



Secure, Automate, and Monitor Server Environments at Scale

This report compares Dell Technologies and Vendor K server management tools and shows which tools deliver superior data center security, ease of use, analytics, and sustainability.

Executive Summary

Effective server management tools help IT teams control growing data center complexity by applying safeguards and resolving issues efficiently at scale. As organizations manage more servers and increasingly complex workloads, these tools can reduce the operational risk associated with downtime, security gaps, and inconsistent administration.

In this report, Prowess Consulting compares server management tools from Dell and an enterprise competitor, referred to as Vendor K, across four focus areas: **security, ease of use, analytics, and sustainability**. Table 1 shows the tools we evaluated and the main feature each tool provides.

Across the four areas examined, we found that **Dell server management tools offered broader feature coverage and more efficient workflows** than the Vendor K tools we tested. Dell provided stronger configuration and access controls while reducing administrative effort through automation and centralized management. Dell tools also delivered greater visibility into server activity and broader power management and carbon emissions analysis. These advantages can reduce operational overhead and help organizations maintain consistent control as infrastructure scales. To evaluate how the differences between these tools impact larger environments, this report scales key test results to a 100-server data center.

Highlights

Our analysis shows that, compared with Vendor K offerings, Dell server management tools provide:



System Lockdown mode to protect server configurations from unauthorized changes
(with iDRAC10 vs. the Vendor K BMC, which offers no equivalent feature)

And provide up to:

13.8x

as many directly accessible BIOS settings without a reboot to improve operational efficiency
(with iDRAC10 vs. the Vendor K BMC)

2.5x

as many telemetry modules for expanded server visibility
(with iDRAC10 vs. the Vendor K BMC)

4.6x

as many built-in power management reports to simplify energy monitoring and analysis
(with OME vs. the Vendor K enterprise management console)

Table 1 | Summary of Dell and Vendor K server management tools (see [Appendix A: Glossary](#) for more information)

Feature	Dell Technologies	Vendor K
Embedded/remote server management	Integrated Dell™ Remote Access Controller 10 (iDRAC10)	Vendor K baseboard management controller (BMC)
One-to-many device management console	Dell OpenManage™ Enterprise (OME)	Vendor K enterprise management console
Cloud-based monitoring	Dell Artificial Intelligence for IT Operations (AIOps)	Vendor K cloud management platform

Evaluating Server Management Features and Capabilities

For this report, we evaluated features within the Dell and Vendor K server management tools that influence day-to-day operational efficiency, configuration integrity, energy consumption, and long-term security. Together, these factors help determine an organization's total cost of ownership (TCO) and return on investment (ROI), forming the true business value of the organization's IT infrastructure.

We tested the real-world effort needed to complete common administrator tasks on Dell and Vendor K server management platforms. For each task, we ran live workflows and measured steps and time to completion. These workflow measurements matter because manual administrative tasks become harder to scale as server counts grow and can increase the risk of configuration inconsistencies across environments. We then extrapolated our results to a 100-server environment to show how small per-task differences can add up to significant additional effort. For a full description of the steps taken for our comparisons, refer to the [Methodology](#) document.

Security Features: Protecting Configurations and Controlling Access

Security in server environments requires maintaining configuration integrity and limiting administrative access to authorized users. We tested OME, iDRAC10, and AIOps from Dell and the BMC, enterprise management console, and cloud management platform from Vendor K. Our testing focused on features that help administrators prevent unauthorized changes, manage privileged credentials, and restrict access to specific groups of systems. The results showed that, in comparison with Vendor K tools, Dell system management tools iDRAC10 and OME provide controls that can help organizations enforce these policies more consistently across large data centers. A full comparison of security features is in the [Methodology](#) document.

