Bolster security with system lockdown in

95% less time & 83% fewer steps

with iDRAC9 vs. iLO 6

Optimize energy efficiency with

4x more power management metrics

and 25 customizable reports in OME vs. 0 reports in OneView

Enhance remote functionality with

16x more remote BIOS features

with 51 in iDRAC9 vs. 3 in iLO 6

Improve security, sustainability, and administrator efficiency with the Dell server management portfolio

vs. comparable server management tools from HPE

When it comes to selecting servers, specifications shouldn't be the only consideration on your list. By choosing a vendor with management tools that reduce hands-on time for administrators, bolster security, and offer sustainability planning, your infrastructure can help you meet a number of business goals. In the Principled Technologies data center, we compared capabilities of the server management portfolios from Dell and HPE to see what they have to offer administrators. We compared:

Table 1: The management tools we tested.

	Dell	HPE
Embedded/remote server management	Dell Technologies Integrated Dell Remote Access Controller (iDRAC9)	HPE Integrated Lights-Out (iLO 6)
One-to-many device management console	Dell Technologies OpenManage™ Enterprise (OME)	HPE OneView

We also looked at APEX AIOps Infrastructure Observability (formerly CloudIQ) and some of the features and benefits this cloud-based monitoring tool provides for server management.

Across the features and use cases we tested, the tools from the Dell management portfolio offered stronger security features, included a broader range of sustainability tools, and provided more granular control and increased flexibility for administrators while reducing time and effort to complete common tasks.

Bolster end-to-end security

Cyberattacks, where malicious actors infiltrate systems to retrieve and exploit private data, are on the rise. A 2023 report noted that "83% of organizations experienced more than one data breach during 2022,"[1] showing that cyber-security is a global concern. Selecting hardware with end-to-end security features can help safeguard your organization's data from these costly attacks. Dell offers strong security features both embedded in the server via iDRAC9 and in overarching console and cloud management software to bolster your organization's security.

Embedded security

Each Dell PowerEdge™ server has security features built in through iDRAC9 to stop bad actors from gaining access to data. Two such important features are:

- **Dynamic USB port enabling/disabling**: Disabling and enabling USB ports give 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.
- **Dynamic System Lockdown:** System Lockdown helps prevent 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 or Datacenter licenses.)

Figure 1 shows the results of our hands-on comparison using iDRAC9 and iLO 6 to dynamically disable USB ports.

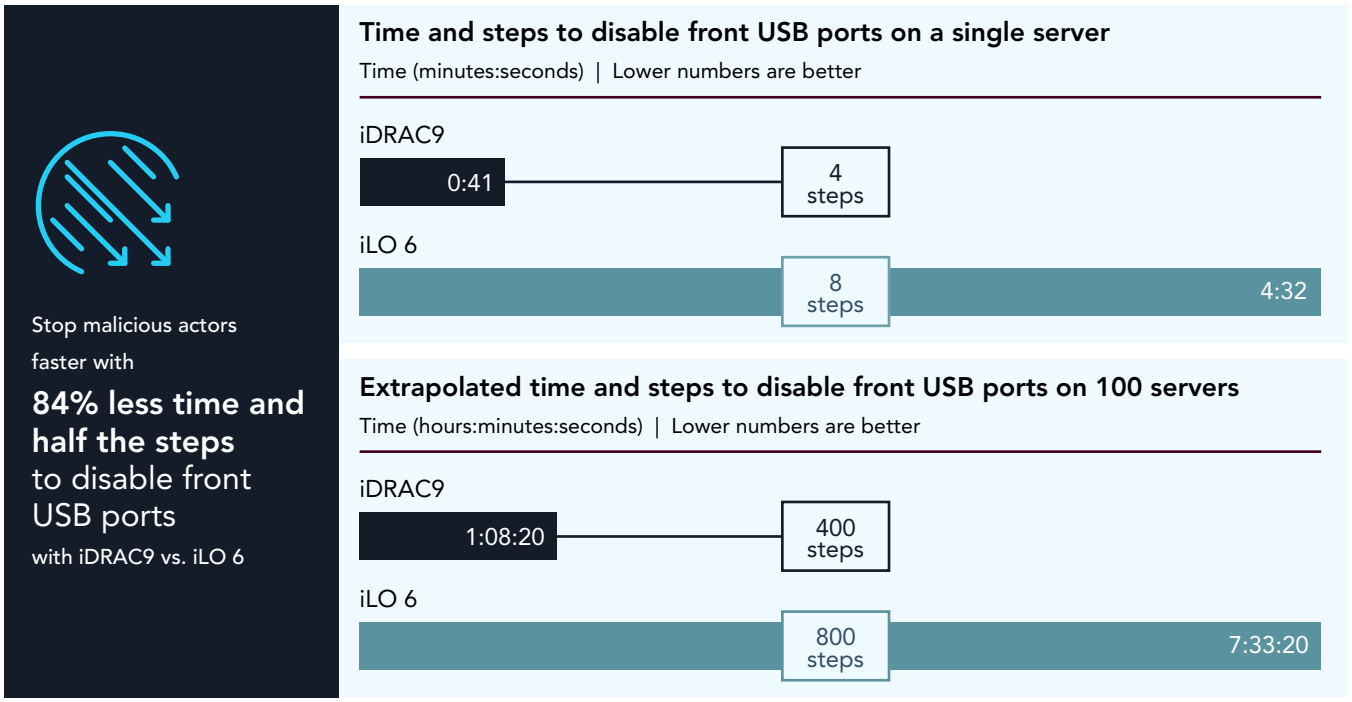

Figure 1: Time to disable front USB ports for a single server and extrapolated time to disable front USB ports for 100 servers. Less time and fewer steps are better. Source: Principled Technologies.

