Strengthen security with

3.5x the security features

Including two-factor authentication and external key management with iDRAC9

Optimize energy efficiency with more than

6x the power consumption reports

With 20 reports in Dell OME vs. 3 reports in Supermicro SSM

Increase operational efficiency by saving 1hr 50 mins admin time

per 100 servers

Using automatic updates with Dell iDRAC9 vs. no automatic updates available with Supermicro IPMI

Increase security, sustainability, and efficiency with robust Dell server management tools

Compared to the Supermicro management portfolio

When you invest in new servers for your data center, you're doing more than just selecting hardware—you're also choosing a manageability solution. When your administrators have efficient, feature-rich tools available to deploy, monitor, maintain, and secure your infrastructure while improving its energy efficiency, they can handle the day-to-day management easily and devote more time to innovations that move your organization forward. By choosing to purchase from a vendor with robust manageability tools, you could be saving yourself time and money down the line.

We assessed the server management portfolios of Dell™ and Supermicro®, comparing three tools from Dell against two tools from Supermicro.

Table 1: The management tools we tested. *Dell CloudIQ is a cloud-based monitoring and analytics tool; Supermicro offers no equivalent tool.
Source: Principled Technologies.

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

In terms of sustainability, security, and everyday management experience, we found that Dell consistently provided more feature-rich toolsets that empower administrators with more options and capabilities.

More and richer features to automate and ease your server management

Your IT teams need modern, feature-rich management tools that can save them time in their everyday work and keep up with standards for security and efficiency. The Dell management tools we assessed include a number of features and capabilities that are not present in the Supermicro management portfolio.

Sustainability

As energy costs rise and environmental regulations increase, many organizations are making sustainability a focus. Data centers inherently require large amounts of power, but careful thermal and power consumption management can allow organizations to reduce the amount of power they consume. Dell OpenManage Enterprise 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 Dell OpenManage Enterprise and SSM. Source: Principled Technologies.

Feature	Dell management tools	Supermicro management tools
Carbon emission usage calculator and capacity planning tool	✓	x
Carbon footprint analysis	✓	x
Temperature-triggered power management policy	✓	x
Static power management policy	✓	✓

Table 3: Summary of our comparison between Dell OME and Supermicro SSM and IPMI. Source: Principled Technologies.

Feature	Key benefits with Dell management tools	Disadvantage with Supermicro management tools
Carbon emission usage calculator and capacity planning tool	Ability to estimate **greenhouse gas emissions** with customizable values to help you meet your sustainability goals	**No comparable feature**; makes it difficult to plan for helping you meet your sustainability goals
Carbon footprint analysis	**Available** via OpenManage Enterprise Power Manager; provides data about carbon emissions, which can help you meet sustainability goals	**No comparable feature**; no way to track carbon footprint to help you monitor meeting your 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	**One static policy type** with no associated trigger options
Power-consumption reports	**More than 6x** the reports, with **20 built-in** reports with scheduled email distribution and customization options	**2 built-in reports** in SSM; 1 report in Supermicro IPMI that is not exportable
Power management metrics	Up to **15x the metrics**, offering more granular insight into power consumption management	**Only 1**, giving less insight and control of power consumption

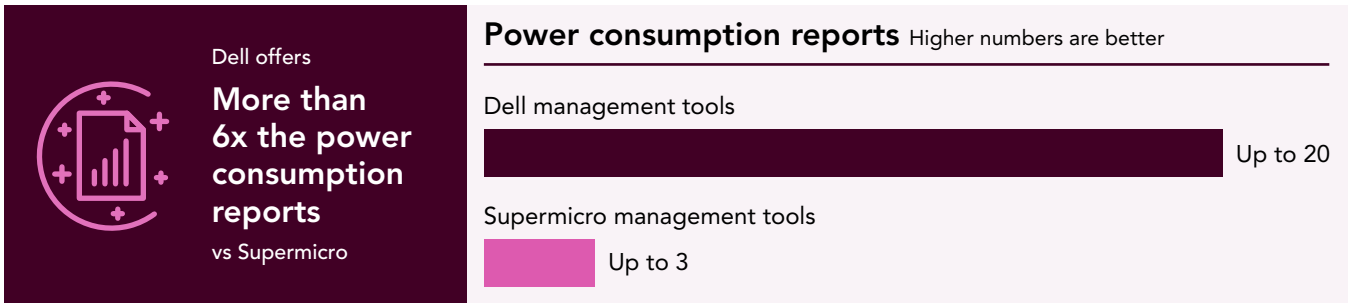

Figure 1: Number of power consumption reports available in Dell OME and Supermicro SSM. Source: Principled Technologies.

