Easier firmware updates

by setting up automatic updates in

74 seconds

with iDRAC9 vs. no automatic updates in Supermicro IPMI

Strengthen security

through dynamic USB configuration in just

37 seconds

with no system downtime

with iDRAC9

Agentless lifecycle management

to ease monitoring and management

in Dell OME

Dell management tools made server deployment and updates easier, offered more comprehensive security, and provided more robust infrastructure analytics

vs. comparable tools from Supermicro

A key consideration in choosing new data center hardware is the efficacy of the embedded management tools that admins use to deploy, monitor, secure, and maintain the infrastructure. Choosing tools with robust features and greater automation can both help keep servers secure and streamline routine administrator tasks, giving them time back in their day.

We performed hands-on testing to compare capabilities and available features of the management portfolios from both Dell™ and Supermicro®. We compared:

Table 1: The management tools we tested. Source: Principled Technologies.

	Dell	Supermicro
Embedded/ remote server management	iDRAC9 (Integrated Dell Remote Access Controller)	Supermicro Intelligent Management (IPMI)
One-to-many device and console management	Dell OpenManage™ Enterprise (OME)	Supermicro Server Manager (SSM)

We found that the Dell management tools made server deployment and configuration easier, offered more security features, delivered agentless lifecycle management, and provided more robust analytics options to monitor infrastructure performance.

Simplify your administrators' days with easier ways to monitor and manage servers

Table 2 offers a glimpse at some of the ways we found tools from the Dell management portfolio were easier to use than comparable tools from the Supermicro portfolio. (Note: We dive into these wins in more depth in the following pages.)

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

	What's different with Dell management tools	How much better
Easier firmware updates *iDRAC9 vs. Supermicro IPMI OME vs. Supermicro SSM*	• Automated online updates with iDRAC9, with scheduling options • OME allows for the creation of custom firmware repositories and can update firmware of BIOS, BMC, and other server components without additional tools or agents	• We set up automatic updates in iDRAC in **just 74 seconds** • Supermicro IPMI has **no automatic update function** available, so admins must update manually • SSM supports only BIOS and BMC firmware updates and requires SUM to update other components
More security features *iDRAC9 vs. Supermicro IPMI OME vs. Supermicro SSM*	• iDRAC9 offers MFA and dynamic disabling of USB ports with no system downtime • OME offers both role-based access control (RBAC) and scope-based access control (SBAC) to restrict device management to a subset of device groups	• Supermicro IPMI has **no MFA features** • Supermicro IPMI requires a system reboot and entering BIOS configuration to disable USB ports • Supermicro SSM offers RBAC but not the more restrictive SBAC
Easier lifecycle management *OME vs. Supermicro SSM*	• Full, agentless lifecycle management via OME to ease management and monitoring	• SSM requires the SuperDoctor5 agent for detailed local system health metrics and Supermicro Update Manager (SUM) to update additional components
Easier server deployment *iDRAC9 vs. Supermicro IPMI*	• Import a complete Dell server profile in just 12 steps using iDRAC9 • Robust BIOS configuration options with iDRAC9 with 52 BIOS features and support for components configuration such as RAID NIC & iDRAC	• Supermicro IPMI allowed us to save and restore only the IPMI configuration rather than the whole server profile • iDRAC9 has 52 BIOS features, while IPMI offers **no BIOS configuration options**
More options for reporting and analytics *iDRAC9 vs. Supermicro IPMI OME vs. Supermicro SSM*	• iDRAC9 offers telemetry streaming, which lets users easily send server data to analytics tools such as Splunk • OME sends telemetry data directly to CloudIQ for easier monitoring	• IPMI offers only a SYSLOG feature admins can use to send messages for aggregation and eventual analysis • SSM has no cloud-based management solution equivalent to Dell CloudIQ
More sustainability features *OME vs. Supermicro SSM*	• More metrics for monitoring in OME Power Manager, including carbon footprint data	• SSM has less robust utilization metrics and **no way to track carbon footprint**
More ways to monitor *OME vs. Supermicro SSM*	• Manage Dell servers from anywhere via the OpenManage mobile app • Monitor third-party devices with OME using server IPs and credentials with support to import 3rd party SNMP MIBS	• SSM has **no mobile app** • SSM **does not allow** monitoring of third-party devices with server IPs

Make server management automated and easier with expanded features in the Dell management portfolio

REMOTE MANAGEMENT

Through iDRAC9, we had access to **52 BIOS configuration features** to help make remote management easier. Supermicro IPMI offers only system information, and admins must configure the BIOS via BIOS settings in the remote console.

