



More security features

Initiate system **lockdown** remotely in just **18 seconds** with iDRAC9
 vs. *no system lockdown via Vendor K BMC*



Manage 8x

the number of devices with Dell OME
 vs. *Vendor K's enterprise management console*



Easier firmware updates

via automation and scheduling with iDRAC9
 vs. *Vendor K BMC*

Streamline administrator duties and gain more security and analytics features with tools from the Dell management portfolio

vs. comparable tools from Vendor K

Servers and the tools that administrators use to maintain and monitor them differ from vendor to vendor. By selecting servers that leverage a more robust management portfolio, you can give your admins time back daily by making common tasks, security, and analytics easier. In the Principled Technologies data center, we compared capabilities of the management portfolios from Dell and Vendor K to see what features they offered, and which could simplify administrator tasks. We compared:

Table 1: The management tools we tested.







	Dell	Vendor K
Embedded/remote server management	iDRAC9 (Integrated Dell Remote Access Controller)	Vendor K BMC
One-to-many device and console management	OpenManage Enterprise (OME)	Vendor K's enterprise management console

For the features and tools that we compared, we found that the Dell management portfolio would streamline administrator tasks compared to comparable Vendor K tools. The Dell tools we assessed offered more features that simplify management; including automatic updates and telemetry streaming; more security features; and custom reporting for targeted analysis of infrastructure performance.

Give administrators more options for easier environment management

Table 2 provides an overview of some of the ways we found tools from the Dell management portfolio were easier to use than comparable tools from the Vendor K portfolio. (Note: We dive into these wins in more depth in the following pages.)

Table 2: Summary of our comparison between Dell and Vendor K management tools. Source: Principled Technologies.

	What's different with Dell management tools	How much better
 <p>Easier firmware updates iDRAC vs. Vendor K BMC</p>	<ul style="list-style-type: none"> Automated online updates with iDRAC9, with scheduling options 	<ul style="list-style-type: none"> Vendor K has no automatic update function available Admins must update manually
 <p>Easier server deployment iDRAC vs. Vendor K BMC OME vs. Vendor K's enterprise management console</p>	<ul style="list-style-type: none"> Portable profiles with iDRAC One-to-many profile deployment with OME 	<ul style="list-style-type: none"> Similar time for initial profile configuration, but Vendor K requires 13 steps and over 2 minutes for every server thereafter, while Dell imports/exports profiles
 <p>More alert-based actions OME vs. Vendor K's enterprise management console</p>	<ul style="list-style-type: none"> Set up alert policies in OME and execute more types of automated actions based on alerts 	<ul style="list-style-type: none"> 3x more alert-based actions available with OME
 <p>More security features iDRAC vs. Vendor K BMC</p>	<ul style="list-style-type: none"> iDRAC9 offers System Lockdown and multi-factor authentication (MFA) features 	<ul style="list-style-type: none"> Vendor K BMC has no system lockdown or MFA features
 <p>Easier to use security features iDRAC vs. Vendor K BMC</p>	<ul style="list-style-type: none"> Fewer steps, less time, and no reboots using iDRAC for dynamic enabling/disabling of server USB ports 	<ul style="list-style-type: none"> Save administrators 4 minutes 13 seconds for dynamic USB, with no system downtime
 <p>Greater options for reporting and analytics OME vs. Vendor K's enterprise management console</p>	<ul style="list-style-type: none"> OME streams telemetry data to the cloud and offers customized reports Note: iDRAC9 also has the native ability for telemetry streaming 	<ul style="list-style-type: none"> Vendor K's enterprise management console has no telemetry streaming and no reporting mechanism

Features that simplify management

REMOTE MANAGEMENT

We assessed the BIOS features that the solutions offer to make remote management easier (see Figure 1). iDRAC9 offers 26 times as many BIOS configuration features as the Vendor K BMC (52 features vs. just 2 features), which gives administrators more granular control.