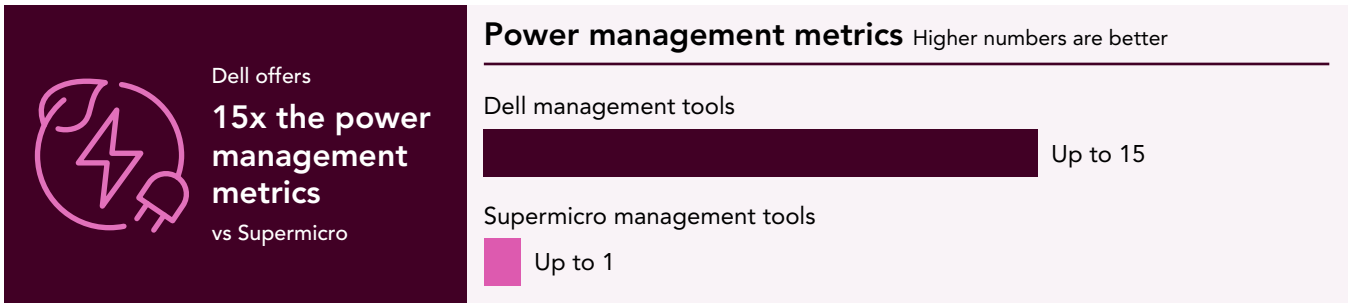

Figure 2: Number of power management metrics available in Dell OME and Supermicro SSM. Source: Principled Technologies.

Automated power and thermal management

OpenManage Enterprise Power Manager offers automated power and thermal management through both static power and temperature-triggered policy options that allow administrators to set limits for power consumption or temperature thresholds to help reduce cooling costs. In contrast, SSM has a single policy, a static limit on power consumption that is not automatically triggered by a server going beyond the limit, which could lead to higher energy costs.

Organizations seeking a deep dive into their data center's power consumption with an eye toward optimization can benefit from the **20 different built-in power consumption reports** OpenManage Enterprise Power Manager offers. These reports are useful in capacity planning and managing power to maximize efficiency. The reporting options in SSM are much more limited. Admins can only run a single host with a service report or see a power consumption trend in the monitoring screen. With the Supermicro IPMI, users can view a component-level power graph in the BMC; however, they cannot export the data in the graph for analysis and can save it only as an image.

The OpenManage Enterprise Power Manager plugin allows administrators to **view up to 15 different metrics**, including power usage by individual components, air flow, and component utilization, whereas SSM offers only total power usage.

Carbon emissions and carbon footprint analysis

OME includes a carbon emission usage calculator and capacity planning tool that, among other functions, can help you estimate your own greenhouse gas emissions. It provides default values for power costs and carbon emissions for a unit of energy consumed, but allows you to customize those values for your own region's power costs and your data center's consumption model. SSM offers no comparable feature, which can make it difficult for organizations to plan and monitor progress towards their sustainability goals.

Security

Cybercrime is increasing exponentially, threatening companies with "damage and destruction of data, stolen money, lost productivity, theft of intellectual property, theft of personal and financial data, embezzlement, fraud, post-attack disruption to the normal course of business, forensic investigation, restoration and deletion of hacked data and systems, and reputational harm."[1] In this landscape, decision makers should factor security into any server purchase. We found that Dell OpenManage Enterprise incorporates several features to help keep your data safe that the Supermicro tools do not have (see Tables 4 and 5).