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

Using iDRAC9, we found that administrators could disable front USB ports on a single server in just 41 seconds and 4 steps. In comparison, the same process with iLO 6 would take 4 minutes 32 seconds and 8 steps per server. This means that **iDRAC9 takes 84 percent less time and half the steps to disable front USB ports**.[2] When you consider completing these steps in a data center, the time savings add up; for a 100-server deployment, admins could disable USB ports in 6 hours less time with iDRAC9 than with iLO 6.

Not only are these features easier and faster to access with iDRAC9 than with iLO 6, but with iDRAC9, admins can also **keep the servers in production** while enabling or disabling these features, **avoiding downtime**. iLO 6 requires both changing the BIOS configuration and rebooting each time.

The ability to quickly unlock a system for updates and lock it down quickly is paramount. As Figure 2 shows, we found that **admins could complete system lockdown of a server in 95 percent less time and 83 percent fewer steps with iDRAC9** compared to using iLO 6, which took over 5 minutes and 12 steps per server.

When you extrapolate this to a data center with 100 servers, admins could lock down systems in just over half an hour using iDRAC9, while it would take over a full workday—nearly 9 hours—to lock down 100 servers using iLO 6. That could be significant time for attackers to gain access to data. Plus, using the iLO 6 solution for system lockdown requires server downtime, while the iDRAC9 solution does not. The iDRAC9 lockdown feature is much faster and easier to use than the iLO 6 lockdown feature.

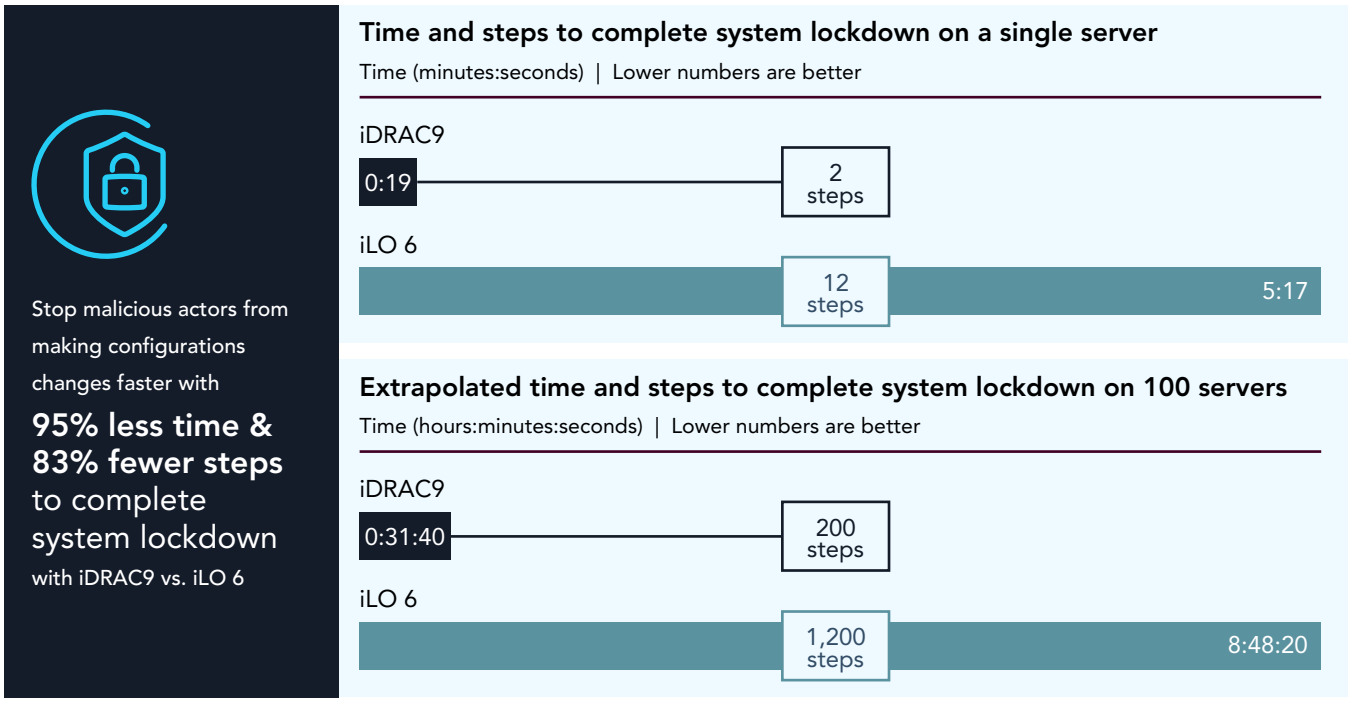

Figure 2: Time to complete system lockdown for a single server and extrapolated time to complete system lockdown for 100 servers. Less time and fewer steps are better. Source: Principled Technologies.

