Reduce data vulnerability with

85% less time to disable front USB ports

in iDRAC9 vs. Vendor K BMC

Help mitigate carbon emissions with

25 customizable power consumption reports

in OME vs. 0 reports in Vendor K's enterprise management console

Schedule automatic

firmware updates in just 41 seconds

in APEX AIOps Infrastructure Observability (formerly CloudIQ)

Dell server management tools can help improve security, sustainability, and management efficiency

vs. comparable server management tools from Vendor K

As data centers continue to grow, so do administrator duties. Infrastructure that offers native robust management and monitoring tools with automation can make securing and managing the data center an easier task for often over-burdened administrators. We compared the features and capabilities of the management portfolios from Dell and a competitor we will refer to as Vendor K:

Table 1: The management tools we tested.

	Dell	Vendor K
Embedded/remote server management	Dell Technologies Integrated Dell Remote Access Controller 9 (iDRAC9)	Vendor K baseboard management controller (BMC)
One-to-many device and console management	Dell Technologies OpenManage™ Enterprise (OME) APEX AIOps Infrastructure Observability (formerly CloudIQ)	Vendor K's enterprise management console

We found that iDRAC9, OME, and APEX AIOps Infrastructure Observability (formerly CloudIQ) offered a strong family of management tools that could improve security, aid in sustainability measures, and make day-to-day admin tasks easier compared to using similar tools from Vendor K.

Strengthening data center security

For organizations storing sensitive customer data, the persistent threat of cyberattacks demands strong end-to-end security features to ensure data doesn't end up in the wrong hands. In fact, up to "83% of organizations experienced more than one data breach during 2022,"[1] a statistic that accentuates how important it is to take precautions with customer data to increase consumer confidence.

To protect your organization and its data from costly cyberattacks, Dell management tools offer strong security features both embedded in the server via iDRAC9 and in overarching console and cloud management software. Below, we explore some of the key security features Dell tools use to protect your system and compare them to corresponding offerings from Vendor K.

Embedded security

Built into every Dell PowerEdge server via iDRAC9 are security features that work to stop bad actors from gaining access to data. Three such important features are:

- **Dynamic System Lockdown:** System Lockdown prevents unintended or malicious activity from changing system BIOS, iDRAC, and firmware settings. Dynamic refers to the ability to set up these capabilities once, and then enact as needed. (Note: This feature is available with iDRAC9 Enterprise and Datacenter licenses.)
- **Multi-factor authentication (MFA):** MFA prompts admins for a passcode in addition to their login credentials to bolster security.
- **Dynamic USB port enabling/disabling:** Disabling and enabling USB ports gives administrators control over access to the server via a USB port. Dynamic refers to the ability to enable and disable these USB ports without rebooting the server or restarting the OS. Until the admin provides access, no one can plug in a memory stick or keyboard to modify any configuration settings of the system, OS, or BIOS.

As Table 2 shows, Vendor K did not offer dynamic system lockdown or MFA, and its dynamic USB capabilities require system downtime (which can be very costly for organizations), making it less useful and more expensive than the Dell solution.

Table 2: Comparison of built-in security features that the server management tools offer. Source: Principled Technologies.

	iDRAC9	Vendor K BMC
Dynamic System Lockdown	✓	✗
MFA	✓	✗
Dynamic USB	✓	✓*

**Requires system downtime*

About Dell Technologies Integrated Dell Remote Access Controller 9

Dell PowerEdge™ servers include iDRAC9 with Dell Lifecycle Controller to provide systems administration functions that include system alerts and remote management capabilities. According to Dell, key benefits of iDRAC9 include:

- Scalable automation. Standards-based APIs such as Redfish and robust scripting tools like RedHat Ansible, Python, PowerShell, Terraform, let you manage thousands of servers.
- Embedded support, offering a view of server health and status monitoring thousands of parameters
- Strong security features and options[2]

To learn more about the features iDRAC9 provides, visit https://www.dell.com/en-us/lp/dt/open-manage-idrac.

Figure 1 shows the results of our hands-on comparison using iDRAC9 and Vendor K BMC to dynamically disable USB ports.

Using iDRAC9, we found that administrators could disable front USB ports on a single server in just 41 seconds and 4 steps. In comparison, with the Vendor K BMC the same process would take 4 minutes 43 seconds and 8 steps per server. This means that per server, **the Dell solution takes 85 percent less time and half the steps to disable front USB ports**.[3] When you consider completing these steps in a data center, the time savings add up; for a 100-server deployment, admins could save 6 hours 43 minutes with iDRAC9 compared to the Vendor K BMC.