System Lockdown

Inconsistent configuration across servers can expose systems to unintended changes after deployment. iDRAC10 includes System Lockdown mode, which blocks configuration changes and firmware updates after a server has been configured. Administrators can enable this feature directly from the iDRAC10 dashboard. Any attempt to change protected settings while the system is locked returns an error. This mode gives administrators a direct way to maintain a known configuration and reduce the risk of unauthorized changes. The Vendor K BMC does not provide a comparable system lockdown feature through its management interface or BIOS.



Protect configurations from unauthorized changes with **System Lockdown mode** in iDRAC10, a safeguard that the Vendor K BMC does not offer

Access Control

Administrators need precise control over which systems each user can access, especially as users and systems scale. OME supports both scope-based access control (SBAC) and role-based access control (RBAC). SBAC brings precise, server group-specific permissions that reduce security risk beyond role alone. Administrators can assign the same role to multiple users while limiting each user's access to the systems within their assigned scope.

The Vendor K enterprise management console is limited to only RBAC, which defines what a role can do, but which cannot natively restrict those permissions to particular device groups. As a result, administrators must either grant broader access than necessary or create additional roles to approximate scope-level separation, adding complexity and overhead.

Cybersecurity Advisories

Administrators need enough context to determine which vulnerable systems require attention first. Both AIOps and the Vendor K cloud management platform show vulnerabilities and affected systems. Vendor K bases vulnerability status on the highest-severity finding and provides counts by severity. AIOps goes further by calculating a system risk score using the impact of cybersecurity issues, evaluation-plan results, Dell Security Advisories, and detected ransomware. This broader assessment can help administrators prioritize remediation across the environment.

Policy-Based Security Configuration

As server environments scale, administrators need a consistent way to identify configuration differences and determine which ones pose the greatest security risk. AIOps compares system configurations with customizable security evaluation plans, assigns each system a risk level, and allows administrators to resolve supported misconfigurations from the security view. The Vendor K cloud management platform can identify drift from a configuration learned from a reference system, but administrators cannot directly author or edit that reference configuration, and the platform does not assign a security classification or risk score to detected differences. These AIOps capabilities can help organizations prioritize remediation and apply security policies consistently across growing environments.

Table 2 | Comparison of security features between Dell and Vendor K server management tools

Security Feature	Dell	Vendor K	Business Impact Summary
System Lockdown	Supported	Not supported	System Lockdown can help organizations maintain configuration integrity after deployment. By blocking unauthorized configuration changes and firmware updates, iDRAC10 can reduce the risk of system drift that could expose servers to security issues or operational instability. Vendor K has no comparable feature in its BMC and BIOS settings.
Access Control	Supported	Limited	OME supports both SBAC and RBAC, which provide precise, server group-specific permissions, reducing security risks. The broader Vendor K RBAC-only model can increase the risk of granting users unnecessary access as environments scale.
Cybersecurity Advisories	Supported	Limited	AIOps consolidates Dell security advisories and shows each advisory's impact and affected component. Connecting advisories to affected systems can help teams prioritize remediation sooner and reduce the time that critical vulnerabilities remain unaddressed. The Vendor K cloud management platform also reports vulnerabilities and affected systems, while AIOps takes the analysis further by incorporating advisory data into a broader system risk score.
Policy-Based Security Configuration	Supported	Limited	AIOps helps reduce manual security checks and shorten remediation time through configurable evaluation plans, whereas the Vendor K cloud management platform provides limited configuration-drift monitoring capabilities. Applying consistent security criteria across systems can also reduce exposure to security gaps as infrastructure scales.

Ease of Use Features: Reducing Administrative Effort at Scale

Managing large server environments requires tools that reduce manual effort and simplify routine administration. Features such as automation, centralized management, and reusable configurations can help administrators complete common tasks quickly and consistently. The following sections compare ease of use features that affect operational efficiency across server environments.

Full-System BIOS Configuration

BIOS configuration is a routine administrative task that can become time-consuming when repeated across many servers. Management tools that provide direct access to BIOS settings can reduce effort and help administrators apply changes efficiently.