Keeping secure with easier credential management in OME

OME provides administrators an easier way to manage iDRAC9 password rotation. Rather than requiring a static, known administrator account, OME manages a service account where customers select the required password rotation policy for which the password is never disclosed. **OneView doesn't have this capability**. In our data center, we confirmed that iDRAC9-managed servers integrated with the OME account with full administrator privileges for easier credential management.

Helping meet your sustainability goals

Data centers have significant power and cooling needs, but thermal and power management can help administrators optimize data center costs and work toward sustainability goals while giving workloads the resources they need for top performance. OME incorporates several features that can enable close monitoring and management of power consumption, thus potentially helping you reach your sustainability goals. Tables 2 and 3 highlight key benefits of these features, which we describe in greater detail below.

Table 2: Sustainability differences between OME and OneView. Source: Principled Technologies.

Feature	OME	OneView
Carbon emission usage calculator and capacity planning tool	✓	x
Temperature-triggered power management policy	✓	x
Static power management policy	✓	x
Power Manager dashboard	✓	x
Power management reports with scheduled email distribution	✓	x

Table 3: Summary of our sustainability features comparison between OME and OneView. Source: Principled Technologies.

Feature	Key benefits with Dell management tools	Disadvantage with HPE management tools
Carbon emission usage calculator and capacity planning tool	Ability to estimate **greenhouse gas emissions** with customizable values to help you meet sustainability goals	**No comparable feature**; makes it difficult to plan for sustainability goals
Automated power and thermal management	**Static and temperature-triggered policy** options with the option to trigger when the server crosses a power consumption or temperature threshold	**No comparable features** for automated power management
Power-consumption dashboard and reports	OME Power Manager Plugin Dashboard **provides quick access** to Power Manager Data. OME Power Manager Plugin provides **25 different default and/or customizable reports** that quickly identify top energy consumers, power offenders, underutilized racks, and idle servers	OneView has **no Power Manager dashboard** and has **no power management reports**
Power management metrics	Up to **5x the metrics**, offering more granular insight into power consumption management with 15 metrics	**Only 3 metrics**, giving less insight and control of power consumption

Carbon emissions and carbon footprint analysis

One of the features that **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 plug in values for their own region's power costs and carbon emissions for each unit of power consumed for data specific to their data center's consumption model. **OneView doesn't have a comparable feature**—making it more difficult for organizations to plan with sustainability in mind.

Automated power and thermal management

OME Power Manager offers automated power and thermal management through both power and temperature-triggered policy options that allow administrators to set limits for power consumption or temperature thresholds to help reduce cooling costs. In contrast, **OneView offers no automated power and thermal management feature**. Because administrators can't set limits based on temperature, cooling costs could grow due to lack of automated controls.

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. **OneView offers no similar power management reports** (see Figure 3).

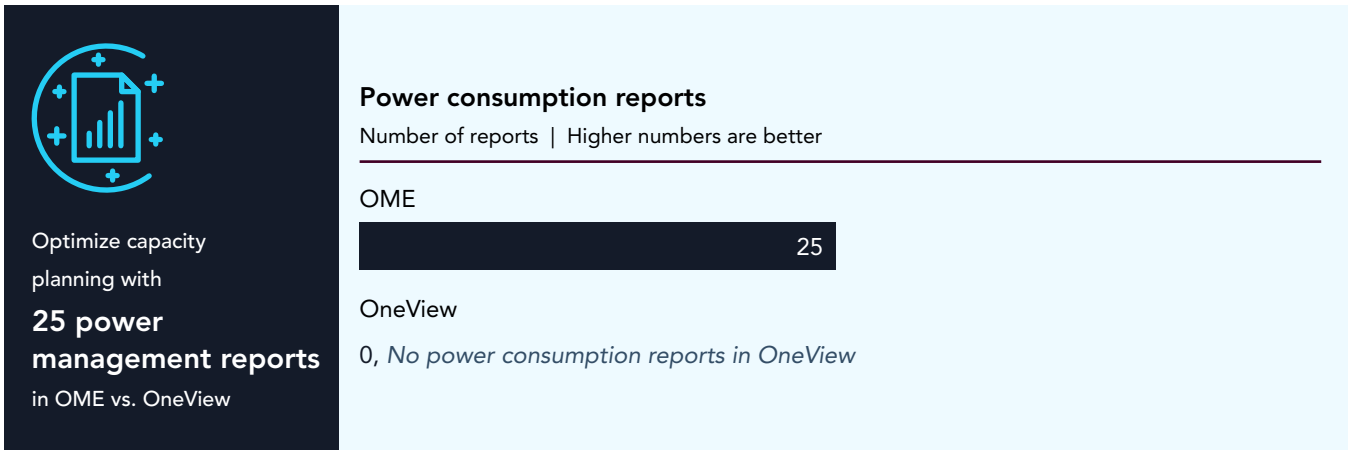

Figure 3: Comparison of the number of power management reports available in OME and OneView. More reports are better.
Source: Principled Technologies.