Table 4: Security differences between Dell management tools and Supermicro management tools. Source: Principled Technologies.

Feature	Dell management tools	Supermicro management tools
Multi-factor authentication	✓	x
External key management	✓	x
Scope-based access controls	✓	x
Policy-based security configuration	✓	x
Cybersecurity advisories	✓	x
Role-based access controls	✓	✓
Dynamic USB port disablement	✓	✓

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

Feature	Key benefits with Dell management tools	Disadvantage with Supermicro management tools
Multi-factor authentication (MFA)	**Two-factor authentication** with iDRAC with either **email and RSA SecurID**, preventing unauthorized users from gaining access to sensitive data	**No comparable feature**, leaving a security gap that could help unauthorized users gain access to sensitive data
External key management	**Secure Enterprise Key Manager** in iDRAC to add another layer of security to protect data-at-rest on servers using drive encryption and centralized management	**No comparable feature**, leaving another gap in security
Access controls	OME offers **both** role-based access control **(RBAC)** and scope-based access control **(SBAC)** to limit the device groups to which a device manager has access	**Only RBAC**, limiting the ability of admins to restrict access
Policy-based security configuration	**Policy-based security configuration** settings through CloudIQ, which alerts admins to discrepancies	**No comparable feature**, which can delay action and remediation of breaches
Cybersecurity advisories	**Security advisory reporting** through Dell CloudIQ security, with vulnerability details and applicable remediation suggestions to enable quick action	**No comparable feature**, leaving security gaps for bad actors to exploit

Multi-factor authentication

Multi-factor authentication (MFA) can help prevent unauthorized users and bad actors from gaining access to sensitive data. We verified that Dell iDRAC enables two-factor authentication both with email and with RSA SecurID, a set of external multi-factor authentication technologies used across many industries.[2] We also verified that neither Supermicro IPMI nor SSM offer this feature, leaving a security gap.

Key management

External key management systems (KMS) allow IT teams to use a separate, third-party server to manage the keys they use to lock and unlock a server's storage, adding a layer of security. iDRAC includes Local Key Manager (LKM) for all new Dell PowerEdge servers. Some licenses also offer Secure Enterprise Key Manager (SEKM), enabling extra security with full disk encryption and external key management. SEKM supports the industry-standard OASIS KMIP protocol, giving organizations their pick of any external KMS provider that uses that standard. Supermicro does not offer this security feature or an equivalent.

Access controls

Role-based access control RBAC, where a user's role determines the parts of the system to which they have access and the tasks they can perform there, is an integral component of many server security strategies. In OpenManage Enterprise, RBAC defines the user privileges for three built-in roles: Administrator, Device Manager, and Viewer.[3] It also offers scope-based access control (SBAC), which allows admins to limit the device groups to which a device manager has access.[4] This gives admins the ability to provide access to a subset of devices. Supermicro offers RBAC, but not SBAC.

Credential management

iDRAC password rotation serves several purposes: It rotates access to OpenManage Enterprise in accordance with the security policy, with a monthly default; it works with an external password handler; and it supports CyberArk to manage passwords.[5,6]

With OpenManage Enterprise, administrators can manage iDRAC password rotation by replacing the need for a static known administrator account with a service account managed by OME. SSM doesn't have this capability.

Policy-based security configuration

Dell offers a policy-based cybersecurity feature in the CloudIQ for PowerEdge AIOps solution. This feature takes the configuration of a deployed PowerEdge server and compares it to a security-related configuration policy based on Dell best practice. In the event that CloudIQ detects a discrepancy, it notifies the administrator and provides steps for remediation.[7] SSM offers no equivalent feature, which could mean delays in detecting breaches.

Cybersecurity advisories

Security Advisories notify the public about security issues. According to Dell, the Dell Security Advisories page in CloudIQ provides a full list of applicable security advisories along with their impact, number of systems they affect, and publish date.[8] Dell CloudIQ provides security advisory reporting with vulnerability details and remediation suggestions. SSM doesn't offer a similar feature, which could leave systems vulnerable.

