar las <b>emisiones de gases de efecto invernadero</b> con valores personalizables que le ayudarán a cumplir sus objetivos de sostenibilidad	La consola de gestión empresarial del Proveedor K <b>no ofrece ninguna función comparable</b>
 <b>Políticas de límite de energía</b>	El plugin OME Power Manager <b>puede gestionar límites de alimentación</b> para dispositivos o grupos de dispositivos que aplican límites de alimentación cuando se habilitan	La consola de gestión empresarial del Proveedor K <b>no ofrece ninguna función comparable</b>
 <b>Gestión automatizada de la energía y la temperatura</b>	<b>Opciones de política activadas por consumo de energía y temperatura</b> con la opción de activarse cuando el servidor supera un umbral de consumo de energía o temperatura.	La consola de gestión empresarial del Proveedor K <b>no ofrece ninguna función comparable</b>
 <b>Panel del consumo de energía</b>	<b>El panel del plugin OME Power Manager proporciona un acceso rápido</b> a los datos de Power Manager, ya que <b>ofrece 2,75 veces más métricas, con 11 métricas</b>	La consola de gestión empresarial del Proveedor K ofrece <b>solo 4 métricas</b> en el panel
 <b>Informes de consumo de energía</b>	El plugin OME Power Manager proporciona <b>25 informes diferentes predeterminados y personalizables adicionales</b>	La consola de gestión empresarial del Proveedor K <b>no proporciona informes de administración de energía</b>
 <b>Métricas de administración de energía</b>	Hasta <b>3 veces más métricas</b> , lo que ofrece información más granular sobre la gestión del consumo de energía con <b>21 métricas</b>	La consola de gestión empresarial del Proveedor K ofrece <b>solo 7 métricas</b> relacionadas con la administración de energía

### Gestión automatizada de la energía y la temperatura

OME Power Manager ofrece administración automatizada de la energía y la temperatura a través de opciones de directivas de energía estáticas y activadas por temperatura que permiten a los administradores establecer límites para el consumo de energía o los umbrales de temperatura para reducir los costes de refrigeración, respaldar las estrategias de reducción de consumo de energía y responder a eventos térmicos. Por el contrario, **el Proveedor K no ofrece ninguna función de gestión térmica y de alimentación automatizada**. Sin la capacidad de establecer límites basados en la temperatura, el uso de energía podría superar las expectativas y dificultar la planificación teniendo en cuenta la sostenibilidad. Optimizar el consumo de energía es una estrategia importante para cumplir los objetivos de sostenibilidad. El plugin OME Power Manager ofrece **25 informes predeterminados o personalizables relacionados con Power Manager** (17 en dispositivos Power Manager y 8 más en grupos Power Manager) que permiten a los administradores optimizar la planificación de la capacidad y gestionar la potencia para maximizar la eficiencia. **La consola de gestión empresarial del Proveedor K no ofrece informes de administración de energía similares** (consulte la Figura 2).