Not only are these features easier and faster to access with iDRAC9 than with the Vendor K BMC, but with iDRAC9, admins can keep the servers in production (no downtime) while enabling or disabling these features. The Vendor K method requires downtime, which can incur significant costs, and system setup configuration changes each time.

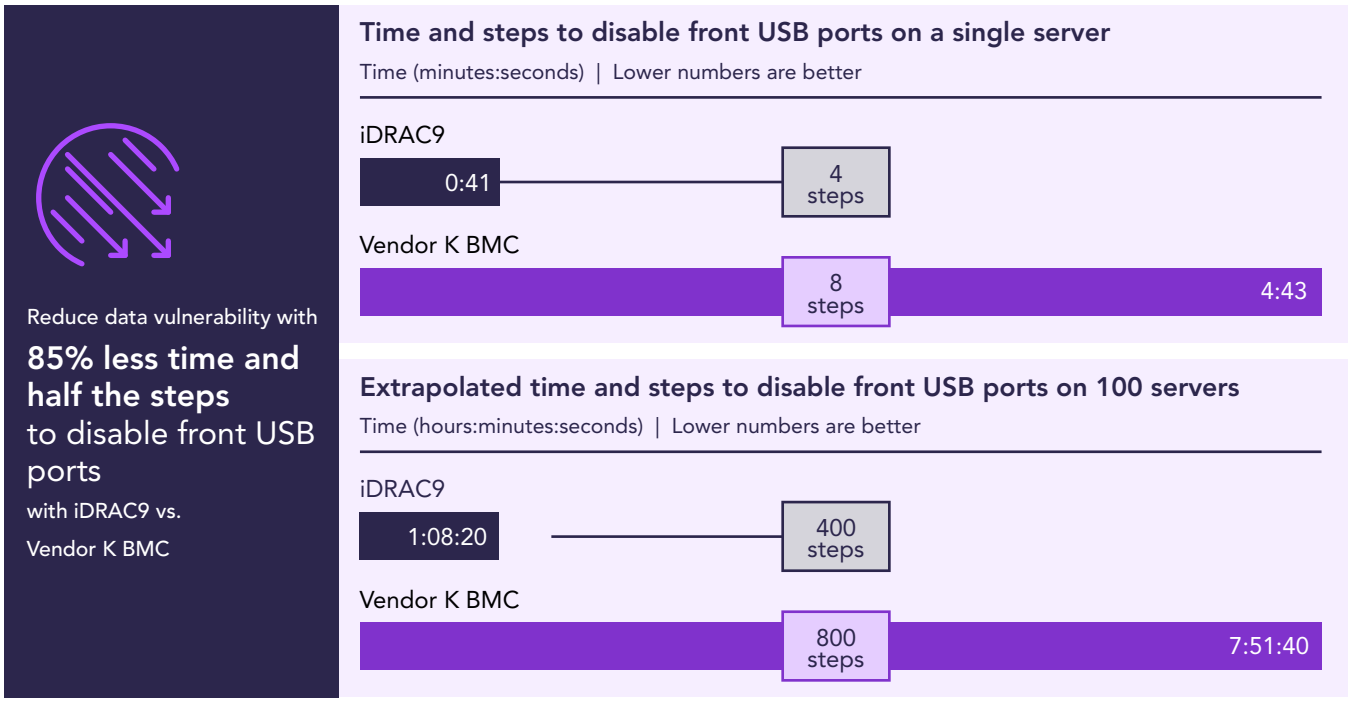

Figure 1: Time to disable front USB ports for a single server and extrapolated time to disable front USB ports for 100 servers. Less time and fewer steps are better. Source: Principled Technologies.

Keeping secure with easier credential management in OME

OME provides administrators a straightforward way to manage iDRAC9 password rotation. Rather than requiring a static, known administrator account, OME manages iDRACs via a service account where customers select the required password rotation policy—for which the password is never disclosed—or administrators can manage externally with a third party. **Vendor K's enterprise management console doesn't have internal password rotation capabilities, forcing admins to rely on a third party if they want this capability.** We confirmed that iDRAC9-managed servers integrated with the OME account with full administrator privileges for easier credential management.

Note: The graphs in this report use different scales.
Please be mindful of each graph's data range as you compare.