To further optimize power management, OME Power Manager plugin allows administrators to view up to 4x more metrics compared to OneView (see Figure 4). OME provides 15 metrics, including power usage by **individual components, virtual machines, air flow, and component utilization**, whereas OneView provides only 3 metrics.

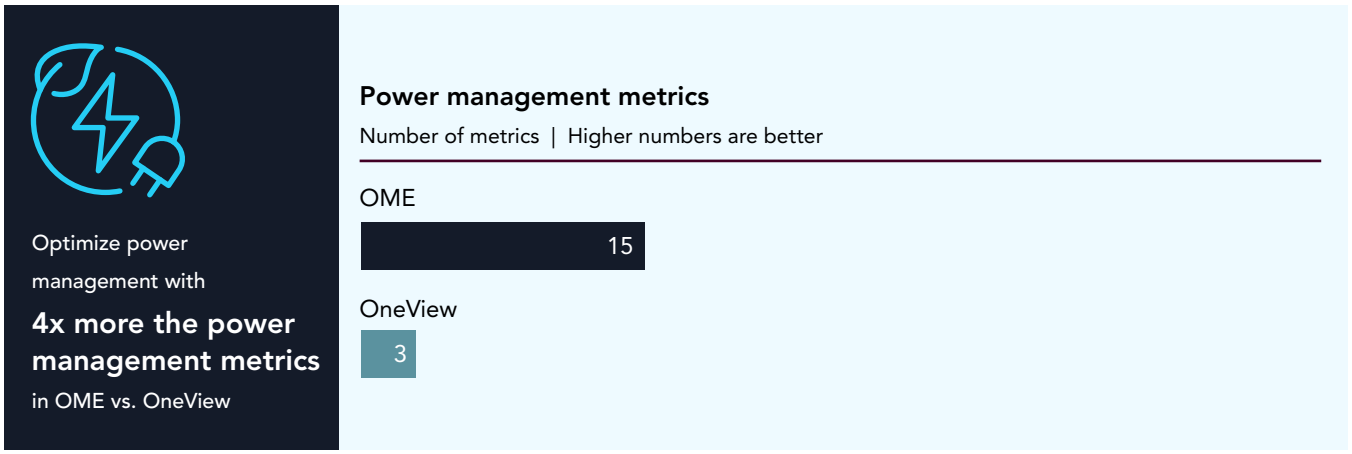

Figure 4: Comparison of the number of power management metrics available in OME and OneView. More metrics are better.
Source: Principled Technologies.

Make administrator tasks easier with stronger ease-of-use features

Data center administrators are busy people, but the right management tools can automate certain tasks, improve day-to-day management, and remove burdens to give them time back to innovate. We found that the Dell 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. HPE management tools.

Table 4: Overview of key ease-of-use features available in iDRAC9 and OME vs. iLO 6 and OneView. Source: Principled Technologies.

Feature	Key benefits with Dell management tools	Disadvantage with HPE management tools
More remote BIOS and HTML5 features	iDRAC9 offers **2.5x as many HTML5 features (with 10)** and **16x more remote BIOS features (with 51)**	iLO 6 offers **only 4 HTML remote features** and 3 remote BIOS features
Easier BIOS configuration changes	**87% less time and half the steps** to make a BIOS configuration change	Requires **administrator presence** to make changes
Telemetry streaming	iDRAC9 **provides telemetry for 8 modules**	iLO 6 provides telemetry for **only 3 modules** using JSON output from HPE
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	iLO 6 has **no physical connection information** to upstream switches
Scalability	OME can **manage up to 8,000 devices**[3]	OneView can manage **only 1,024 devices**[4]
Alert-based actions	OME **provides alert policies** that trigger actions based on input from an alert for one, a group, or all servers Setting up an alert requires a **one time setup** of 13 steps and 65 seconds, then **action occurs automatically**	OneView **does not offer alert-based actions** Setting up an alert requires **5 steps and 36 seconds for each and every server**, requiring significant admin time for large deployments
Firmware management	OME Firmware management **allows the updating of a single component, or all components,** for compliance with a defined baseline	OneView **offers only firmware baseline compliance** through attachment within the server profile
Third-party device monitoring	OME **supports third-party device and server monitoring**	OneView **does not support** third-party device and server monitoring.
Reporting	OME offers **4.2x as many reports** with **42 built-in reports** with customization to granularly select the most important data for their purposes	OneView offers only **10 built-in reports without customization**
Mobile monitoring/ management	OME **integrates with OpenManage Mobile**, providing visibility and manageability for infrastructure on an admin's iOS or Android mobile device	OneView **has no mobile application**, which makes management less flexible for admins