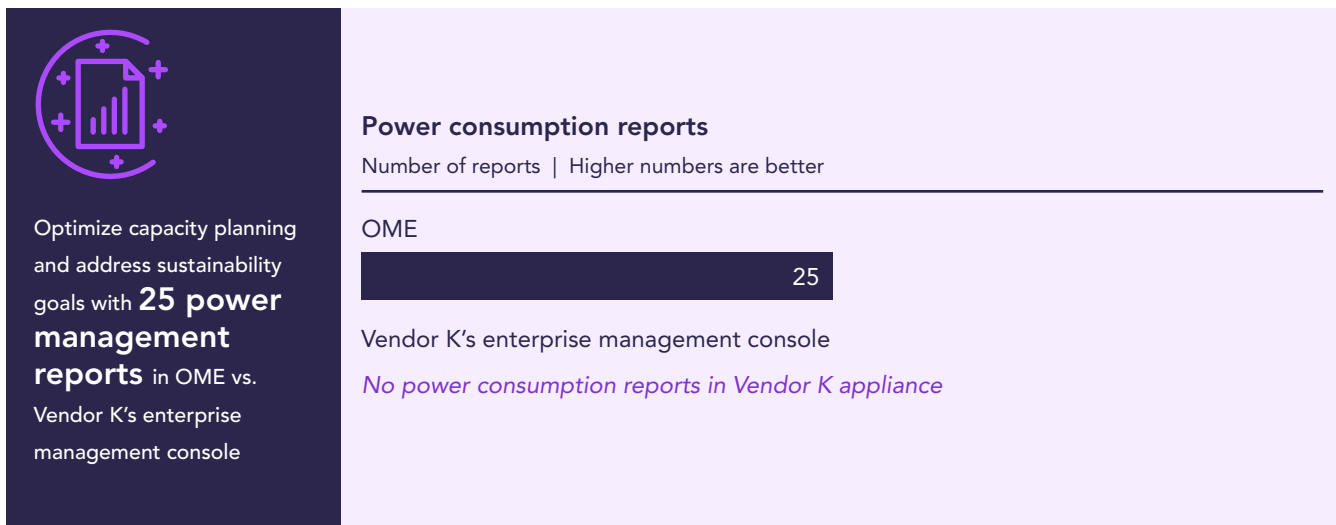


Figura 2: Comparación del número de informes de administración de energía disponibles en la consola de gestión empresarial de OME y el Proveedor K. Mejor cuantos más informes. Fuente: Principled Technologies.

Para optimizar aún más la administración de energía, el plugin OME Power Manager permite a los administradores ver hasta **3 veces más métricas en comparación con la consola de gestión empresarial del Proveedor K** (consulte la Figura 3). OME proporciona 21 métricas diferentes, incluido el uso de energía por componentes individuales, flujo de aire y uso de componentes, mientras que la consola de gestión empresarial del Proveedor K proporciona solo 7 métricas diferentes.

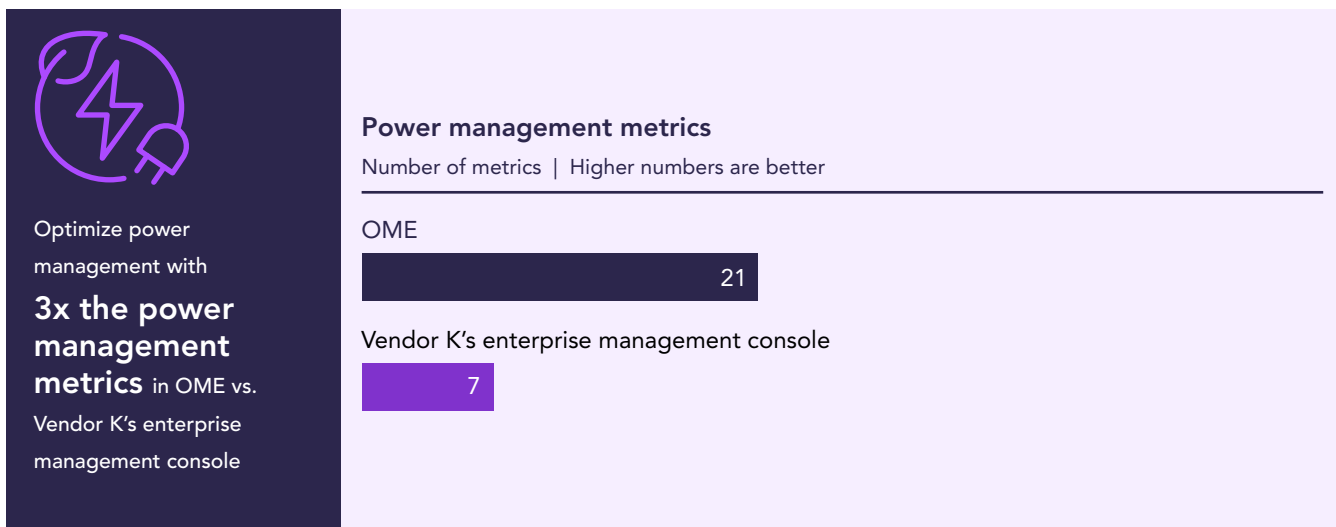


Figura 3: Comparación del número de métricas de administración de energía disponibles en la consola de gestión empresarial de OME y el Proveedor K. Mejor cuantas más métricas. Fuente: Principled Technologies.