Meeting sustainability goals

According to the US Department of Energy, "data centers account for approximately 2% of total U.S. electricity consumption, while data center cooling can account for up to 40% of data center energy usage overall."[4] As data continues to proliferate, these numbers will only grow, making thermal and power management vital to keeping data center costs down as well as meeting sustainability goals to help mitigate carbon emissions. To help organizations reduce power usage, OME incorporates several features for monitoring and management of power consumption. Table 3 highlights key benefits of these features, which we describe in greater detail below.

Table 3: Overview of key sustainability features available in OME vs. Vendor K's enterprise management console. Source: Principled Technologies.

Feature	Key benefits with Dell management tools	Disadvantage with Vendor K management tools
Carbon emission usage calculator and capacity planning tool	Ability to estimate **greenhouse gas emissions** with customizable values to help meet sustainability goals	Vendor K's enterprise management console offers **no comparable feature**
Power cap policies	OME Power Manager plugin **can manage power caps** for devices or groups of devices that enforce power limits when enabled	Vendor K's enterprise management console offers **no comparable feature**
Automated power and thermal management	**Power and temperature-triggered policy** options with the option to trigger when the server crosses a power consumption or temperature threshold	Vendor K's enterprise management console offers **no comparable feature**
Power-consumption dashboard	OME Power Manager Plugin **dashboard provides quick access** to Power Manager Data, **offering 2.75x the metrics, with 11 metrics**	Vendor K's enterprise management console offers **just 4 metrics** on the dashboard
Power consumption reports	OME Power Manager Plugin provides **25 different default and additional customizable reports**	Vendor K's enterprise management console provides **no power management reports**
Power management metrics	Up to **3x the metrics**, offering more granular insight into power consumption management with **21 metrics**	Vendor K's enterprise management console offers **just 7 metrics** related to power management

Automated power and thermal management

OME Power Manager offers automated power and thermal management through both static power and temperature-triggered policy options that allow administrators to set limits for power consumption or temperature thresholds to reduce cooling costs, support reduction power strategies, and respond to thermal events. In contrast, **Vendor K offers no automated power and thermal management feature**. Without the ability to set temperature-based limits, energy usage could exceed expectations and make it difficult to plan with sustainability in mind. Optimizing power consumption is an important strategy in meeting sustainability goals. OME Power Manager Plugin offers **25 default and/or customizable Power Manager-related reports** (17 in Power Manager Devices and 8 more in Power Manager Groups) that allow administrators to optimize capacity planning and manage power to maximize efficiency. **Vendor K's enterprise management console offers no similar power management reports** (see Figure 2).

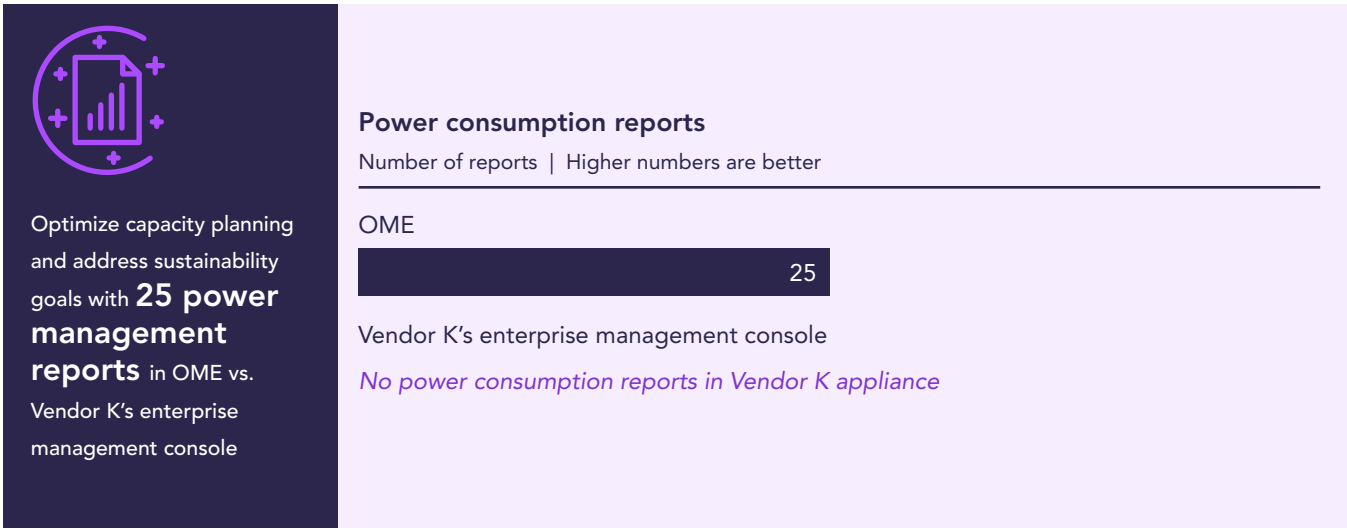

Figure 2: Comparison of the number of power management reports available in OME and Vendor K's enterprise management console. More reports are better. Source: Principled Technologies