About Dell CloudIQ

Dell 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 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 CloudIQ at https://www.dell.com/en-us/dt/solutions/cloudiq.htm.

Dynamic USB port disablement

Disabling and enabling USB ports gives administrators control over access to the server via a USB port thereby avoiding malicious use and introduce risk of installation of prohibited applications or viruses.

Dell iDRAC offers independent, dynamic USB port disablement with no downtime required. While Supermicro offers dynamic front side USB (and rear USB) disablement within the BIOS, it requires the Supermicro DataCenter Management Suite per Node License key to enable it. IT can trigger it by implementing the system lockdown command, which can be executed from either the BMC or the Supermicro IPMI console, but it's not independent of system lockdown mode.[11]

As Figure 3 shows, disabling the ports using Dell iDRAC was a simple process **requiring only 41 seconds and 4 steps** while the Supermicro IPMI took **more than four times as long, 2 minutes and 50 seconds and 6 steps**. Extrapolating these time savings to 100 systems, the time savings would grow to 3 hours and 35 minutes, meaning an admin would spend nearly half of a workday using Supermicro IPMI versus a little more than an hour using Dell iDRAC.

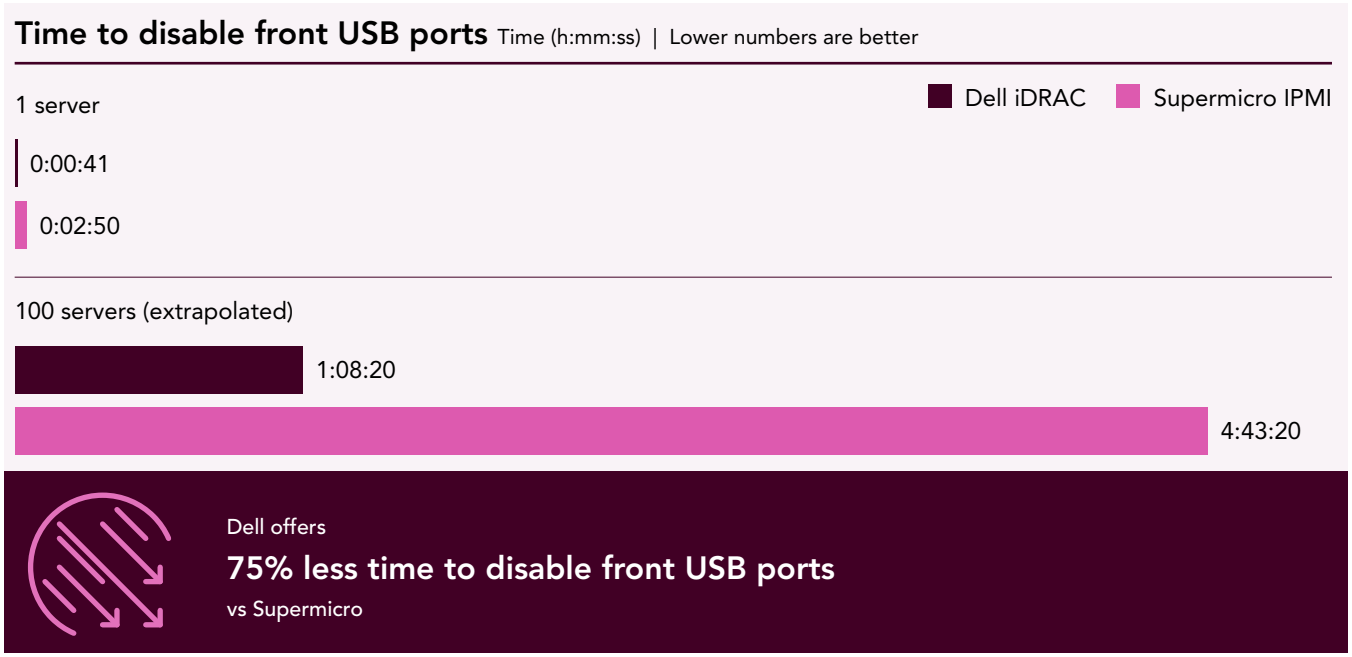

Figure 3: Time to disable front USB ports for a single server and extrapolated time to disable front USB ports for 100 servers. Lower is better. Source: Principled Technologies.