### Análisis de emisiones de carbono y huella de carbono





Una función clave de sostenibilidad que OME incluye es una calculadora de uso de emisiones de carbono y una herramienta de planificación de la capacidad. Esta herramienta ayuda a las organizaciones a calcular sus emisiones de gases de efecto invernadero, proporcionando valores predeterminados para los costes de energía y las emisiones de carbono por unidad de energía consumida. Esta función también permite la personalización, lo que ofrece a las organizaciones la capacidad de introducir valores para los costes de energía y las emisiones de carbono de su región para el modelo de consumo de su centro de datos. La consola de gestión empresarial del Proveedor K no tiene una función comparable, lo que puede obstaculizar la capacidad de una organización para planificar teniendo en cuenta la sostenibilidad.

## Reduzca la carga de gestión con funciones sólidas de supervisión y gestión

A medida que crece la infraestructura, también pueden crecer las responsabilidades de los administradores del centro de datos. Al elegir herramientas de gestión de servidores que automatizan ciertas tareas y mejoran la gestión diaria, las organizaciones permiten a los administradores ser más eficientes y tener más tiempo para planificar el futuro. Descubrimos que la cartera de gestión de servidores de Dell ofreció una serie de funciones que pueden simplificar las tareas de los administradores. En la tabla 4 se ofrece un resumen de las funciones clave de facilidad de uso disponibles en la cartera de gestión de Dell frente a las herramientas de gestión del Proveedor K.

Tabla 4: Descripción general de las funciones clave de facilidad de uso disponibles en las herramientas de gestión de Dell frente a las herramientas de gestión del Proveedor K. Fuente: Principled Technologies.

Característica	Ventajas clave de las herramientas de gestión de Dell	Desventaja con las herramientas de gestión del Proveedor K
 <b>Más funciones remotas del BIOS</b>	Gestión remota más sencilla con <b>51 funciones remotas del BIOS en iDRAC9</b>	El BMC del Proveedor K <b>solo ofrece una función remota del BIOS</b>
 <b>Cambios más sencillos en la configuración del BIOS</b>	<b>Un 87 % menos de tiempo y la mitad de pasos</b> para realizar un cambio en la configuración del BIOS	El Proveedor K requiere <b>la intervención manual del administrador</b> para realizar cambios desde las utilidades del sistema
 <b>Importar/exportar la configuración completa del servidor</b>	<b>Configuración más rápida de varios servidores idénticos</b> con la capacidad de exportar/importar los ajustes de configuración de un servidor completamente configurado	El Proveedor K <b>solo proporciona copias de seguridad y restauración del BMC para cada servidor individual</b>
 <b>Actualizaciones programadas automatizadas</b>	iDRAC9 proporciona a los administradores la capacidad de <b>programar actualizaciones automatizadas</b> desde un repositorio durante una ventana de mantenimiento sin intervención adicional del administrador	El BMC del Proveedor K <b>no ofrece actualizaciones automatizadas programadas</b>
 <b>Descripción general completa del estado del almacenamiento</b>	iDRAC9 proporciona una representación visual del estado de almacenamiento para <b>identificar rápidamente las unidades con estado de alerta</b>	El BMC del Proveedor K <b>no proporciona una vista similar</b>
 <b>Streaming de telemetría</b>	iDRAC9 <b>proporciona telemetría para el doble de categorías de métricas, con un total de 8 categorías</b>	El BMC del Proveedor K <b>BMC proporciona telemetría para solo 4 categorías</b>
 <b>Vista de conexión</b>	La vista de conexión en iDRAC9 <b>proporciona detalles de la asignación física de los puertos del switch</b> a los puertos de red del servidor y las conexiones de puertos dedicados de iDRAC	El BMC del Proveedor K <b>no tiene información de conexión física</b> para los switches ascendentes
 <b>Capacidad de ampliación</b>	OME <b>puede gestionar hasta 8000 dispositivos<sup>5</sup></b>	El Proveedor K <b>solo puede gestionar hasta 1000 dispositivos</b>