EASIER SERVER DEPLOYMENT

Dell iDRAC and OME offer features that make configuring new servers easier for administrators. As Figure 2 shows, it took similar time and steps to export and import a complete Dell server profile with iDRAC9 compared to a backup/restore of the Vendor K baseboard management controller (BMC) only with the Vendor K server.

With iDRAC9, after the initial 12 steps and 2m 22s to configure a profile, admins can port those complete templates to other servers. Conversely, when we tried to restore the Vendor K BMC profile from one server onto another server, we lost communication with the restored server, which means the profiles are not portable across servers. This means that Vendor K admins would need to complete these steps and take over two minutes for each server they wish to deploy, while admins managing Dell servers can complete this configuration task a single time.

Admins can import and export a complete server profile via iDRAC alone—a profile that includes all BIOS settings, drive configurations, power policies, and more. The Vendor K BMC doesn't have this feature natively (it requires the addition of the Vendor K enterprise management application to provide similar function) and ports only the base BMC configuration settings, requiring additional administrator effort for each new server.

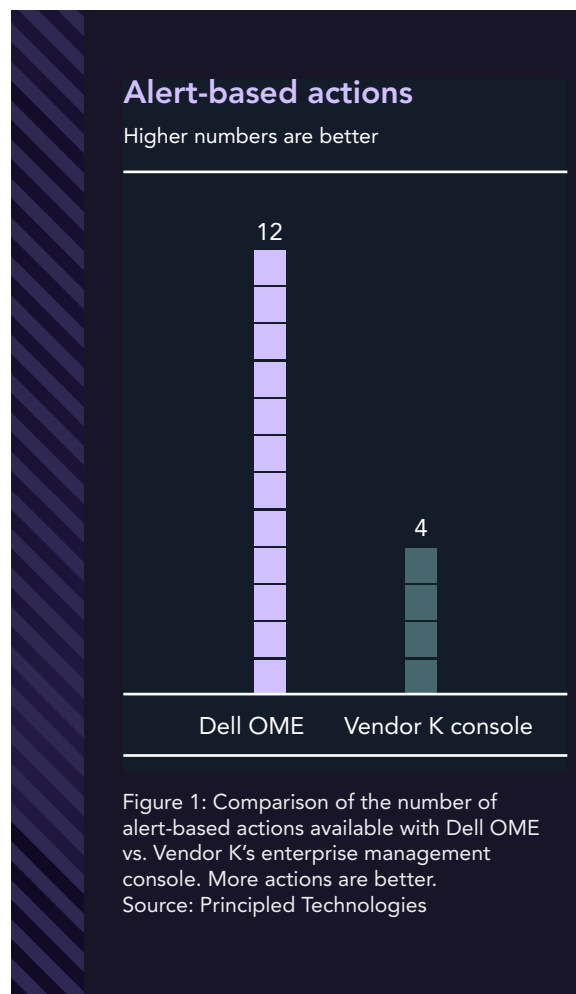
EASIER FIRMWARE UPDATES

Ensuring firmware is up to date is a vital task to help keep production servers secure and operating efficiently, but tracking and implementing these updates can be a hassle for administrators. iDRAC9 provides automatic updates and the ability to schedule firmware updates as desired, but we found nothing relating to automatic updating in Vendor K BMC. While multiple other manual methods exist for updating firmware (including from a direct file or updating from a repository), we were unable to find a way to perform even a check without administrator intervention on the Vendor K solution. By providing automatic firmware checks and updates, iDRAC removes this burden from the administrator task list.

MORE ALERT-BASED ACTIONS

We found that Dell OpenManage Enterprise offered more options for monitoring infrastructure. While both Dell OME and Vendor K's enterprise management console enable users to set up alert policies once and then automatically assign them for future alerts, OME offers 12 automated alert-based actions, while Vendor K's enterprise management console offers four event-based actions (see Figure 3).

By offering more alert-based actions, Dell OME gives administrators more choices in how they monitor their environment, depending on what is of concern to them.