To further optimize power management, the OME Power Manager plugin allows administrators to view up to **3x the metrics compared to Vendor K's enterprise management console** (see Figure 3). OME provides 21 different metrics, including power usage by individual components, air flow, and component utilization, whereas Vendor K's enterprise management console provides only 7 different metrics.

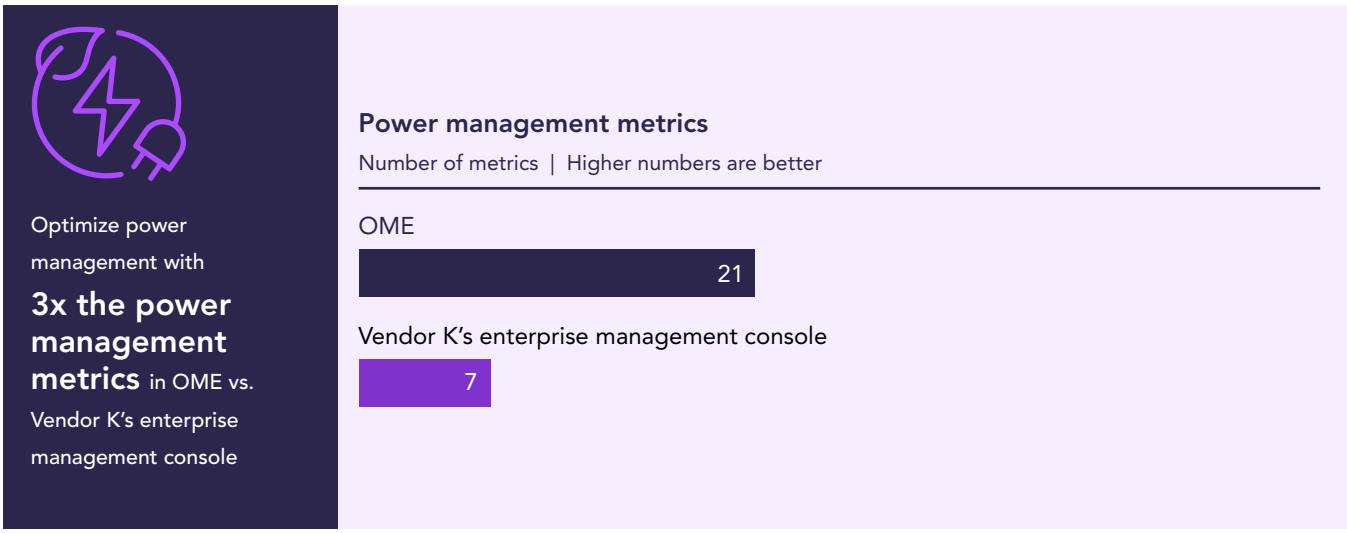

Figure 3: Comparison of the number of power management metrics available in OME and Vendor K's enterprise management console. More metrics are better. Source: Principled Technologies.

Carbon emissions and carbon footprint analysis

A key sustainability feature **OME includes is a carbon emission usage calculator and capacity planning tool**. This tool helps organizations estimate their greenhouse gas emissions, providing default values for power costs and carbon emissions per unit of energy consumed. This feature also allows for customization, giving organizations the ability to enter values for their own region's power costs and carbon emissions for data specific to their data center's consumption model. **Vendor K's enterprise management console doesn't have a comparable feature**—which can hamper an organization's ability to plan with sustainability in mind.

Easing the management burden with robust monitoring and management features

As infrastructure grows, so can data center administrator responsibilities. By choosing server management tools that automate certain tasks and improve day-to-day management, organizations can help admins become more efficient and give them more time to plan for the future. We found the Dell server management portfolio offered a number of features that can simplify administrator tasks. Table 4 provides a summary of key ease-of-use features available in the Dell management portfolio vs. Vendor K management tools.

Table 4: Overview of key ease-of-use features available in Dell management tools vs. Vendor K management tools. Source: Principled Technologies.