About Dell OpenManage Enterprise

OpenManage Enterprise is a one-to-many systems management console for the data center. The console offers a modern HTML5 graphical user interface and deploys as a virtual appliance for VMware ESXi™, Microsoft Hyper-V, and Kernel-based Virtual Machine (KVM) environments. OpenManage Enterprise 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.[12] In a recent PT study, we found that a Dell environment with OpenManage Enterprise and OpenManage Enterprise Modular (OME-M) can save time making changes to VLANs and help avoid interventions during scheduled firmware updates.[13]

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

Monitoring, analytics, and ease of use

Manageability tools vary greatly in how they support admins carrying out monitoring and analysis activities as well as other routine tasks, such as scheduling updates. In this section, we look at the differences in these areas between the Dell and Supermicro management tools we studied. As we found when we investigated sustainability and security features, the Dell suite of management tools offers numerous features to make the lives of administrators easier—features that the Supermicro tools do not have. Table 6 compares the managements benefits that the tools have to offer.

Table 6: Summary of our comparison between Dell and Supermicro management tools. Source: Principled Technologies.

Feature	Key benefits with Dell management tools	Disadvantage with Supermicro management tools
Telemetry streaming	iDRAC9 **telemetry streaming available** to remote syslog servers; helps predict failures and optimize performance; can stream server metrics to analytics tools such as Grafana and Splunk	**No automatic telemetry streaming**
Mobile monitoring and management	Feature-rich OpenManage Mobile app for iOS and Android, which integrates with OME and iDRAC9	Supermicro IPMIView app, which **does not integrate** with SSM
Third-party device and server monitoring	OME **supports third-party device and server monitoring**, including support for its major competitors	**Supports only third-party devices that use their agents**, their BMCs, earlier versions of their gear that are IPMI-capable, and Redfish-capable devices
Estate monitoring	Available via OME and CloudIQ; OME can transmit data on licensed managed servers to CloudIQ for monitoring across multiple data centers	**No cloud-based portal** to aggregate monitoring data across data centers
Alert-based actions	Policies in OME that trigger actions based on input from an alert	**No alert-based actions available**
Easier server deployment (Ability to import/export system configurations)	Can use iDRAC9 to **import/export** all configuration items for servers, requiring only **48 seconds and 5 steps for import and 1 minute and 9 seconds and 7 steps for export**	Can import/export **only baseboard management controller (BMC) configuration**, requiring significant manual configuration for each server
Less time to change BIOS configuration settings	Can quickly change **full BIOS settings directly from iDRAC** and stage the update and reboot for a maintenance window, saving significant admin time	**Limited BIOS changes available** from the BMC, otherwise server reboot required; takes more manual steps and admin time
Runs as a virtual appliance	**Available** in OME, which eliminates the need to update OS	**No comparable feature**, must run within a managed OS. This gives administrators one more component to patch and update
Connection View	**Available** in iDRAC; troubleshooting tool using LLDP for diagnosing networking issues such as cabling, bad switch ports, and more	**No Connection View**, no physical connectivity information about the upstream switch ports
Ability to schedule firmware and driver updates	**Available** in OME and iDRAC	Can schedule BIOS and BMC firmware updates, but **cannot schedule driver updates**

BIOS configuration item change

Dell offers full BIOS configurations settings changes directly from iDRAC with the ability to stage those changes for the next reboot. Supermicro offers a limited set of BIOS settings from its BMC. Apart from the limited set, a BIOS configuration change on Supermicro servers for a single configuration item requires the administrator to reboot the server to access the BIOS configuration menu from the boot screen.

Figure 4 shows the time to perform a BIOS configuration change on a single server using Dell iDRAC and Supermicro IPMI. The manual process using the **Supermicro tool takes an extra 2 minutes and 6 seconds**, or **4.9x longer** than setting up the automated process in iDRAC. If we extrapolate these times to 100 servers that are configured identically, the time savings with iDRAC would be 3.5 hours. (If the servers were not configured identically, we would not see these time savings.)