Security features

We found that through iDRAC, the Dell management portfolio offers more built-in security features than Vendor K BMC. Some key security features we investigated include:

- **Dynamic System Lockdown:** System Lockdown helps prevent unintended or malicious activity from changing settings or accessing data on the server. (Note: This feature is available with iDRAC9 Enterprise or 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 set up these capabilities once, and then deploy as needed without configuration changes. Until the admin provides access, no one can plug in a zip drive or keyboard to modify any configuration settings of the system/OS/BIOS.

Table 3: Comparison of built-in security features that the management tools offer. Source: Principled Technologies.

	Dell	Vendor K
Dynamic system lockdown	✓	✗
MFA	✓	✗
Dynamic USB	✓	✓*

*Requires system downtime

Dell offers an easy method to prevent configuration from iDRAC: We found that administrators could lock down a system remotely in just three steps and 18 seconds. In contrast, we were unable to locate any system lockdown mode within the UEFI setup of the Vendor K server we tested.

The second security feature we looked for, MFA, was also not available using Vendor K BMC. We found that through iDRAC, setting MFA through SecurID was straightforward, taking just 7 steps to configure. In contrast, we found no MFA features under the User Security section within the Vendor K UEFI setup, nor within the Vendor K BMC configuration security or user/LADP settings. By providing a simple path to MFA, Dell management tools offer another layer of protection from bad actors to help keep data secure.

Dell iDRAC allows administrators to disable front side USB ports with no system downtime in only four steps and 37 seconds (see Figure 3). Vendor K BMC requires a system reboot and entering the BIOS configuration to achieve the same result in 14 steps and 290 seconds of admin time, including required system downtime while in the Vendor K BIOS configuration utility.

Time and steps to complete the Dynamic USB use case

Time (m:ss) | Lower numbers are better



Figure 2: Comparison of the time and steps it took to complete the Dynamic USB use case with iDRAC9 vs. Vendor K BMC. Less time and fewer steps are better. Source: Principled Technologies.

About iDRAC9

Dell PowerEdge servers include the Integrated Dell Remote Access Controller 9 (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:

- **Increased server availability** due to early notification of issues that can prevent downtime or reduce recovery time
- **Environment security** via secure remote access capabilities
- **Ease of administration** through simplified deployment and serviceability¹

To learn more about the features iDRAC9 provides, visit www.dell.com/support/iDRAC.

Analytics and reporting features

In our comparison of analytics and reporting, we found that OME provided more options to gain insight into infrastructure health compared to Vendor K's enterprise management console. OME offers a custom report builder that admins can use to granularly select the most important data for their purposes, while Vendor K's enterprise management console has no reporting mechanism. Dell iDRAC9 provides detailed real-time analytics data from individual servers into Dell OME, and OME allows admins to send telemetry data directly to CloudIQ for PowerEdge. (Note: This feature is available with iDRAC9 Enterprise or Datacenter licenses.) We were unable to locate automatic telemetry streaming in the Vendor K tools we tested.

Table 4: Comparison of telemetry streaming options that the management tools offer. Vendor K tools offer no telemetry capabilities for analytics. Source: Principled Technologies.

Does the tool have telemetry streaming?	Dell	Vendor K
Embedded server management <i>iDRAC9 v Vendor K BMC</i>	✓	✗
Console management <i>Dell OME vs. Vendor K's enterprise console management</i>	✓	✗

Table 5 compares some of the key features and options available in Dell OME and Vendor K's enterprise management console. Notably, Dell OME makes admins' tasks easier by giving them more monitoring options, such as third-party device monitoring, reporting options, and streaming telemetry data for granular monitoring.

Table 5: Comparison of analytics and reporting features in Dell OME and Vendor K's enterprise management console. Source: Principled Technologies.