Feature	Key benefits with Dell management tools	Disadvantage with Vendor K management tools
 **More remote BIOS features**	Easier remote management with **51 remote BIOS features in iDRAC9**	Vendor K BMC offers **only 1** remote BIOS feature
 **Easier BIOS configuration changes**	**87% less time and half the steps** to make a BIOS configuration change	Vendor K requires **manual admin intervention** to make changes from within the system utilities
 **Full server configuration import/export**	**Faster configuration of multiple identical servers** with the ability to export/import configuration settings for a fully configured server	Vendor K provides **only backup and restore of the BMC for each individual server**
 **Automated scheduled updates**	iDRAC9 provides administrators the ability to **schedule automated updates** from a repository during a maintenance window without additional administrator intervention	Vendor K BMC **doesn't offer scheduled automated updates**
 **Comprehensive storage status overview**	iDRAC9 provides a visual representation of storage status, for **quickly identifying drives with alert status**	Vendor K BMC **does not** provide a similar view
 **Telemetry streaming**	iDRAC9 **provides telemetry for 2x as many metric categories, with 8 total categories**	Vendor K BMC provides telemetry for **only 4 categories**
 **Connection View**	Connection View in iDRAC9 **provides details of the physical mapping of switch ports to server's network ports and iDRAC dedicated port connections**	Vendor K BMC has **no physical connection information** to upstream switches
 **Scalability**	OME **can manage up to 8,000 devices**[5]	Vendor K can manage **only** up to **1,000 devices**

Feature	Key benefits with Dell management tools	Disadvantage with Vendor K management tools
Alert-based actions	OME provides **2x more alert-based actions (with 12)** that trigger actions based on input from an alert	Vendor K offers only **4 alert-based actions**
Plugin architecture	OME offers the ability to **expand functionality with plugins** that admins can add to the console without the need for additional applications to manage	Vendor K's enterprise management console **does not offer plugin-based architecture** for expandability
Third-party device monitoring	OME **supports third-party device and server monitoring**	Vendor K's enterprise management console **does not support** third-party device and server monitoring
Reporting	OME offers admins **42 built-in reports** with customization so admins can granularly select the most important data for their purposes	Vendor K's enterprise management console has **no native report creation**

Remote management

With iDRAC9, admins needn't enter the data center for every change. iDRAC9 offers 51 remote BIOS features to give admins the freedom to make more changes from outside the data center, compared to just one for Vendor K BMC, which gives administrators significantly more granular control over BIOS configuration from anywhere (see Figure 4).

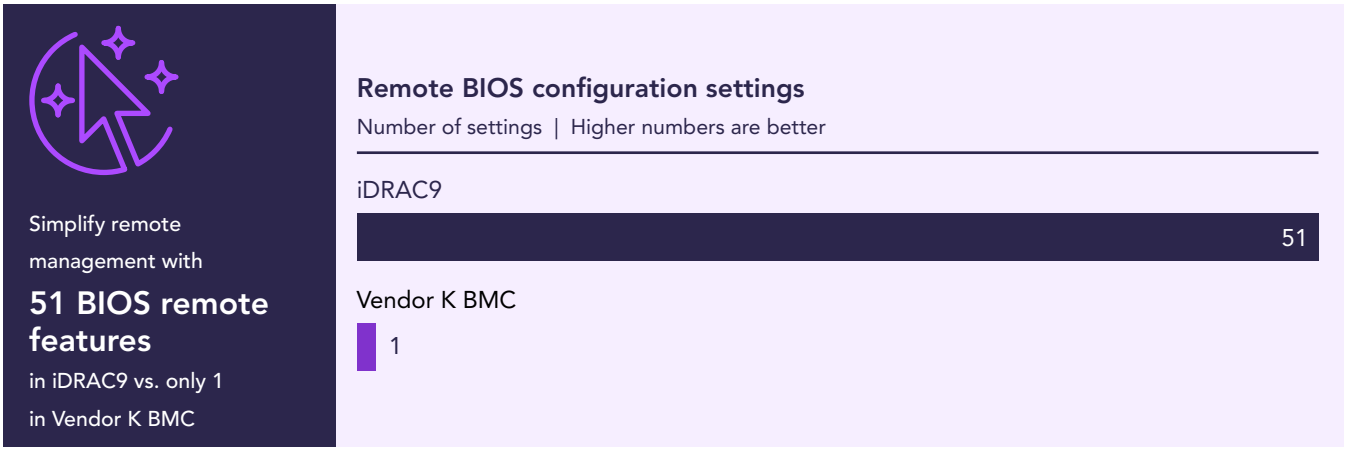

Figure 4: Comparison of BIOS remote features each management tool offers. More features are better. Source: Principled Technologies.