We found that iDRAC10 provided direct access to 111 BIOS settings without a reboot, up to 13.8x as many as the 8 accessible through the Vendor K BMC. This broader access allows administrators to stage more changes through the iDRAC10 interface, while many changes on the Vendor K system require booting into the BIOS, which takes time, causes downtime, and can introduce additional risk. In our testing, staging a BIOS change took 17 seconds on a Dell server and 146 seconds on a Vendor K system. Across 100 servers, that scales to less than 30 minutes for Dell and more than 4 hours for Vendor K, saving up to 3.5 hours with iDRAC10.



Access up to **13.8x more BIOS settings** and save up to **3.5 hours staging a BIOS change** (without reboot) with iDRAC10 vs. the Vendor K BMC

Automatic Firmware Updates

Keeping firmware current across a large server environment can require significant administrative effort. iDRAC10 lets administrators schedule automatic firmware updates for a specific time and day, helping maintain firmware consistency with less manual effort. The Vendor K BMC has no equivalent scheduling capability, so administrators must initiate firmware updates manually.

Import/Export Full Server Configuration Profile

Reusing server configuration profiles can reduce repetitive work during deployment. iDRAC10 lets administrators export and import a full server configuration profile that includes BMC, network interface controller (NIC), RAID, and BIOS settings. Administrators can save the profile locally or to a remote destination and apply it to multiple servers, supporting faster, consistent deployments. The Vendor K BMC supports exporting and importing BMC settings only, requiring administrators to configure the remaining server components separately.

Alert-Based Automated Actions

Manually reviewing and responding to every infrastructure alert can increase the risk of delayed action on critical issues. OME allows administrators to associate predefined actions with specific infrastructure events, enabling the platform to respond automatically when those conditions occur. Administrators can configure these policies once and apply them across groups of servers, including the execution of predefined actions or custom scripts. Our testing showed how this difference can reduce administrative time and effort. Once configured, automated actions allow OME to execute predefined responses without requiring administrators to review and act on each event individually. The Vendor K enterprise management console also supports alerts, but within the platform we tested, administrators must review those alerts and perform the necessary actions manually. Including the initial alert setup, OME resolved 100 alerts in 11 steps and 32 seconds, compared to 703 steps and 1,604 seconds (26.73 minutes) with the Vendor K enterprise management console, requiring up to 98% fewer steps and less time.



Complete alert-based actions with OME with up to a **98% reduction in both time and required steps** compared with the Vendor K management console

Heterogeneous Server Monitoring

Mixed-vendor environments can require administrators switch between management consoles to monitor server health. OME gives administrators a consolidated view of Dell servers and supported third-party servers, including Vendor K servers. The Vendor K enterprise management console documentation identifies support for Vendor K servers and storage, with no defined support for monitoring third-party servers. OME can therefore reduce console switching and simplify health monitoring in mixed-vendor environments.

Report Builder with Customization

Manually gathering and organizing server-management data can consume administrative time and make operational reporting harder to standardize. OME addresses this challenge with 52 built-in reports covering system inventory, performance, and operational status, along with a report builder for creating custom reports. Administrators can run reports on demand or schedule them for automatic distribution. This combination of predefined and customizable reporting provides flexible access to management data from a single platform. The Vendor K enterprise management console provides 6 built-in reports and does not support custom report creation.



Access more than **8x as many built-in reports plus custom report creation** with OME vs. the Vendor K enterprise management console

Management Scalability

Management platforms must accommodate expanding server environments without requiring additional instances. A single OME instance can manage up to 8,000 servers, compared to 4,000 with the Vendor K enterprise management console, or up to 2x as many on-premises devices. That additional capacity can help organizations scale server management without deploying additional management instances.



Manage up to **2x as many on-premises devices** with OME vs. the Vendor K enterprise management console

Connection View

Tracing physical network connections can require time-consuming manual checks when administrators lack visibility into the switch ports connected to each server interface. Both iDRAC10 and the Vendor K BMC support Link Layer Discovery Protocol (LLDP) for their dedicated management ports. iDRAC10 extends switch-port identification to supported server network cards, which can help administrators identify cabling errors remotely and reduce troubleshooting effort.