To ease the management burden and give administrators a single location for management and monitoring, OME offers expanded support for a wide range of servers, chassis, networking devices, and more. For the full OpenManage support matrix, visit https://www.dell.com/support/kbdoc/en-us/000217909/openmanage-enterprise-4-0-support-matrix.[5]

Easier server deployment with one-to-many configuration templates

For deployments with multiple servers, using OME can cut the time to deploy configuration templates compared to using OneView. Deploying a configuration template for a single server takes similar time with both solutions: 47 seconds and 10 steps for OME, and 49 seconds and 5 steps for OneView. But admins can deploy configuration templates to groups of servers in OME, while in OneView, admins must deploy configurations to each server individually.

This means that for an identically configured 100-server deployment, OME would take only 47 seconds and 10 administrator steps, but OneView would take roughly 1 hour 21 minutes and 500 steps to deploy configuration templates to servers—taking 99 percent less time and 98 percent fewer steps (see Figure 5).

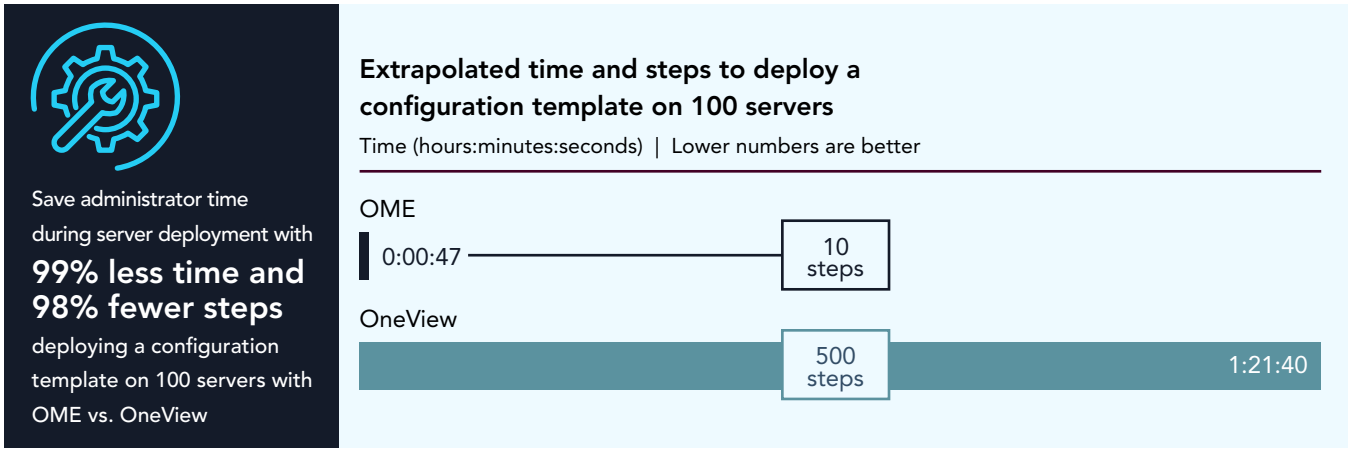

Figure 5: Comparison of the time and steps it took to deploy configuration templates with OME vs. OneView. OME can apply a template to many servers at once, increasing time savings even more. Less time and fewer steps are better. Source: Principled Technologies.

Easier alert setup

We found that OME offered more options for monitoring infrastructure. OME enables users to set up alert policies once and then automatically assign them for future alerts. We created an alert policy that would perform a graceful shutdown if the system received a critical temperature warning from the iDRAC9 in 13 steps and 65 seconds. While the one-time setup process for automating alerts takes longer (1 minute 5 seconds) than using OneView (36 seconds and 5 steps), OneView has no automated options for alerts, so administrators must execute actions manually every time. This means that for a 100-server deployment, using OME would save up to 98 percent less time and 97 percent fewer steps by automating actions based on alerts after admins have created a policy compared to OneView.