Making configuration changes

With iDRAC9, administrators can change BIOS configuration settings and stage the update for a later reboot without the need for additional administrator presence, while the Vendor K BMC requires changes from within the system utilities and manual administrator intervention during the change. As Figure 5 shows, staging the BIOS configuration change for a scheduled reboot took 87 percent less time and half the steps with iDRAC9 vs. Vendor K BMC. When you extrapolate these savings to large deployments, the admin time savings grow. For example, in a 100-server deployment, admins could save over 6 hours changing BIOS configuration items.

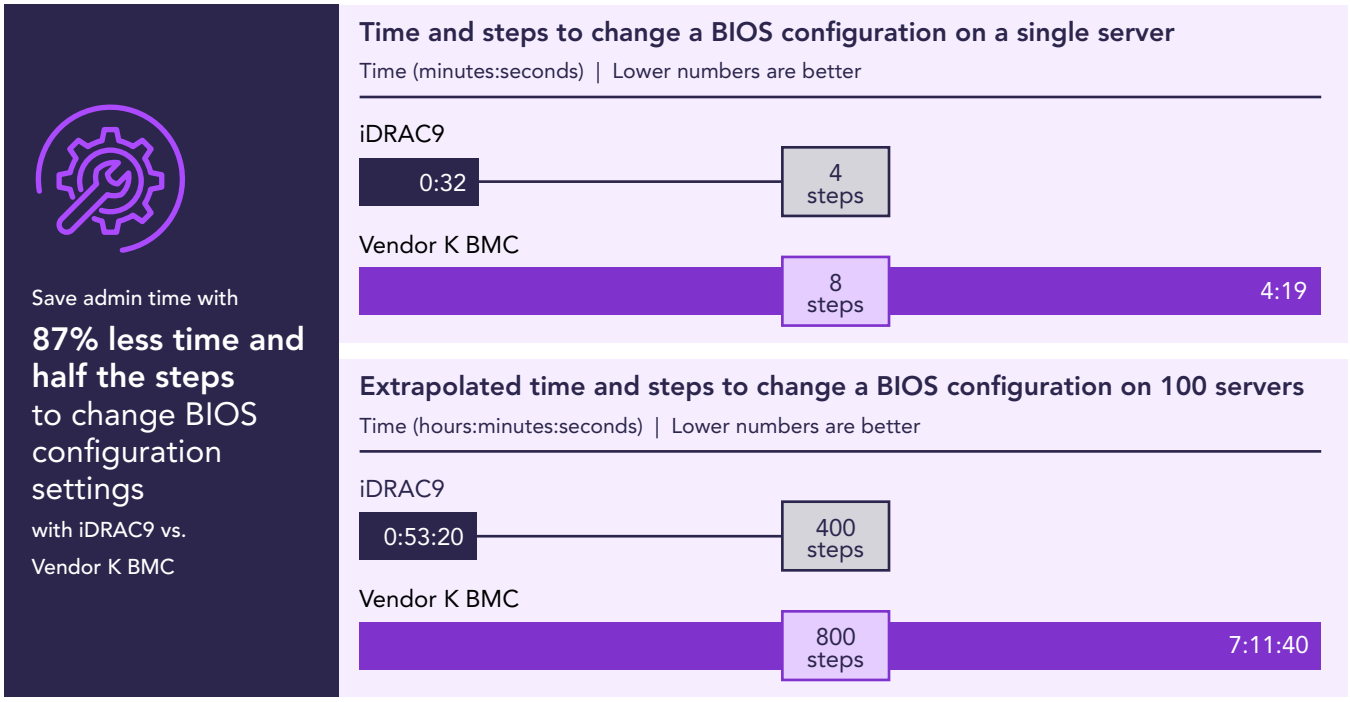

Figure 5: Time to change BIOS configuration settings and stage the update for a later reboot for a single server and extrapolated time for 100 servers. Less time and fewer steps are better. Source: Principled Technologies.

Setting up alert-based actions

Admins can make better use of their time when they aren't tied to a desk, monitoring environment health. As Figure 6 shows, OME provides 12 policy-driven options for alert-based actions so issue mitigation automatically starts whenever the environment reaches certain thresholds. In contrast, Vendor K's enterprise management console allows admins to configure only four alert-based events.