Multiple Performance Reports

Fragmented performance data can force administrators to compile reports manually, which is time consuming, before they can identify trends or act on system issues. AIOps provides centralized, schedulable dashboards that administrators can customize using 75 server performance and inventory metrics. The Vendor K interface provides 6 performance-reporting metrics, and administrators must manually export tabular data from individual pages to save it. AIOps can therefore reduce manual reporting effort while providing broader, more flexible access to performance data.

Table 3 | Comparison of ease of use features between Dell and Vendor K server management tools

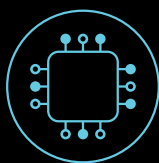
Ease of Use Feature	Dell	Vendor K	Business Impact Summary
Full-System BIOS Configuration	Supported	Limited	iDRAC10 provides direct access to 111 BIOS settings without a reboot, up to 13.8x as many as the 8 accessible through the Vendor K BMC. This broader access can reduce reboot-related downtime and save up to 3.5 hours when the tested workflow is scaled across 100 servers.
Automatic Firmware Updates	Supported	Not supported	iDRAC10 lets administrators schedule firmware updates for a specific time and day. The Vendor K BMC requires an administrator to initiate each update manually, so scheduled updates with iDRAC10 can reduce repeated work.
Import/Export Full Server Configuration Profile	Supported	Limited	iDRAC10 supports profiles that include the full server configuration, including BMC, NIC, RAID, and BIOS settings. The Vendor K BMC supports importing and exporting of BMC settings only, requiring administrators to configure the remaining server components separately. Reusing a full server profile can reduce repetitive configuration work.
Alert-Based Automated Actions	Supported	Not supported	OME can apply predefined actions automatically after an alert policy is configured. Across 100 alerts, OME would enable up to a 98% reduction in both time and required steps compared with Vendor K.
Heterogeneous Server Monitoring	Supported	Not supported	OME supports monitoring Dell and supported third-party servers from a single console. Vendor K enterprise management console documentation identifies support for Vendor K servers and storage, with no defined support for monitoring third-party servers. OME can therefore reduce console switching and simplify health monitoring in mixed-vendor environments.
Third-Party Integration Support	Supported	Not supported	OME supports multiple third-party management plug-ins for platforms such as VMware vCenter® and Microsoft® management tools, whereas the Vendor K enterprise management console does not provide comparable third-party management plug-in support. These capabilities can help organizations integrate server management into existing operational workflows and reduce fragmented administration.
Report Builder with Customization	Supported	Limited	OME provides 52 built-in reports and custom report creation, compared with 6 built-in reports and no custom report builder for Vendor K. These capabilities can reduce manual data collection and support consistent operational reporting.
Management Scalability	Supported	Limited	A single OME instance can manage up to 8,000 servers, compared with 4,000 with the Vendor K enterprise management console, or up to 2x as many on-premises devices. This additional capacity can help organizations scale without deploying more management instances.
Connection View	Supported	Limited	Both iDRAC10 and the Vendor K BMC provide LLDP information for their dedicated management ports. iDRAC10 also provides switch-port identification for supported server network cards. This broader visibility can help administrators identify cabling issues remotely and reduce troubleshooting effort.
Multiple Performance Reports	Supported	Limited	AIOps provides centralized, schedulable performance reporting with customizable report options, whereas Vendor K relies on manual exports from individual interface pages. These capabilities can reduce reporting effort and help administrators access operational data efficiently.

Analytics Features: Improving Visibility and Insight

Administrators need centralized visibility to maintain performance and control across complex server environments. Our testing examined the depth and accessibility of analytics features available through iDRAC10 and AIOps compared with the Vendor K BMC and cloud management platform. The results showed differences in telemetry access and the range of system data available to administrators.