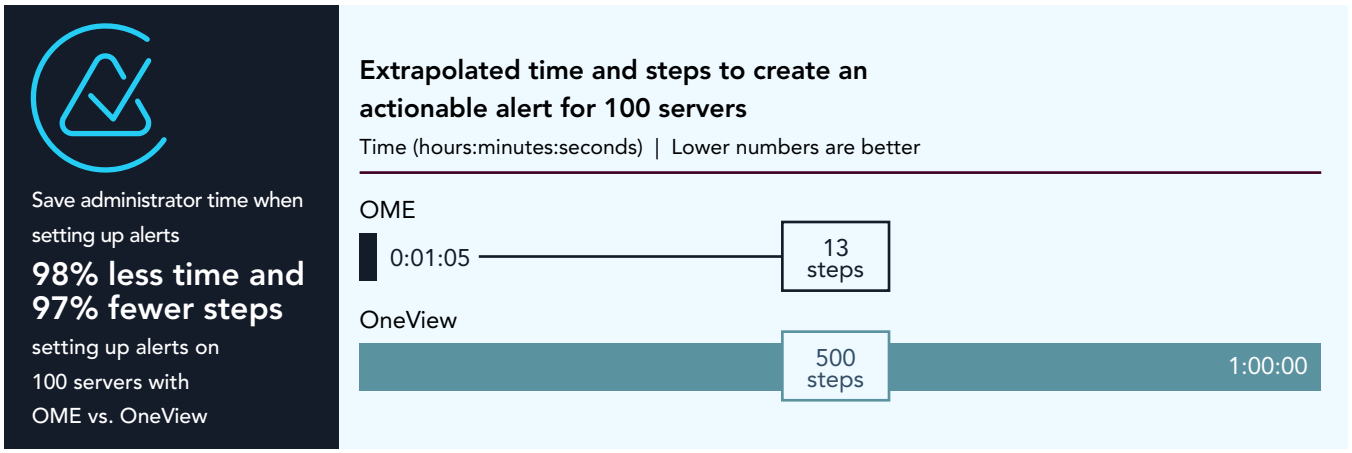

Figure 6: Comparison of the time and steps it took to set up alerts with OME vs. OneView. OME automates alerts after a single setup, saving admin time and effort. Less time and fewer steps are better. Source: Principled Technologies.

About Dell Technologies OpenManage Enterprise

OME is a one-to-many systems management console for the data center and beyond. 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 offers complete lifecycle management of Dell PowerEdge servers and 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.

Remote management

Remote management features give admins the freedom to make more changes from outside the data center. We found that iDRAC9 offers 1.5 times more HTML5 remote console features than iLO 6 provides, with 10 total features compared to just 4, making iDRAC9 remote server management easy and efficient. iDRAC9 also offers 16 times more BIOS configuration features than iLO 6 (51 features vs. just 3 features), giving administrators more granular control over BIOS configuration (see Figure 7 and Figure 8).

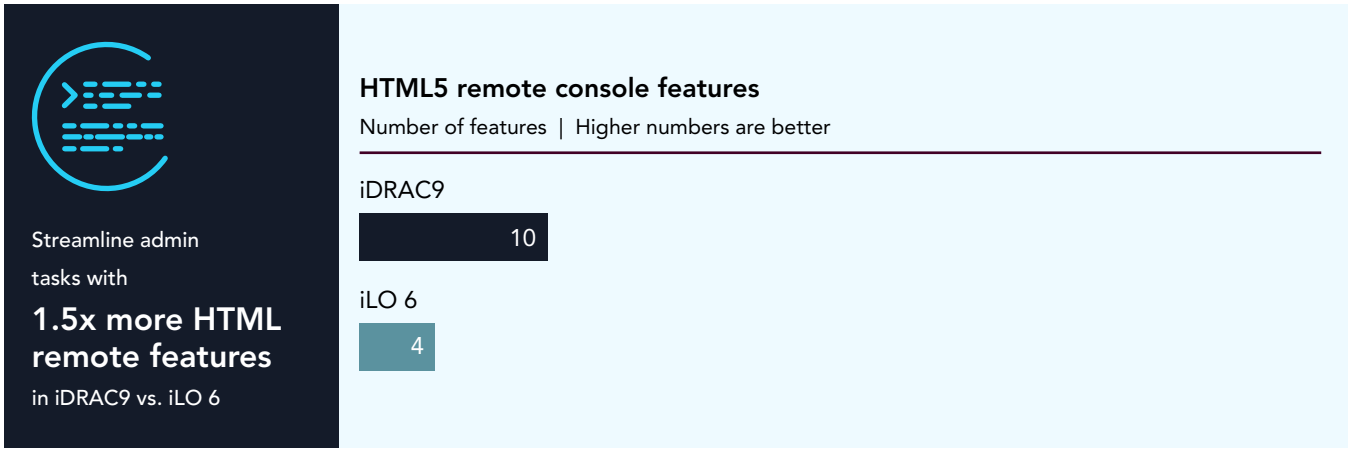

Figure 7: Comparison of the HTML5 remote features each management tool offers. More features are better. Source: Principled Technologies.