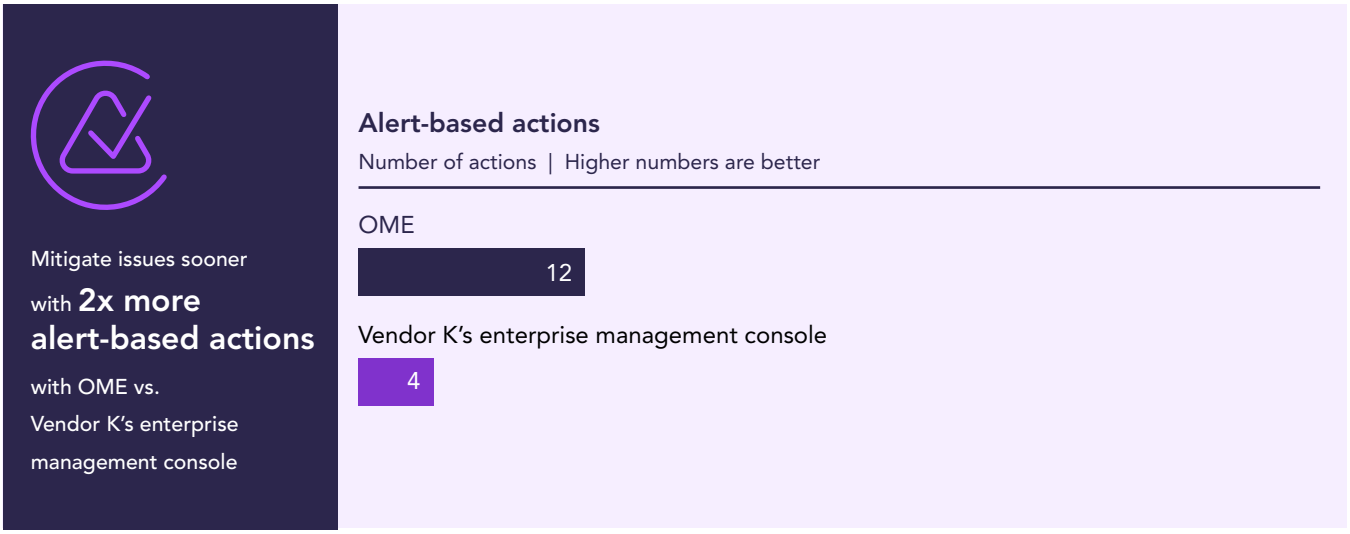

Figure 6: Comparison of the alert-based action each management tool offers. More actions are better. Source: Principled Technologies.

About Dell Technologies OpenManage Enterprise

OME is a one-to-many systems management console for the data center. The console offers a modern HTML5 graphical user interface and deploys as a virtual appliance for VMware ESXi™, Microsoft Hyper-V, and Kernel-based Virtual Machine (KVM) environments. OME can discover and inventory on IPV4 and IPV6 networks for up to 8,000 devices, including Dell rack servers, Dell tower servers, and Dell blades and chassis.[6] In a recent PT study, we found that a Dell environment with OME and OpenManage Enterprise Modular (OME-M) can save time making changes to VLANs and help avoid interventions during scheduled firmware updates.[7]

Learn more about OME at https://www.dell.com/en-us/lp/dt/open-manage-enterprise.

Cloud-based management with APEX AIOps Infrastructure Observability (formerly CloudIQ)

Embedded tools and enterprise management consoles aren't the only tools in the Dell server management portfolio. With APEX AIOps Infrastructure Observability (formerly CloudIQ), administrators gain another easy-to-use, automated way to keep their infrastructure's health and security in check—this time from the cloud.

Additional security features available in APEX AIOps Infrastructure Observability (formerly CloudIQ)

APEX AIOps Infrastructure Observability (formerly CloudIQ) offers several security features that can further strengthen your organization against attacks. Table 5 highlights some of these key security features.

Table 5: Overview of key security features available in APEX AIOps Infrastructure Observability (formerly CloudIQ). Source: Principled Technologies.