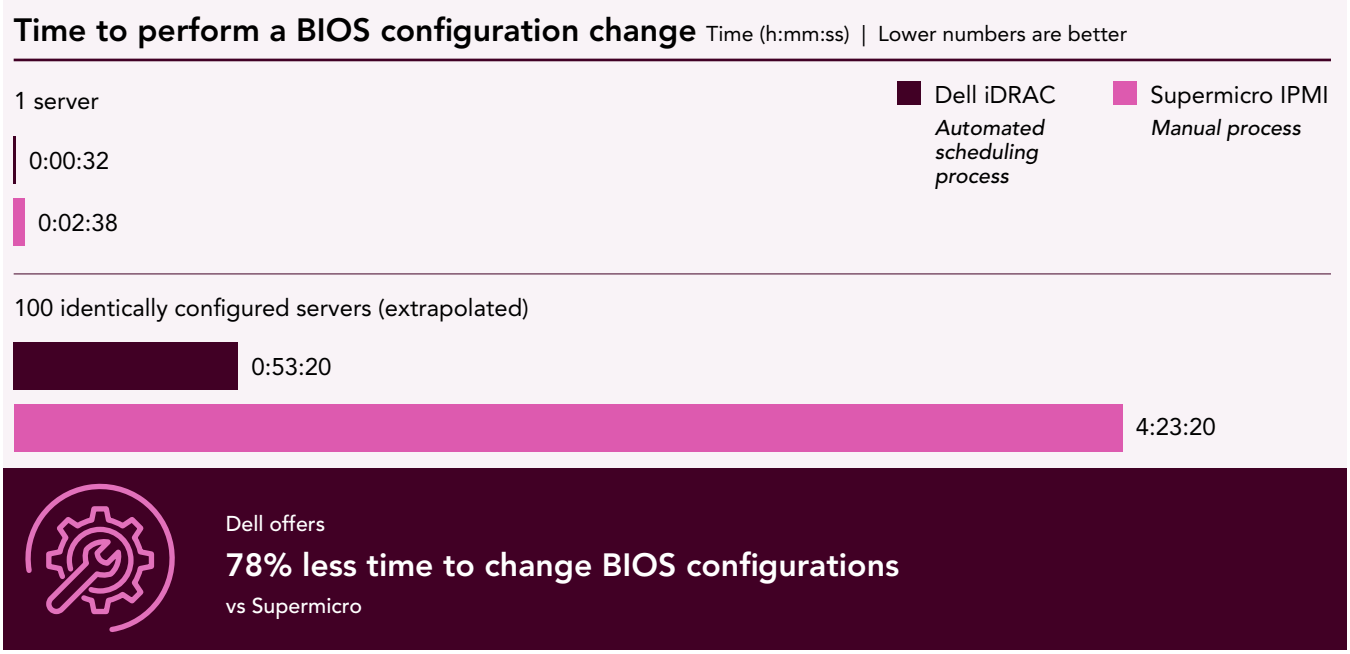

Figure 4: Time to perform a BIOS configuration change on both a single server and 100 identically configured servers (extrapolated). Lower is better. Source: Principled Technologies.

About iDRAC9

Dell PowerEdge™ servers include the Integrated Dell Remote Access Controller 9 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
- Strong security features and options[14]

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

Automated firmware and driver updates

iDRAC

Unlike Supermicro IPMI, Dell iDRAC lets you schedule automatic firmware updates. This means that configuring automatic updates on a schedule is a one-time task that would save time on every update cycle. Figure 5 shows the extrapolated time to schedule automatic firmware updates for the first time for 100 servers using Dell iDRAC and Supermicro IPMI. The manual process using the Supermicro tool takes **an extra 13 minutes** than setting up the automated process in iDRAC.