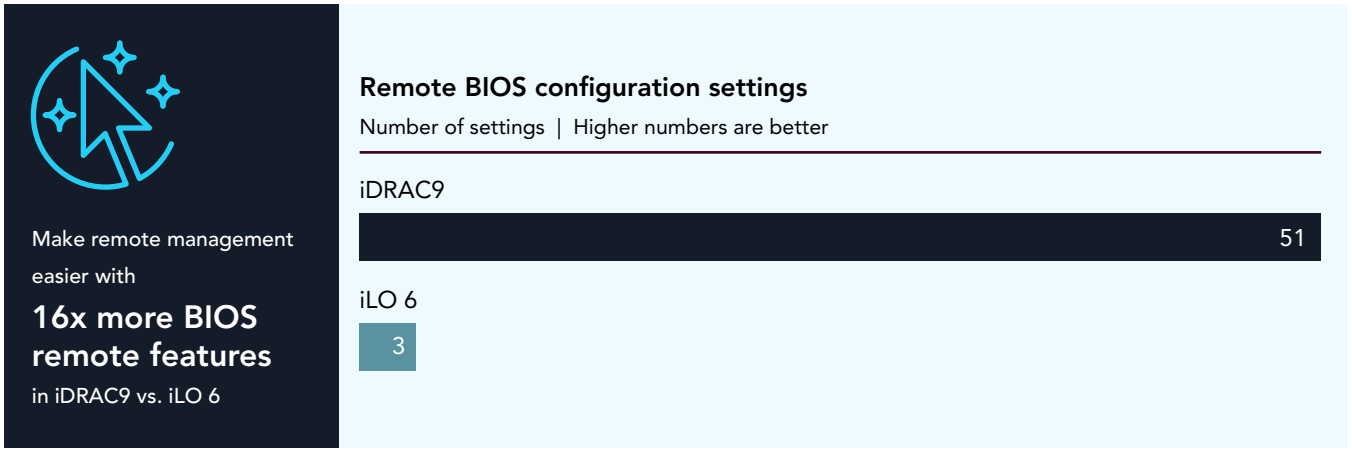

Figure 8: Comparison of the BIOS remote features each management tool offers. More features are better. Source: Principled Technologies.

Making BIOS 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 iLO 6 requires changes from within the system utilities and manual administrator intervention during the change. As Figure 9 shows, staging the BIOS configuration change for a scheduled reboot took 87 percent less time and half the steps with iDRAC9 vs. iLO 6. These per-server time savings can lead to more significant admin time saved in larger deployments. For example, in a 100-server deployment, you could save over 6 hours. iDRAC9 and iLO 6 both require individual per-server BIOS configuration changes.

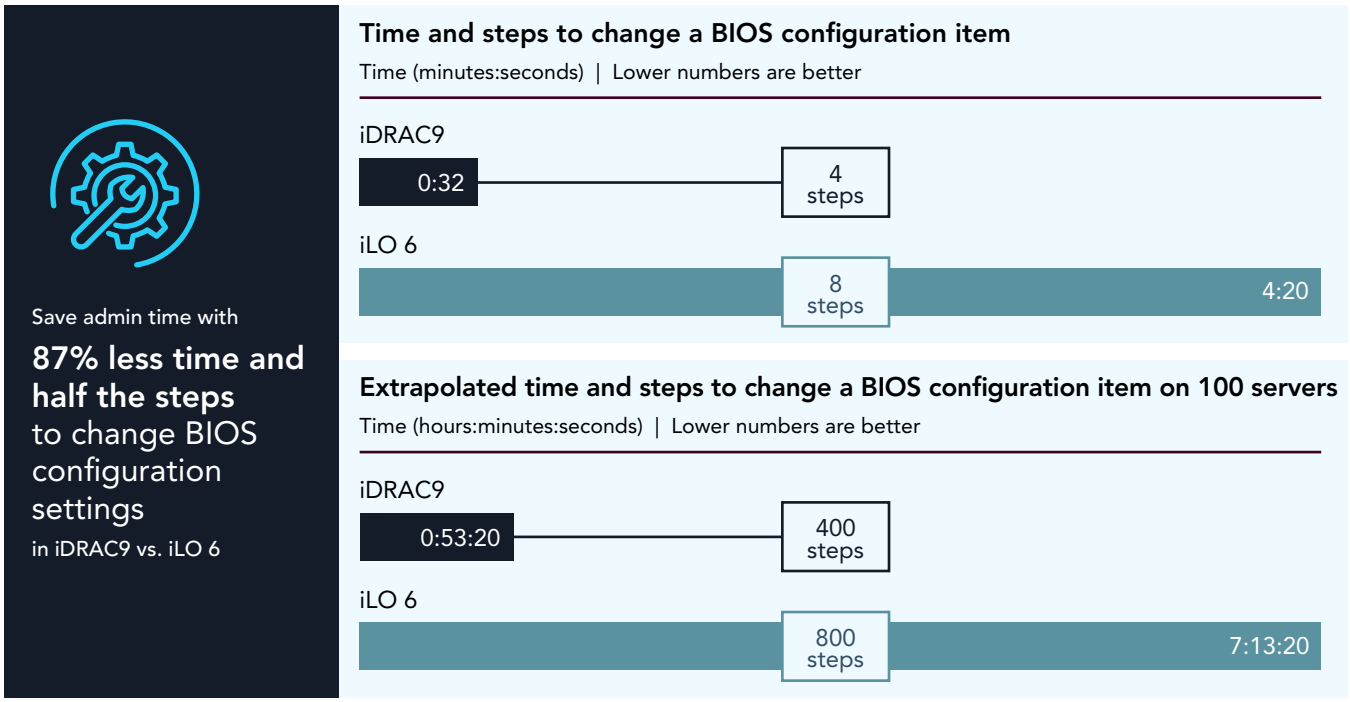

Figure 9: Time to change BIOS configuration settings and stage the update for a later reboot for a single server and extrapolated time for 100 servers. Less time and fewer steps are better. Source: Principled Technologies.