Dell OME offers **HTML5 remote console features** for remote management. Supermicro SSM **does not have an HTML5-based console**, but instead provides a JRE-based console that requires updates.

EASIER SERVER DEPLOYMENT

Configuring and deploying servers with images and settings can require significant administrator effort. Dell iDRAC9 and OME offer features to ease this process and get servers into production faster. **Using iDRAC9, we configured a complete server profile in just 12 steps and 2 minutes 22 seconds, which we could then port to other servers.** These complete server profiles included all BIOS settings, drive configurations, power policies, and more. This helps maintain uniformity across systems and eases the administrative burden.

Supermicro IPMI doesn't offer a similar feature; it allows admins to save only the IPMI configuration itself and restore it onto other platforms. Configuring other servers with the same IPMI configuration can create conflicts: For example, duplicating IP addresses could make one or both of the servers unreachable on the network.

EASIER FIRMWARE UPDATES

Keeping servers up to date with the latest firmware helps keep the environment secure, but tracking and updating firmware can be a time-consuming task without automation. **iDRAC9 offers automatic firmware updates and the ability to schedule updates as administrators desire. Conversely, we found no evidence that Supermicro IPMI offers a similar feature.** In IPMI, we could click Maintenance and access the Firmware Management tab to complete updates, but we didn't find any features to perform even a firmware check without administrator interaction.

Dell OME utilizes the Dell Update Manager plugin, which lets admins create custom repositories and select automatic online synchronization with Dell. (Note: OME can perform these tasks without this plugin as well.) With SSM, admins can update system BIOS and BMC firmware. However, they must update all other components via Supermicro Update Manager (SUM), which comes as a unified extensible firmware interface (UEFI) in Supermicro X12 hardware and older models, or administrators can install SUM software on an OS to manage servers in- or out-of-band. **Dell OME allows for full lifecycle management without needing any additional agents.** SSM requires admins use the SuperDoctor5 agent to monitor local system health and SUM or the local BMC to manage and configure the BIOS/BMC firmware.

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 serviceability[1]

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

Keep systems secure with more comprehensive and easy-to-use security features

We found that through iDRAC9 and OME, the Dell management portfolio offers more built-in security features than the Supermicro tools. The security features we assessed include:

- **Multi-factor authentication (MFA):** MFA prompts admins for a passcode in addition to their login credentials, which helps 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, or BIOS.
- **Scope-based access control (SBAC):** A way to extend the capabilities of role-based access control, this feature lets admins restrict rights to certain devices for additional security.

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

	Dell	Supermicro
MFA	✓	✗
Dynamic USB with no downtime	✓	✗
SBAC	✓	✗

Dell iDRAC9 offers MFA through SecurID, a straightforward process that took us just 7 steps to configure. In contrast, we found no evidence of MFA features within Supermicro IPMI. Because Dell iDRAC9 offers MFA, these systems have an additional layer of protection that helps keep critical data secure.

After a one-time dynamic USB configuration of 46 seconds and four steps in Dell iDRAC9, we could disable front and side USB ports without any system downtime in only four steps and 37 seconds. As Figure 1 shows, Supermicro IPMI required six steps and 2 minutes 50 seconds to disable USB ports—while also requiring us to reboot the system and enter the BIOS to achieve the same result.

While Supermicro SSM offers only RBAC, Dell OME offers both RBAC and SBAC, which goes one step further in restricting access to systems to bolster security. Dell OME SBAC allows restriction of a Device Manager role to a subset of device groups called scopes, which again provides an additional layer of security and more options for admins to manage infrastructure.