If we assume an administrator sets up a monthly schedule on the first Saturday night of each month, an admin using iDRAC would have a one-time time investment of 58 seconds per server. For 100 servers, this comes out to 1 hour, 36 minutes, 40 seconds as a one-time setup. In comparison, an admin using Supermicro IPMI would have an investment of 1 hour and 50 minutes for 100 servers in each maintenance window. If we compare the one-time setup for iDRAC and the first of many setup times for Supermicro IPMI, the Dell management tool saves about 13 minutes, 20 seconds. (See Figure 5.)

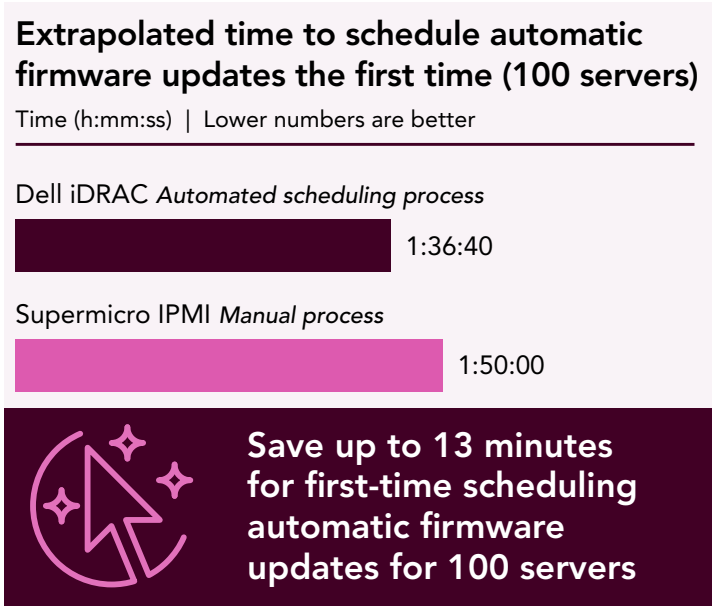

Figure 5: Extrapolated time to update firmware on 100 servers the first time. Lower is better. Source: Principled Technologies.

However, the second time, and every subsequent time, **Dell saves 110 minutes because it is no longer necessary for the admin to perform the task**. (See Figure 6.) This time savings occurs even if the 100 servers are not identically configured. Please note that these times include only the uploading of the firmware to the BMC, and do not reflect the download and extraction times for the Supermicro firmware.

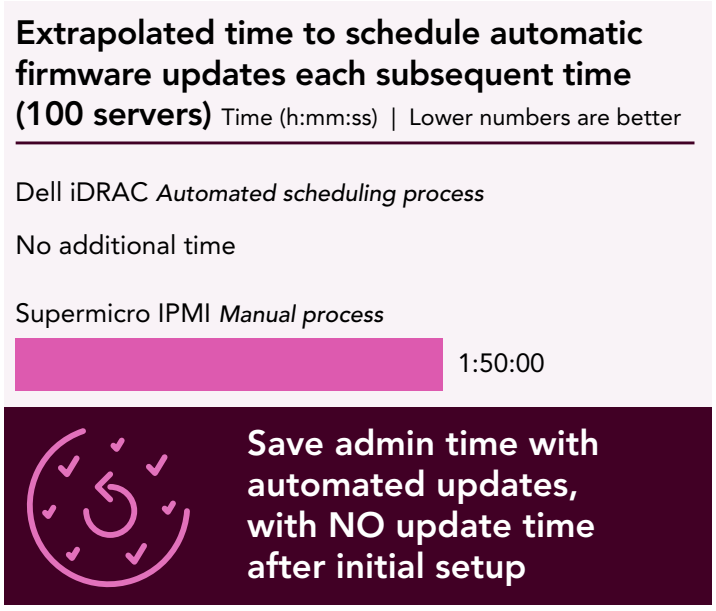

Figure 6: Extrapolated time to update firmware on 100 servers every subsequent time. Lower is better. Source: Principled Technologies.

OME

Dell OME supports **firmware updates for all components** and Windows driver updates. SSM supports BIOS and BMC firmware updating, but **not driver updates, or updating of other components**.