Característica	Ventajas clave de las herramientas de gestión de Dell	Desventaja con las herramientas de gestión del Proveedor K
 <b>Acciones basadas en alertas</b>	OME proporciona <b>2 veces más acciones basadas en alertas (con 12)</b> que desencadenan acciones basadas en la entrada de una alerta.	El Proveedor K solo ofrece <b>4 acciones basadas en alertas</b>
 <b>Arquitectura de plugin</b>	OME ofrece la capacidad de <b>ampliar la funcionalidad con plugins</b> que los administradores pueden añadir a la consola sin necesidad de gestionar aplicaciones adicionales	La consola de administración empresarial del Proveedor K <b>no ofrece arquitectura basada en plugins</b> para capacidad de ampliación
 <b>Supervisión de dispositivos de terceros</b>	OME <b>admite la supervisión de dispositivos y servidores de terceros</b>	La consola de gestión empresarial del Proveedor K <b>no admite</b> la supervisión de dispositivos y servidores de terceros
 <b>Generación de informes</b>	OME ofrece a los administradores <b>42 informes integrados</b> con personalización para que los administradores puedan seleccionar granularmente los datos más importantes para sus fines	La consola de gestión empresarial del Proveedor K <b>no tiene creación de informes nativos</b>

## Gestión remota

Con iDRAC9, los administradores no necesitan entrar en el centro de datos para cada cambio. iDRAC9 ofrece 51 funciones remotas del BIOS para dar a los administradores la libertad de realizar más cambios desde fuera del centro de datos, en comparación con solo uno para BMC del Proveedor K, que proporciona a los administradores un control significativamente más granular sobre la configuración del BIOS desde cualquier lugar (consulte la Figura 4).

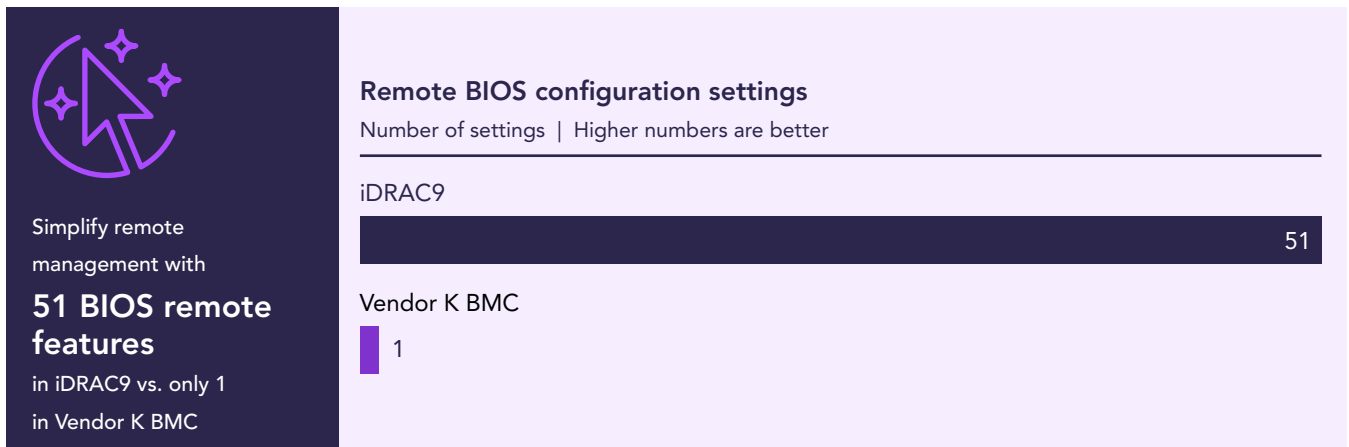


Figura 4: Comparación de las funciones remotas del BIOS que ofrece cada herramienta de gestión. Cuantas más funciones mejor. Fuente: Principled Technologies.