	Dell OME	Vendor K's enterprise management console
Scalability	Manage up to 8,000 devices ²	Manage up to 1,000 devices ³
Third-party device monitoring	OME allows users to monitor third party devices using server IPs and credentials. This allows heterogenous device monitoring in the environment without switching consoles	Vendor K's enterprise management console does not support third-party devices
Third-party device monitoring with management information base (MIB import)	OME supports the importing of third party created MIBs for SNMP monitoring	No functionality within Vendor K's enterprise management console
Carbon emission analysis	Collect, calculate, store, and report on a customer's carbon footprint by utilizing default or customer defined variables that calculate carbon emissions based on power usage	No carbon emission analysis in Vendor K's enterprise management console
Plugin based architecture	Dell OME utilizes plugins to increase the functionality of the base level OME. Using the Update Management plugin, create custom repositories and use automatic online synchronization for firmware updates ⁴	No enhancement through plugins
Reporting options	OME offers built-in reports with the ability to build customized reports	Vendor K's enterprise management console has no reporting mechanism . Admins can export alerts, logs, and activities to CSV only, and can save historical metrics only as an image
Streaming telemetry data	OME automatically streams environment performance data to CloudIQ for PowerEdge for easy viewing, if CIQ plugin is installed and enabled	No automatic telemetry streaming in Vendor K's enterprise management console

About Dell OpenManage Enterprise

For more advanced one-to-many server administration features, Dell offers OpenManage Enterprise. OpenManage Enterprise simplifies IT management by unifying servers for management from a single console and automating tasks to increase efficiency. According to the OpenManage solution brief, administrators can use it to manage up to 8,000 devices (regardless of form factor), manage the entire configuration lifecycle through editable templates, and streamline remote management through batch scheduling.⁵

To learn more about the features OpenManage Enterprise offers, visit <https://www.dell.com/en-us/dt/solutions/openmanage/enterprise.htm#scroll=off>.

Conclusion

In our comparison of tools in the Dell and Vendor K management portfolios, we found that Integrated Dell Remote Access Controller 9 (iDRAC9) and Dell OpenManage Enterprise was easier to use and offered more security and analytics/reporting features to ease server management hassles for administrators. By reducing hands-on admin time and automating more tasks, organizations can watch the productivity of their IT staff climb, giving them more time to commit to bigger projects. Plus, additional security features offer more layers of protection for critical data, while expanded reporting/analytics features provide Dell OME users with better ways to gain insights about application performance.

1. Dell, "Integrated Dell Remote Access Controller 9 User's Guide," accessed January 6, 2023, https://www.dell.com/support/manuals/en-us/idrac9-lifecycle-controller-v6.x-series/idrac9_6.xx_ug/overview-of-idrac?guid=guid-a03c2558-4f39-40c8-88b8-38835d0e9003&lang=en-us.
2. Dell, "Dell EMC OpenManage Enterprise 3.9 Support Matrix," accessed November 15, 2022, <https://dl.dell.com/content/manual57108123-dell-emc-openmanageenterprise-3-9-support-matrix.pdf?language=en-us&ps=true>.
3. Vendor K enterprise management console documentation.
4. Dell, "Dell EMC OpenManage Enterprise 3.9 User's Guide," accessed November 15, 2022, <https://dl.dell.com/content/manual56903993-dell-emc-openmanage-enterprise-3-9-user-s-guide.pdf?language=en-us&ps=true>.
5. Dell, "OpenManage Enterprise Solution Brief," accessed November 14, 2022, https://www.dell.com/en-us/dt/solutions/openmanage/enterprise.htm#pdf-overlay=//www.delltechnologies.com/asset/en-us/products/servers/briefs-summaries/dell_emc_openmanage_enterprise_solution_brief.pdf.

Read the science behind this report at <https://facts.pt/RAai25A> ►

This project was
commissioned by
Dell Technologies.



Facts matter.®

Principled Technologies is a registered trademark of Principled Technologies, Inc. All other product names are the trademarks of their respective owners. For additional information, review the science behind this report.