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:

- The ability to manage thousands of servers using APIs and scripting tools
- Embedded support, offering a view of server health and status monitoring thousands of parameters
- Telemetry and automation
- Strong security features and options[8]

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

Boosting security, sustainability, and admin efficiency with APEX AIOps Infrastructure Observability (formerly CloudIQ)

Cloud-based monitoring tool APEX AIOps Infrastructure Observability (formerly CloudIQ) offers administrators a way to monitor, manage, and analyze performance across deployments of Dell PowerEdge infrastructure, including servers, storage, and more. APEX AIOps Infrastructure Observability (formerly CloudIQ) offers several security features that can further strengthen your organization against attacks. We highlight some of these features in Table 5.

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 frequent insights for cyber-security with specific security risk level alerts so admins can react faster and address problems quickly to safeguard their data.
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 security gaps.

By employing these security monitoring features from the cloud, APEX AIOps Infrastructure Observability (formerly CloudIQ) offers administrators another easy-to-use, automated way to keep their infrastructure's health and security in check.

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

The cloud-based monitoring platform APEX AIOps Infrastructure Observability (formerly CloudIQ) offers additional ease-of-use features that integrate with iDRAC9 and OME and make it easier for administrators to observe the status of their PowerEdge environment and take action where required. Some of these features include:

- **Carbon footprint analysis**: Located in the Monitoring section, this tool that gives a higher view and forecast of carbon emission usage across environments.
- **Performance views:** APEX AIOps Infrastructure Observability (formerly CloudIQ) provides Performance views and anomaly and utilization charts to alert administrators at the first sign of problems.
- **Customizable performance and inventory reports:** APEX AIOps Infrastructure Observability (formerly CloudIQ) 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.

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.[9] In a 2022 Principled Technologies study, we found that APEX AIOps Infrastructure Observability (formerly CloudIQ) had negligible impact on network bandwidth while allowing us to monitor telemetry, health status, alerts, and inventory from a single console.[10] Learn more about APEX AIOps Infrastructure Observability (formerly CloudIQ) at https://www.dell.com/en-us/dt/apex/aiops.htm.

After we finished testing, Dell released new functionality that enables administrators to make **system updates** from within APEX AIOps Infrastructure Observability (formerly CloudIQ). According to Dell documentation, the System Updates page has up to five categories available for system updates—Storage, Networking, HCI, Data Protection, and Server. While we did not test this functionality at this time, we plan to validate this capability in a later paper.[11]

Conclusion

Anytime you make a hardware purchase, you're also getting the portfolio of management tools the hardware vendor offers to manage and monitor your infrastructure. Specifications are important, but so is end-to-end security, meeting sustainability goals, and the ability to streamline administrator tasks. In our data center, we compared the features and capabilities of server management tools from Dell and HPE, comparing iDRAC9 against iLO 6 for embedded server management and OME against OneView for one-to-many device and console management and monitoring.

In the areas of security, sustainability, and management/monitoring features, we found that Dell server management tools had more to offer than comparable HPE tools—giving administrators more remote management options, reducing the time to lock down systems, and offering more granular control to help meet sustainability goals. By reducing the administrator time and effort for certain routine monitoring and maintenance tasks with the Dell management portfolio, you can give your team time back to innovate and support other initiatives.

---

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. Note: This method on HPE iLO 6 shuts down all external USB ports, not just front ports.
3. Dell, "OpenManage Enterprise 4.0.x Support Matrix," accessed April 19, 2024, https://www.dell.com/support/kbdoc/en-us/000217909/openmanage-enterprise-4-0-support-matrix.
4. HPE, "HPE OneView 8.7 Support Matrix," accessed April 19, 2024, https://support.hpe.com/hpesc/public/docDisplay?docId=sd00003831en_us&page=GUID-D7147C7F-2016-0901-066B-000000000529.html.
5. Dell, "OpenManage Enterprise 4.0.x Support Matrix," accessed April 19, 2024, https://www.dell.com/support/kbdoc/en-us/000217909/openmanage-enterprise-4-0-support-matrix.
6. Dell, "OpenManage Enterprise," accessed April 9, 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 April 9, 2024, https://www.principledtechnologies.com/Dell/PowerEdge-MX-OME-OME-M-0124.pdf.
8. Dell, "Integrated Dell Remote Access Controller (iDRAC)," accessed April 9, 2024, https://www.dell.com/en-us/lp/dt/open-manage-idrac.
9. Dell, "APEX AIOps: Tame IT complexity in your digital business," accessed June 10, 2024, https://www.dell.com/en-us/dt/apex/aiops.htm.
10. 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.
11. Dell, "System Updates," accessed April 19, 2024, https://infohub.delltechnologies.com/en-US/l/cloudiq-a-detailed-review/system-updates-2/.

Read the science behind this report at https://facts.pt/2iPWgc5 ▶

Principled Technologies®

Facts matter.®

This project was commissioned by Dell Technologies.