## Aplicación de cambios en la configuración

Con iDRAC9, los administradores pueden cambiar la configuración del BIOS y realizar la actualización para un reinicio posterior sin necesidad de presencia adicional de administradores, mientras que el BMC del Proveedor K requiere cambios desde las utilidades del sistema y la intervención manual del administrador durante el cambio. Como se muestra en la Figura 5, la preparación del cambio en la configuración del BIOS para un reinicio programado llevó un 87 % menos de tiempo y la mitad de los pasos con iDRAC9 en comparación con el BMC del Proveedor K. Al extrapolar estos ahorros a grandes implementaciones, el ahorro de tiempo de administración aumenta. Por ejemplo, en una implementación de 100 servidores, los administradores podrían ahorrar más de 6 horas cambiando los elementos de configuración del BIOS.

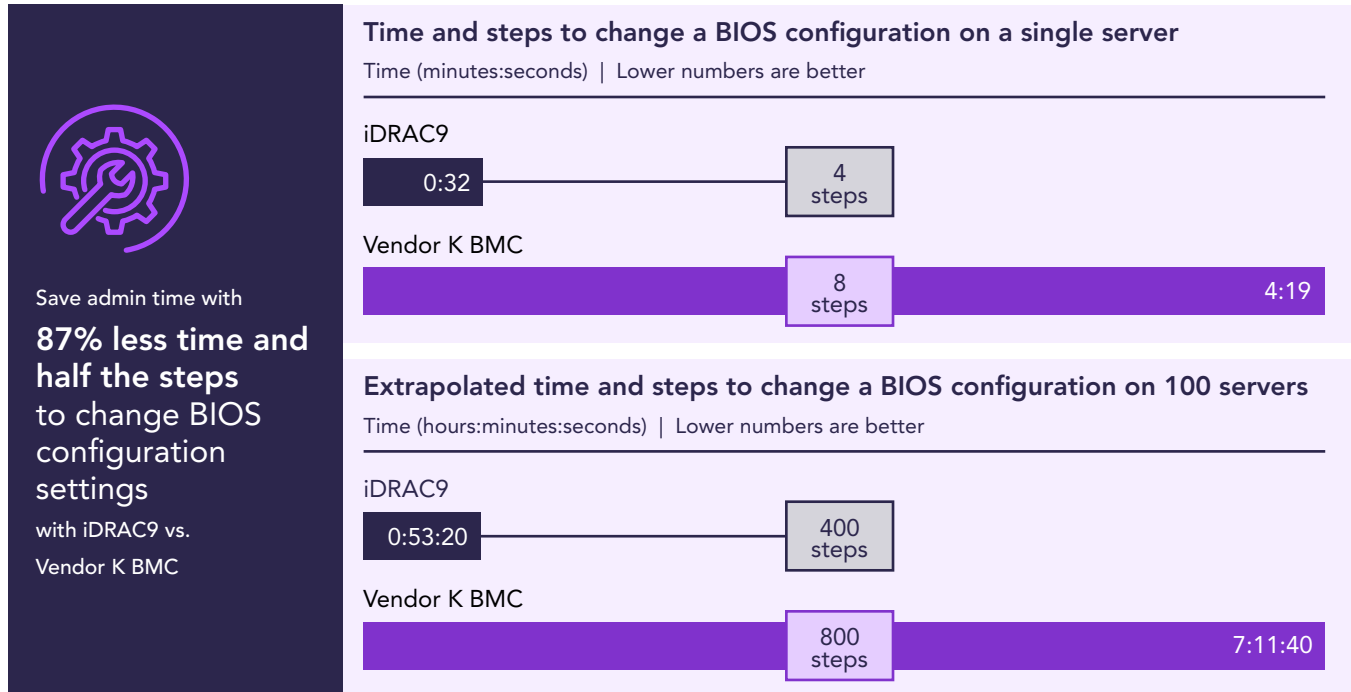


Figura 5: Hora de cambiar la configuración del BIOS y poner en marcha la actualización para un reinicio posterior de un solo servidor y tiempo extrapolado para 100 servidores. Menos tiempo y menos pasos: todo ventajas. Fuente: Principled Technologies.