Feature	How APEX AIOps Infrastructure Observability (formerly CloudIQ) works to secure your environment
Cyber-security risk level alerts	Provides automated insights for cybersecurity with **specific security risk level alerts** so admins can react faster and address problems quickly to keep data secure
Policy-based security configuration	Offers **policy-based security configuration settings and easy-to-apply templates** that allow an administrator to ensure security best practice settings are in place, protecting the PowerEdge environment
Cyber-security advisories	Provides **relevant security advisory reporting**, offering specific vulnerability details and suggestions for remediation, which allows for quick action to close any security gaps

About APEX AIOps Infrastructure Observability (formerly CloudIQ)

APEX AIOps Infrastructure Observability (formerly CloudIQ) is a cloud-based AIOps tool offering "proactive monitoring, machine learning and predictive analytics" for a large number of Dell products and services, including servers, storage, data protection appliances, and hyperconverged infrastructure.[8] In a 2022 Principled Technologies study, we found that CloudIQ had negligible impact on network bandwidth while allowing us to monitor telemetry, health status, alerts, and inventory from a single console.[9]

Learn more about APEX AIOps Infrastructure Observability (formerly CloudIQ) at https://www.dell.com/en-us/dt/apex/aiops.htm.

Additional sustainability and efficiency features available in APEX AIOps Infrastructure Observability (formerly CloudIQ)

APEX AIOps Infrastructure Observability (formerly CloudIQ) also provides features that bolster sustainability and efficiency, and integrate with iDRAC9 and OME to make it easier for administrators to monitor the health of their PowerEdge environment. Table 6 highlights some of these features.

Table 6: Overview of sustainability and ease-of-use management features available in APEX AIOps Infrastructure Observability (formerly CloudIQ). Source: Principled Technologies.

Feature	Key benefits with APEX AIOps Infrastructure Observability (formerly CloudIQ)
Carbon footprint analysis	Located in the Monitoring section, this tool gives a higher view of and **can forecast carbon emissions** across environments
Performance views	Provides performance views and anomaly and utilization charts to **alert administrators at the first sign of problems**
Custom compliance reports	Provides users the ability to **create custom compliance reports** for selected devices
Customizable performance and inventory reports	Provides **custom reporting options** for server performance and inventory data, giving administrators more control over the performance and device metrics they're interested in tracking
Scheduling power action jobs	Perform power actions such as power capping on multiple monitored Dell PowerEdge servers in **only 35 seconds and 6 steps**
Scheduling firmware updates	Schedule PowerEdge firmware updates for multiple monitored servers in **just 41 seconds and 9 steps**

Conclusion

In our comparison of security, sustainability, and management/monitoring features, we found that the Dell server management tools portfolio provided more robust management and monitoring features than the Vendor K portfolio. In the realm of security, iDRAC9 offered more features, including dynamic system lockdown and multifactor authentication, which Vendor K didn't offer at all. Plus, iDRAC9 significantly reduced the time to disable USB ports to reduce data vulnerability.

With carbon footprint analysis and robust power management tools, we found that OME could better help organizations plan to meet sustainability goals than using Vendor K's enterprise management console. Additionally, we found that the Dell server management portfolio provided more automation and more remote management options, reducing administrator time and effort for certain routine monitoring and maintenance tasks. These wins in security, sustainability, and management/monitoring features make the Dell server management portfolio an attractive option for organizations seeking a more efficient, secure data center.

---

1. Harvard Business Review, "The Devastating Business Impacts of a Cyber Breach," accessed April 10, 2024, https://hbr.org/2023/05/the-devastating-business-impacts-of-a-cyber-breach.
2. Dell, "Integrated Dell Remote Access Controller (iDRAC)," accessed May 17, 2024, https://www.dell.com/en-us/lp/dt/open-manage-idrac.
3. Note: Vendor K's USB port disablement is customizable, though this means admins have to select each port for disablement, instead of by group.
4. DOE, "DOE Announces $40 Million for More Efficient Cooling for Data Centers," accessed May 20, 2024, https://www.energy.gov/articles/doe-announces-40-million-more-efficient-cooling-data-centers.
5. Dell, "OpenManage Enterprise Support Matrix," accessed May 21, 2024, https://www.dell.com/support/kbdoc/en-us/article/lkbprint?ArticleNumber=000217909&AccessLevel=10&Lang=en.
6. Dell, "OpenManage Enterprise," accessed May 17, 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," accessed May 17, 2024, https://www.principledtechnologies.com/Dell/PowerEdge-MX-OME-OME-M-0124.pdf.
8. Dell, "APEX AIOps: Tame IT complexity in your digital business," accessed June 11, 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," accessed April 9, 2024, https://www.principledtechnologies.com/dell/CloudIQ-network-0422.pdf.

Read the science behind this report at https://facts.pt/tZdME2D ►

Principled Technologies®

Facts matter.®

This project was commissioned by Dell Technologies.