Conclusion

Choosing a vendor for server purchases is about more than just the hardware platform. Decision-makers must also consider more long-term concerns, including system/data security, energy efficiency, and ease of management. These concerns make the systems management tools a vendor offers as important as the hardware.

We investigated the features and capabilities of server management tools from Dell and Supermicro, comparing Dell iDRAC9 against Supermicro IPMI for embedded server management and Dell OpenManage Enterprise and CloudIQ against Supermicro Server Manager for one-to-many device and console management and monitoring. We found that the Dell management tools provided more comprehensive security, sustainability, and management/monitoring features and capabilities than Supermicro servers did. In addition, Dell tools automated more tasks to ease server management, resulting in significant time savings for administrators versus having to do the same tasks manually with Supermicro tools.

When making a server purchase, a vendor's associated management products are critical to protect data, support a more sustainable environment, and to ease the maintenance of systems. Our tests and research showed that the Dell management portfolio for PowerEdge servers offered more features to help organizations meet these goals than the comparable Supermicro management products.

1. Steve Morgan, "Cybercrime To Cost The World $10.5 Trillion Annually By 2025," accessed February 15, 2024, https://cybersecurityventures.com/cybercrime-damages-6-trillion-by-2021/.
2. Dell, "Using iDRAC9 RSA SecurID 2FA," accessed February 15, 2024, https://dl.dell.com/Manuals/Common/dellemc-idrac9-rsa-securid-2fa.pdf.
3. Dell, "Dell EMC OpenManage Enterprise SupportAssist Version 1.1 User's Guide," accessed February 15, 2024, https://www.dell.com/support/manuals/en-us/openmanage-enterprise-supportassist/omesapuserguide11/role-and-scope-based-access-control-in-openmanage-enterprise?.
4. Dell, "Dell EMC OpenManage Enterprise SupportAssist Version 1.1 User's Guide."
5. Dell, "OpenManage Enterprise 4.0: iDRAC Password Management and Rotation," accessed February 15, 2024, https://www.dell.com/support/kbdoc/en-us/000219279/openmanage-enterprise-4-0-idrac-password-management-and-rotation.
6. Dell, "OpenManage Portfolio Software Licensing Guide," accessed April 3, 2024, https://www.delltechnologies.com/asset/en-us/products/servers/industry-market/openmanage-portfolio-software-licensing-guide.pdf.
7. Mark Maclean and Kyle Shannon, "Dell CloudIQ Cybersecurity For PowerEdge: The Benefits Of Automation," accessed February 15, 2024, https://infohub.delltechnologies.com/en-US/p/dell-cloudiq-cybersecurity-for-poweredge-the-benefits-of-automation/.
8. Dell, "Security Advisories," accessed February 15, 2024, https://infohub.delltechnologies.com/en-US/l/cloudiq-a-detailed-review/security-advisories/.
9. Dell, "Dell CloudIQ - AIOps for Intelligent IT Infrastructure Insights," accessed February 15, 2024, https://www.dell.com/en-us/dt/solutions/cloudiq.htm
10. Principled Technologies, "Dell CloudIQ provides a single console for proactive monitoring and had negligible impact on network bandwidth in our tests," accessed January 17, 2024, https://www.principledtechnologies.com/dell/CloudIQ-network-0422.pdf.
11. Supermicro, "X13DEM User's Manual," accessed February 16, 2024, https://www.supermicro.com/manuals/motherboard/X13/MNL-2407.pdf.
12. Dell, "OpenManage Enterprise," accessed December 20, 2023, https://www.dell.com/en-us/work/learn/openmanage-enterprise.
13. Principled Technologies, "A Dell PowerEdge MX environment using OpenManage Enterprise and OpenManage Enterprise Modular can make life easier for administrators," accessed January 17, 2024, https://www.principledtechnologies.com/Dell/PowerEdge-MX-OME-OME-M-0124.pdf.
14. "Integrated Dell Remote Access Controller (iDRAC)," accessed January 16, 2024, https://www.dell.com/en-us/lp/dt/open-manage-idrac.

Read the science behind this report ▶

This project was commissioned by Dell Technologies.