Telemetry Streaming

Limited telemetry coverage and complex data-collection workflows can make it harder to monitor systems and analyze trends across server environments. In testing, both iDRAC10 and the Vendor K BMC supported telemetry streaming to external analytics platforms. The Vendor K BMC supported 14 telemetry modules, while iDRAC10 automated telemetry streaming through a built-in configuration workflow and supported 36 telemetry modules, or up to 2.5x as many. This data can help administrators for current-state monitoring and historical trend analysis.



Access up to **2.5x the telemetry modules** in iDRAC10 vs. the Vendor K BMC

Performance Metrics with Anomaly Detection

Administrators need efficient ways to identify abnormal system behavior and emerging capacity constraints before they affect operations. Centralized performance monitoring with anomaly detection can help administrators identify unusual system behavior without manually reviewing data across individual servers. AIOps and the Vendor K cloud management platform both provide anomaly detection and predictive analytics, but they apply them differently.

AIOps highlights performance anomalies in metric charts and provides forecasting for CPU, memory, system, and input/output (I/O) utilization. These capabilities can help administrators identify abnormal resource-consumption patterns and potential capacity constraints without reviewing performance data server-by-server.

The Vendor K cloud management platform provides usage-metric charts, but its anomaly and predictive analytics apply to component-failure prediction rather than resource-utilization trends.

GPU Utilization and Visibility

Administrators managing AI, machine learning (ML), and high-performance computing (HPC) workloads need visibility into how accelerator resources are performing and being used. AIOps provides GPU data while the Vendor K cloud management platform does not.

Together, iDRAC10 and AIOps can support workload planning by helping teams understand GPU behavior under load and identify underused resources. These insights can also support the management of AI, ML, and HPC workloads.

Table 4 | Comparison of analytics features between Dell and Vendor K server management tools

Analytics Feature	Dell	Vendor K	Business Impact Summary
Telemetry Streaming	Supported	Limited	Both iDRAC10 and the Vendor K BMC support telemetry streaming to external analytics platforms. iDRAC10 adds a built-in configuration workflow and supports up to 2.5x as many telemetry modules, providing broader data access for current-state monitoring and historical trend analysis.
Performance Metrics with Anomaly Detection	Supported	Limited	AIOps and the Vendor K cloud management platform both provide anomaly detection and predictive analytics for different purposes. AIOps highlights performance anomalies and forecasts CPU, memory, system, and I/O utilization, while Vendor K focuses on component-failure prediction. AIOps can help administrators identify abnormal resource-consumption patterns and potential capacity constraints.
GPU Utilization and Visibility	Supported	Limited	AIOps provides GPU utilization metrics and performance graphs for individual GPUs and groups of GPUs. The Vendor K cloud management platform provides basic GPU inventory but does not provide GPU utilization insights. This additional visibility can help teams understand GPU behavior under load and identify underused resources for workload planning.

Sustainability Features: Managing Power Consumption Across Large Server Environments

As server counts increase, administrators need visibility into where power is being consumed, which systems are operating inefficiently, and how energy use affects available capacity. Management tools that provide detailed power data, centralized reporting, automated power policies, and carbon-emissions analysis can help administrators identify inefficiencies and make more informed infrastructure-planning decisions.

We compared how Dell and Vendor K tools help administrators understand and control power consumption. The evaluation covered power data and carbon-emissions analysis, along with automated controls for power and thermal conditions. Our findings showed that OME and AIOps provide broader insight and greater control than the Vendor K enterprise management console and cloud management platform.

Power Management Reporting and Visibility

Administrators need clear visibility into power consumption to identify inefficiencies and plan infrastructure growth effectively. Centralized power-management reporting helps provide that visibility without requiring manual data collection across the environment. OME includes 28 built-in reports focused on energy consumption, capacity planning, and infrastructure efficiency, and it supports customizable reports. Administrators can generate these reports on demand or use them to support ongoing analysis of power usage trends across the data center without manually collecting and compiling data. Vendor K also provides power-management reporting through its enterprise management console, but with 6 built-in reports and no custom report creation. OME therefore provides up to 4.6x as many reports, including consumption, temperature, airflow, and utilization data at the device, component, and group levels.