## Configurar acciones basadas en alertas

Los administradores pueden aprovechar mejor su tiempo cuando no están vinculados a un escritorio y supervisar el estado del entorno. Como se muestra en la Figura 6, OME proporciona 12 opciones basadas en políticas para acciones basadas en alertas, de modo que la mitigación de problemas se inicia automáticamente cuando el entorno alcanza ciertos umbrales. Por el contrario, la consola de gestión empresarial del Proveedor K permite a los administradores configurar solo cuatro eventos basados en alertas.

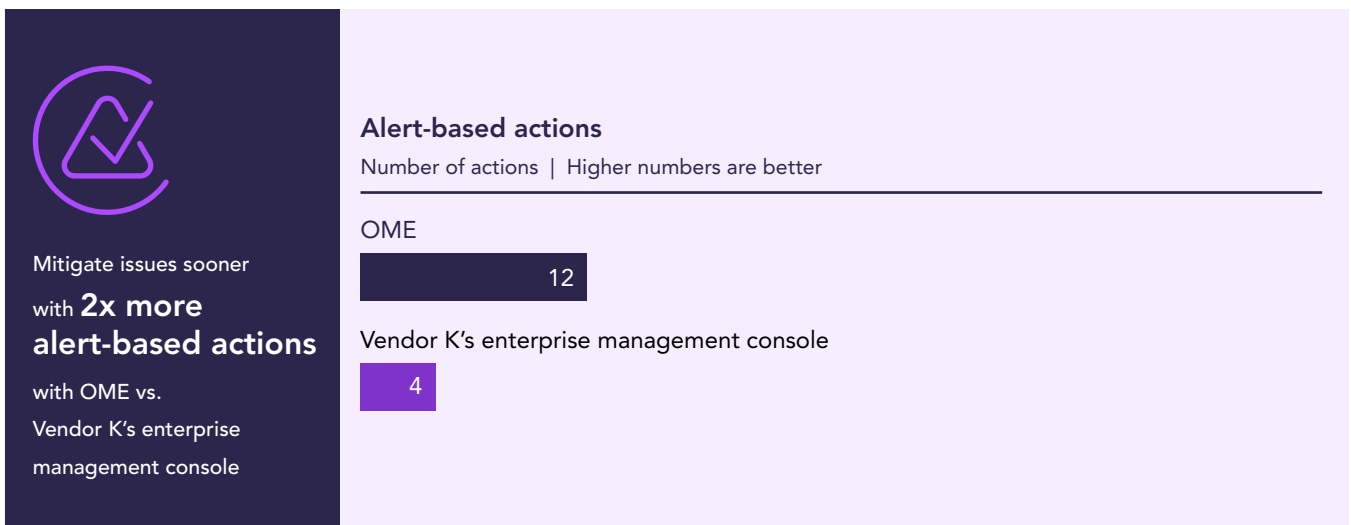


Figura 6: Comparación de la acción basada en alertas que ofrece cada herramienta de gestión. Mejor cuantas más acciones. Fuente: Principled Technologies.

## Acerca de Dell Technologies OpenManage Enterprise

OME es una consola de administración de sistemas de tipo uno a muchos para el centro de datos. La consola ofrece una interfaz gráfica de usuario HTML5 moderna y se implementa como un dispositivo virtual para entornos VMware ESXi™, Microsoft Hyper-V y máquinas virtuales basadas en kernel (KVM). OME puede detectar e inventariar redes IPv4 e IPv6 para hasta 8000 dispositivos, incluidos servidores de montaje en rack Dell, servidores torre Dell, y blades y chasis Dell.<sup>6</sup> En un estudio reciente de PT, descubrimos que un entorno de Dell con OME y OpenManage Enterprise Modular (OME-M) puede ahorrar tiempo al realizar cambios en las VLAN y ayudar a evitar intervenciones durante las actualizaciones de firmware programadas.<sup>7</sup>

Obtenga más información sobre OME en <https://www.dell.com/en-us/lp/dt/open-manage-enterprise>.