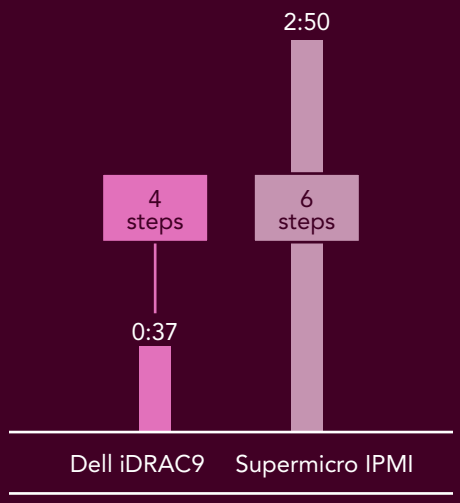

Figure 1: Comparison of the time and steps it took to complete the Dynamic USB use case with iDRAC9 vs. IPMI. Less time and fewer steps are better. Source: Principled Technologies.

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.[2]

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

Monitor system health with more analytics and reporting options

Monitoring infrastructure health is critical to keeping applications running at optimal performance. In both embedded server management and console management, Dell offers telemetry streaming data that can sync with cloud-based management tools for easier monitoring and analysis. 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, another Dell management tool. (Note: This feature is available with iDRAC9 Enterprise or Datacenter licenses.)

Neither of the Supermicro tools we tested offered telemetry streaming to a cloud-based management system (see Table 4). Supermicro IPMI does have a SYSLOG feature that collects some data that can help administrators in troubleshooting active events, but it is less useful than telemetry when it comes to determining states leading up to events.

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

Does the tool have telemetry streaming?	Dell	Supermicro
Embedded server management *iDRAC9 vs. IPMI*	✓	✗
Console management *Dell OME vs. SSM*	✓	✗

Table 5 compares some of the key features and options available in Dell OME and Supermicro SSM. Notably, Dell OME can make admins' tasks easier by giving them more monitoring options, such as third-party device monitoring, reporting options, and streaming telemetry data for granular monitoring. Dell OME alert-based automation also gives administrators the ability to automatically power down systems when serious issues arise.

Table 5: Summary of our comparison between Dell and Supermicro management tools. Source: Principled Technologies.

	Dell OME	Supermicro SSM
Third-party device monitoring	OME allows users to monitor third-party devices using server IPs and credentials—this allows heterogeneous device monitoring in the environment without switching consoles	**No support** for third-party devices
Mobile monitoring/ management	OpenManage Mobile allows management of servers connected to OME from anywhere	**No mobile app** equivalent, though the Supermicro IPMIView app offers some limited management function
Agentless lifecycle management	Full, agentless lifecycle management via OME	Requires SuperDoctor5 agent for local system health and SUM for managing firmware
Sustainability	Collect, calculate, store, and report on a customer's carbon footprint by utilizing default or customer defined variables that calculate carbon emissions based on extensive power usage metrics	SSM includes **limited power utilization metrics**: current power usage, max power usage, minimum power usage, and average power usage in watts—no carbon footprint data is available
Plugin-based architecture	Dell OME utilizes plugins to increase the functionality of the base level OME. Using the Update Manager plugin, create custom repositories and use automatic online synchronization for firmware updates	**No enhancement through plugins**
Robust reporting options	OME offers built-in reports with the ability to create customized reports	SSM offers limited built-in reports with **fewer reporting metrics** and no customization
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**

Conclusion

Streamlining administrator tasks through robust management tools can improve environment health and give admins time back to innovate and help business grow. In our comparison of tools in the Dell and Supermicro management portfolios, we found that Integrated Dell Remote Access Controller 9 (iDRAC9) and Dell OpenManage Enterprise offered more features and were easier to use than comparable Supermicro tools. Dell iDRAC9 and OME automate routine tasks that can save administrators time and effort. Additionally, the expanded security features of the Dell tools bolster security from bad actors, and advanced reporting options offer greater insight into environment health—key concerns for the modern organization that seeks to expand.

1. Dell, "Integrated Dell Remote Access Controller 9 User's Guide," accessed March 9, 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, "OpenManage Enterprise Solution Brief," accessed March 9, 2023, 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/OS2Up1L ►

Principled Technologies®

Facts matter.®

This project was commissioned by Dell Technologies.