Detailed power management reporting can help administrators reduce manual sustainability reporting effort, identify inefficient systems sooner, and make more informed capacity-planning decisions.



Access up to **4.6x as many power-usage reports** with OME vs. the Vendor K enterprise management console

Carbon Emissions and Footprint Analysis

Administrators need more than power-consumption data alone to understand the sustainability impact of their infrastructures. Carbon-emissions analysis can help translate energy usage into actionable insights for planning and reporting. OME calculates carbon emissions from measured energy use using a configurable conversion factor. AIOps provides summary, system, and workload-level metrics for carbon emissions and energy usage, including year-to-date usage and forward forecasts for both energy and emissions. These capabilities can help organizations evaluate the operational impact of energy consumption and support sustainability planning with measured data and forecasted trends. The Vendor K enterprise management console and cloud management platform do not provide carbon-emissions analysis or forecasting capabilities.

Automated Power and Thermal Management Policies

As server environments scale, organizations can benefit from consistent ways to respond to power and thermal events without requiring manual intervention for every system. Policy-based power management can help administrators enforce energy and cooling strategies consistently across large environments. OME supports static and temperature-triggered policies for individual devices or groups. It also includes Emergency Power Reduction (EPR), which can reduce power consumption when temperature thresholds are exceeded. These policy-based controls can help organizations respond to power or thermal events consistently across larger environments. The Vendor K enterprise management console does not provide comparable policy-based power-management capabilities.

Table 5 | Comparison of sustainability features between Dell and Vendor K server management tools

Sustainability Feature	Dell	Vendor K	Business Impact Summary
Power Management Reporting and Visibility	Supported	Limited	OME provides 28 built-in power-management reports and supports customizable report creation, compared with 6 built-in reports in the Vendor K enterprise management console. This broader reporting coverage and visibility into power-consumption data can reduce manual data collection, help administrators identify inefficient systems sooner, and support more informed capacity-planning decisions.
Carbon Emissions and Footprint Analysis	Supported	Not supported	OME calculates carbon emissions from measured energy use, while AIOps provides system, workload, and environment-level energy and emissions metrics, including historical usage and forecasted trends. The Vendor K enterprise management console and cloud management platform do not provide carbon-emissions analysis or forecasting capabilities. These features can help organizations evaluate the operational impact of energy consumption and support sustainability planning.
Automated Power and Thermal Management Policies	Supported	Not supported	OME supports static and temperature-triggered policies for individual devices or groups, including EPR. The Vendor K enterprise management console does not provide policy-based power-management controls. These capabilities can help organizations respond consistently to power and thermal events without requiring manual intervention for every system.

Business Value

Our testing found clear differences between Dell and Vendor K server management tools across security, ease of use, analytics, and sustainability. While both vendors support enterprise server management, Dell delivers more granular security controls, stronger automation, deeper telemetry, and broader sustainability reporting than the Vendor K tools we evaluated. Those differences can reduce administrative effort while giving IT teams greater visibility into system health, policy compliance, and energy use.

Across the four areas evaluated in this study, we found that Dell provides the following advantages:

- **Security:** Dell tools help organizations maintain configuration integrity and enforce security policies across large environments. iDRAC10 includes System Lockdown mode, which prevents configuration changes and firmware updates after deployment. The Vendor K BMC offers no equivalent capability. OME supports both RBAC and SBAC for granular access control, while AIOps adds centralized security visibility through cybersecurity advisories, configuration evaluation plans, and system risk scoring.
- **Ease of use:** Dell reduces routine administrative effort through automation and centralized management. iDRAC10 provides access to 111 BIOS settings without requiring a reboot and supports scheduled firmware updates, a capability unavailable in the Vendor K platform. In our testing, OME completed alert-driven actions with up to 98% fewer steps and less time than the Vendor K workflow. OME also supports up to 8,000 managed servers per instance, compared to 4,000 for the Vendor K management console.
- **Analytics:** Dell gives administrators deeper visibility into infrastructure performance and utilization. iDRAC10 supports 36 telemetry modules, compared to 14 in the Vendor K BMC. AIOps combines performance monitoring, anomaly detection, utilization forecasting, and GPU visibility within a single platform. The Vendor K cloud management platform provides less visibility into long-term utilization trends and GPU activity.
- **Sustainability:** Dell gives organizations more insight into energy consumption and environmental impact. OME includes 28 built-in power management reports, compared to 6 in the Vendor K management console. Administrators can create custom reports and apply policy-based power and thermal controls. AIOps extends visibility with workload-level energy analysis, carbon-emissions tracking, and forecasting.

In our testing, Dell's advantage was most apparent in automation and operational visibility. The Dell server management tools can automate more routine tasks, expose more infrastructure data, and deliver deeper insight into system performance, energy consumption, and sustainability metrics than the Vendor K counterparts. Those capabilities become increasingly valuable as server environments grow in size and complexity.

FAQ

1. Who should read this report?

This report is designed for server administrators, IT decision-makers (ITDMs), and business decision-makers (BDMs) involved in selecting server platforms and management solutions. It focuses on the factors that often drive platform selection, including cost, operational efficiency, and risk.

2. What is the primary goal of this report?

The goal is to compare the server management capabilities provided by Dell and Vendor K across security, ease of use, analytics, and sustainability. Through hands-on testing and feature analysis, Prowess Consulting examines how each platform supports common administrative tasks, infrastructure visibility, and operational efficiency, and how those differences can affect server management as environments scale.

3. Which tools does Prowess Consulting compare, and what is the scope of this report?

On the Dell side, we compare iDRAC10, OME, and AIOps server management tools. On the Vendor K side, we compare its BMC, enterprise management console, and cloud management platform. Our comparisons focus on validated features across security, ease of use, analytics, and sustainability, including capabilities that affect configuration management, administrative effort, infrastructure visibility, telemetry access, power management, and carbon-emissions analysis.

4. What testing methodology does Prowess Consulting use?

For this report, we use hands-on testing to measure the steps and time required to complete selected administrative tasks using Dell and Vendor K server management tools. We also review product documentation for the capabilities included in the comparison. Where appropriate, we extrapolate measured results from a single server to an environment of 100 servers. This approach shows how small differences in repeated workflows can affect administrative effort at scale.

5. What are the key findings of the comparison between Dell and Vendor K server management tools?

Across the areas tested, we found that Dell tools provide stronger security controls, reduce repeated administrative work, and expand visibility into server environments. In our testing, iDRAC10 provided features such as System Lockdown and direct access to more BIOS settings, and it supported scheduled firmware updates. OME automated actions based on alerts, supported more devices through a single management instance, and provided scope-based access control for granular administration. During our testing, the Dell tools also provided broader telemetry access, enhanced analytics capabilities, and more extensive power management and sustainability features than the Vendor K tools.

6. How do these findings benefit IT administrators and decision-makers?

For IT administrators, the findings show where management tools can reduce repeated work and provide more detailed system information. Features such as direct BIOS configuration and scheduled firmware updates can simplify routine administration. Alert-based automation can reduce manual response effort across large environments. For decision-makers, these features can support consistent operations and help limit the management overhead associated with infrastructure growth.

7. How does this report relate to AI, GPU workloads, and modern analytics needs?

Many organizations run GPU-intensive workloads for AI, ML, and HPC. iDRAC10 provides GPU-related metrics that can help administrators monitor accelerator activity and health at the server level. AI Ops extends this visibility with GPU utilization metrics for individual GPUs and groups of GPUs. Each Dell tool provides GPU-related data for monitoring accelerator activity and health, insights that can help teams identify underused accelerator resources and support workload planning.