## Gestión basada en la cloud con APEX AIOps Infrastructure Observability (anteriormente CloudIQ)

Las herramientas integradas y las consolas de gestión empresarial no son las únicas herramientas de la cartera de gestión de servidores de Dell. Con APEX AIOps Infrastructure Observability (anteriormente CloudIQ), los administradores obtienen otra forma automatizada y fácil de usar de mantener bajo control el estado y la seguridad de su infraestructura, esta vez desde la cloud.

### Características de seguridad adicionales disponibles en APEX AIOps Infrastructure Observability (anteriormente CloudIQ)

APEX AIOps Infrastructure Observability (anteriormente CloudIQ) ofrece varias características de seguridad que pueden reforzar aún más su organización contra los ataques. En la tabla 5 se destacan algunas de estas características de seguridad clave.

Tabla 5: Descripción general de las funciones de seguridad clave disponibles en APEX AIOps Infrastructure Observability (anteriormente CloudIQ). Fuente: Principled Technologies.

Característica	Cómo funciona APEX AIOps Infrastructure Observability (anteriormente CloudIQ) para proteger su entorno
 <b>Alertas de nivel de riesgo de ciberseguridad</b>	Proporciona información automatizada sobre la ciberseguridad con <b>alertas de nivel de riesgo de seguridad específicas</b> para que los administradores puedan reaccionar más rápido y abordar los problemas rápidamente para proteger los datos
 <b>Acceso seguro basado en directivas</b>	Ofrece <b>ajustes de configuración de seguridad basados en políticas y plantillas fáciles de aplicar</b> que permiten a los administradores garantizar que los ajustes de las prácticas recomendadas de seguridad estén establecidos, protegiendo el entorno PowerEdge.
 <b>Asesorías de ciberseguridad</b>	Proporciona <b>informes de asesoría de seguridad relevantes</b> , que ofrecen detalles específicos de vulnerabilidad y sugerencias para la corrección, lo que permite tomar medidas rápidas para eliminar las brechas de seguridad.

## Acerca de APEX AIOps Infrastructure Observability (anteriormente CloudIQ)







APEX AIOps Infrastructure Observability (anteriormente CloudIQ) es una herramienta de AIOps basada en la cloud que ofrece "supervisión proactiva, aprendizaje automático y análisis predictivo" para una gran cantidad de productos y servicios de Dell, incluidos servidores, almacenamiento, dispositivos de protección de datos e infraestructura hiperconvergente.<sup>8</sup> En un estudio de Principled Technologies de 2022, descubrimos que CloudIQ tenía un impacto insignificante en el ancho de banda de la red, al tiempo que nos permitía supervisar la telemetría, el estado, las alertas y el inventario desde una sola consola.<sup>9</sup>

Obtenga más información sobre APEX AIOps Infrastructure Observability (anteriormente CloudIQ) en <https://www.dell.com/en-us/dt/apex/aiops.htm>.

## Funciones adicionales de sostenibilidad y eficiencia disponibles en APEX AIOps Infrastructure Observability (anteriormente CloudIQ)

APEX AIOps Infrastructure Observability (anteriormente CloudIQ) también proporciona funciones que refuerzan la sostenibilidad y la eficiencia, y se integran con iDRAC9 y OME para facilitar a los administradores la supervisión del estado de su entorno PowerEdge. En la Tabla 6 se destacan algunas de estas funciones.

Tabla 6: Descripción general de las funciones de gestión de sostenibilidad y facilidad de uso disponibles en APEX AIOps Infrastructure Observability (anteriormente CloudIQ). Fuente: Principled Technologies.