Appendix A: Glossary

Alert-based automated actions are actions that a management platform triggers in response to specified alerts. OME can run predefined actions or custom scripts after an alert policy is configured. The Vendor K enterprise management console requires administrators to manually review alerts and perform any necessary actions.

Automatic telemetry streaming sends detailed server data to external analytics tools. iDRAC10 automates telemetry streaming through a built-in configuration workflow and supports 36 telemetry modules. The Vendor K BMC supports telemetry reporting with fewer reports and metrics.

Baseboard management controller (BMC) is the embedded controller that provides out-of-band management functionality for a server. iDRAC10 and the Vendor K BMC both provide embedded server management capabilities.

Dell Artificial Intelligence for IT Operations (AI Ops) is a cloud-based analytics and observability layer for Dell environments. It centralizes server data across multiple sites to help administrators identify issues and maintain visibility across distributed environments. AI Ops and the Vendor K cloud management platform both provide analytics capabilities, with AI Ops offering additional features such as anomaly detection and GPU utilization metrics.

Dell OpenManage Enterprise (OME) is the Dell one-to-many management console for Dell PowerEdge™ servers. It provides centralized configuration and reporting capabilities. OME also supports firmware management and integration with AI Ops and iDRAC10.

Firmware update scheduling is a feature in iDRAC10 that automates firmware updates on a set schedule. It reduces repetitive manual work and can help maintain consistent firmware levels across a server environment. The Vendor K BMC does not provide a scheduling feature.

GPU metrics are measurements that describe GPU activity (such as usage, memory usage, and power consumption) or condition, such as GPU board temperature. AI Ops provides GPU utilization metrics and performance graphs for individual GPUs and groups of GPUs. The Vendor K cloud management platform provides basic GPU inventory but does not provide GPU utilization insights.

Import/export server configuration profile is a feature in iDRAC10 that allows administrators to reuse a complete server configuration across multiple systems. The profile can include BIOS settings and other server components. The Vendor K BMC supports backup and restore of BMC settings only.

Integrated Dell Remote Access Controller 10 (iDRAC10) is Dell’s embedded management controller for PowerEdge servers. It provides remote access and configuration control without requiring an operating system (OS). It also provides security, telemetry, and automation capabilities.

Role-based access control (RBAC) is an access-control model that assigns permissions based on a user’s role. RBAC defines the actions that users can perform, helping organizations manage access consistently across systems and administrative functions.

Scope-based access control (SBAC) is an extension of role-based access control (RBAC) that limits a user’s access to specified device groups. OME supports SBAC and RBAC, whereas the Vendor K enterprise management console supports RBAC only.

System Lockdown is a security feature in iDRAC10 that blocks configuration changes and firmware updates after a server has been configured. The Vendor K BMC does not provide a comparable feature through its management interface or BIOS.

Appendix B: Test Configurations

Feature	Dell	Vendor K
Server Model	PowerEdge R770	Vendor K server
OS	None	None
CPU	2 x Intel® Xeon® 6767P	1 x Intel Xeon 6747P
Storage	2 x 447.13 GB NVM Express® (NVMe®); 6 x 1,489.88 GB NVMe	2 x 480 GB M.2 NVMe solid-state drive (SSD); 2 x 1.92 TB 2.5-inch NVMe SSD
Memory Size	2,048 GB	128 GB
Memory Configuration	32 x 64 GB at 5,200 MHz	4 x 32 GB at 6,400 MHz
NIC	Broadcom® Advanced Quad-Port 25 Gb Ethernet adapter	Broadcom 5719 1GbE RJ45 4-port OCP Ethernet Adapter
BMC Software Version	iDRAC10 v1.30.10.50	Vendor K BMC
BMC License	iDRAC10 Datacenter	Vendor K BMC premier license
Enterprise Management Software	OME v4.7	Vendor K enterprise management console
Enterprise Management License	OME Advanced+	Vendor K starter, per-endpoint license
Cloud Analytics Software	AIOps plug-in v2.7.0.12	Vendor K cloud management platform