Característica	Ventajas clave de APEX AIOps Infrastructure Observability (anteriormente CloudIQ)
 <b>Análisis de la huella de carbono</b>	Esta herramienta, que se encuentra en la sección de monitorización, <b>puede predecir las emisiones de carbono</b> y ofrece una visión más detallada en todos los entornos
 <b>Vistas de rendimiento</b>	Proporciona vistas de rendimiento y gráficos de anomalías y uso para <b>alertar a los administradores ante el primer indicio de problemas</b>
 <b>Informes de cumplimiento normativo personalizados</b>	Proporciona a los usuarios la capacidad de <b>crear informes de cumplimiento normativo personalizados</b> para determinados dispositivos
 <b>Informes de inventario y rendimiento personalizables</b>	Proporciona <b>opciones de creación de informes personalizadas</b> para el rendimiento de los servidores y los datos de inventario, lo que da a los administradores un mayor control sobre el rendimiento y las métricas de los dispositivos que les interesan realizar el seguimiento
 <b>Programación de trabajos de acciones de alimentación</b>	Realice acciones de alimentación, como la limitación de la alimentación en varios servidores Dell PowerEdge supervisados en <b>solo 35 segundos y 6 pasos</b> .
 <b>Programación de actualizaciones de firmware</b>	Programa actualizaciones de firmware de PowerEdge para varios servidores supervisados en <b>tan solo 41 segundos y 9 pasos</b>

## Conclusión

En nuestra comparación de las funciones de seguridad, sostenibilidad y gestión y supervisión, descubrimos que la cartera de herramientas de gestión de servidores de Dell proporcionaba funciones de gestión y supervisión más sólidas que la cartera del Proveedor K. En el ámbito de la seguridad, iDRAC9 ofrecía más funciones, como el bloqueo dinámico del sistema y la autenticación multifactor, que el Proveedor K no ofrecía en absoluto. Además, iDRAC9 redujo significativamente el tiempo necesario para deshabilitar los puertos USB y reducir la vulnerabilidad de los datos.

Gracias al análisis de la huella de carbono y a las sólidas herramientas de administración de energía, descubrimos que OME podría ayudar mejor a las organizaciones a planificar sus objetivos de sostenibilidad que con la consola de administración empresarial del Proveedor K. Además, descubrimos que la cartera de gestión de servidores de Dell proporcionaba más automatización y más opciones de gestión remota, lo que reducía el tiempo y el esfuerzo del administrador para ciertas tareas rutinarias de supervisión y mantenimiento. Estos logros en seguridad, sostenibilidad y funciones de gestión y supervisión convierten a la cartera de gestión de servidores de Dell en una opción atractiva para las organizaciones que buscan un centro de datos más eficiente y seguro.

1. Harvard Business Review, "The Devastating Business Impacts of a Cyber Breach", acceso el 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)", acceso el 17 de mayo de 2024, <https://www.dell.com/en-us/lp/dt/open-manage-idrac>.
3. Nota: La desactivación de puertos USB del Proveedor K es personalizable, aunque esto significa que los administradores tienen que seleccionar cada puerto para desactivarlo, en lugar de por grupo.
4. DOE, "DOE Announces \$40 Million for More Efficient Cooling for Data Centers", acceso el 20 de mayo de 2024, <https://www.energy.gov/articles/doe-announces-40-million-more-efficient-cooling-data-centers>.
5. Dell, "OpenManage Enterprise Support Matrix", acceso el 21 de mayo de 2024, <https://www.dell.com/support/kbdoc/en-us/article/lkbprint?ArticleNumber=000217909&AccessLevel=10&Lang=en>.
6. Dell, "OpenManage Enterprise", acceso el 17 de mayo de 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", acceso el 17 de mayo de 2024, <https://www.principledtechnologies.com/Dell/PowerEdge-MX-OME-OME-M-0124.pdf>.
8. Dell, "APEX AIOps: Tame IT complexity in your digital business", acceso el 11 de junio de 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", acceso el 9 de abril de 2024, <https://www.principledtechnologies.com/dell/CloudIQ-network-0422.pdf>.

Lea la ciencia detrás de este informe ▶

▶ Consulte la versión original en inglés de este informe



Facts matter.®

Este proyecto fue encargado por Dell Technologies.

Principled Technologies es una marca comercial registrada de Principled Technologies, Inc. El resto de los nombres de productos son las marcas comerciales de sus respectivos propietarios. Para obtener información adicional, consulte los datos científicos sobre los que se fundamenta este informe.