Technical Research Report

PROWESS

Smarter IT Operations with Dell Technologies Server Management Tools

This report compares Dell and Supermicro server management portfolios to identify which tools deliver superior efficiency and control in data center security, ease of use, analytics, and sustainability.

Executive Summary

As data center environments grow, so do the stakes: more servers, more workloads, and zero tolerance for downtime or security gaps. To stay ahead, IT teams depend on effective server management tools that turn complexity into control by applying safeguards, deploying systems, and resolving issues efficiently at scale.

In this report, Prowess Consulting compares Dell and Supermicro server management tools across four key areas: **security**, **ease of use**, **analytics**, and **sustainability**.

Because AIOps stands out as an offering from Dell with no equivalent from Supermicro, we also evaluate the capabilities of AIOps independently of the four functional areas.

To demonstrate how small per-server differences can compound into hours of extra effort in larger environments, this report scales out test results to emulate a 100-server data center. Our findings indicate that Dell solutions provided measurable advantages across the four areas in automation, visibility, and integration, resulting in streamlined workflows, deeper visibility, and actionable sustainability insights. As environments scale, these operational efficiencies can lead to measurable return on investment (ROI) improvements through reduced licensing costs, faster deployment cycles, and a lower total cost of ownership (TCO).

Highlights

Prowess Consulting found that, compared to Supermicro, Dell server management tools can provide up to:

8x more security features to strengthen protection of critical systems (with Dell vs. Supermicro server management tools)

44x faster server deployment (with OME vs. SSM)

3.7x more GPU metrics and advanced system insights to help optimize AI workloads (with iDRAC10 vs. IPMI)

13x more power management reports to monitor energy use and carbon impact (with OME vs. SSM)

Table 1 | Summary of Dell and Supermicro server management tools (see Appendix A: Glossary for more information)

Feature	Dell Technologies	Supermicro
Embedded/remote server management	Integrated Dell™ Remote Access Controller 10 (iDRAC10)	Supermicro® Intelligent Platform Management Interface 2.0 (IPMI)
One-to-many device management console	Dell OpenManage™ Enterprise (OME)	Supermicro Server Manager (SSM)
Cloud-based monitoring	Dell Artificial Intelligence for IT Operations (AIOps)	*No equivalent*

Why Effective Server Management Tools Matter

Modern data centers demand tools that help administrators manage growing environments with speed and consistency. Small inefficiencies on a single server can scale into hours of repetitive work across a server environment, while gaps in security, configuration control, or visibility can introduce real operational risks. Strong management platforms can counter these risks by centralizing workflows, automating routine tasks, and surfacing issues before they escalate.

Testing Server Management Features and Capabilities

For this report, we performed testing to evaluate features within the Dell and Supermicro management tools that influence day-to-day operational efficiency, configuration integrity, energy consumption, and long-term security posture. Together, these factors help determine an organization's TCO and ROI, forming the true business value of the organization's IT infrastructure.

We tested the real-world effort to complete common admin tasks on Dell and Supermicro server management platforms. For each task, we ran live workflows and measured steps and time to completion. This matters because repetitive work increases error risk and limits scale. We then extrapolated our results to a 100-server environment to show how small per-task differences add hours of effort. For a full description of the steps taken for our comparisons, refer to the **Methodology** document.

Security Features: Reducing Risk Through Consistent Control

Organizations face increasing threats, making extensive security capabilities essential. Beyond protecting sensitive data, hardware with robust built-in security features helps reduce the time administrators spend performing routine security tasks, freeing them to focus on strategic initiatives, protect data, and prevent costly attacks. Our results show that Dell server management tools help harden enterprise infrastructure with more security-related features than Supermicro's tools. Additional coverage of the security features we tested is in **Appendix C: Testing Data**.

Dynamic USB Port Control

Controlling physical USB access is a key safeguard against unauthorized devices, malware insertion, and unintended configuration changes. This capability forms a key layer of protection for equipment that is co-located within shared environments. With iDRAC10, administrators can enable or disable front USB ports directly from the management interface. The initial change requires a one-time reboot, but it can be staged and applied during a scheduled maintenance window to avoid unplanned downtime; after that, subsequent front USB changes through iDRAC10 are applied live with no reboot required.

In our testing, staging this change with iDRAC10 took 4 steps and 9 seconds once the feature was enabled. By contrast, IPMI exposes USB port control only through the BIOS and forces an immediate, unscheduled reboot to apply the change, an 8-step workflow taking 4 minutes and 25 seconds. For this task, iDRAC10 delivered up to 96% time savings compared to IPMI.

At the scale of 100 servers, the ability to align USB-port changes with planned maintenance windows could eliminate more than 7.1 hours of avoidable administrative disruption and reduce the operational risk associated with unscheduled reboots.

Up to **96% less admin time to dynamically lock down** front USB ports and protect against unauthorized devices with iDRAC10 vs. IPMI

Two-Factor Authentication via RSA

Support for enterprise authentication platforms helps organizations apply consistent access controls across infrastructure and align server management with broader security policies. Strong authentication reduces the risk of unauthorized access to sensitive management interfaces. iDRAC10 supports two-factor authentication using RSA® SecurID®, providing hardware-backed, enterprise-grade authentication for server management access. RSA SecurID is widely deployed in enterprise environments as a privileged access standard, particularly for out-of-band management interfaces like baseboard management controllers (BMCs), where a compromised credential can grant full hardware-level control independent of the operating system. Supermicro uses RADIUS® to support two-factor authentication, but it lacks support for RSA-based authentication. As a result, organizations that standardize on RSA SecurID for privileged access cannot enforce the same authentication model across Supermicro tools.

BIOS Live Scanning

Firmware integrity is a foundational security requirement. iDRAC10 includes BIOS live scanning, which verifies BIOS integrity during normal operation and records results in Dell Lifecycle Controller, helping administrators detect tampering or corruption early without downtime.

Supermicro tools do not offer an equivalent BIOS integrity verification feature, increasing the risk that firmware issues go unnoticed until they create operational or security incidents.

Credential Management

Managing privileged credentials across large data centers is difficult to do safely and consistently by hand; manual password updates are labor-intensive and error-prone, and they can create windows during which stale or inconsistent credentials can be exploited. OME mitigates this risk with centralized credential management, including automated rotation of iDRAC passwords either natively in OME or via integration with external platforms such as CyberArk®. CyberArk is a widely adopted privileged access management (PAM) platform that many enterprises already use to govern credentials across their broader IT environments; native integration with OME means that server management credentials can participate in the same vaulting, rotation, and audit workflows rather than existing as a separate, manually managed credential silo. This capability reduces administrative overhead, shrinks the attack surface, and helps ensure consistent enforcement of security policies at scale.

By contrast, SSM offers no comparable credential-management capability. Administrators must manage credentials manually on individual systems or rely on external processes, which can increase operational effort, drive inconsistency, and make it significantly harder to sustain strong, uniform security controls as environments scale.

Scope-Based Access Control (SBAC)

As environments grow, who can access which systems becomes as important as what they are allowed to do on those systems. For organizations, this level of control directly impacts risk, compliance, and operational agility, and it can limit the potential of internal bad actors. OME supports SBAC, enabling administrators to apply the same role to multiple users while scoping each user's access to specific server groups. Users can see and control only the systems they own, which mitigates over-privileged accounts, simplifies delegation to regional or line-of-business (LOB) teams, and makes least-access enforcement practical at scale.

SSM is limited to role-based access control (RBAC). While RBAC defines what a role can do, it 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.

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

Security Feature	Dell	Supermicro	Business Impact Summary
Dynamic USB Ports	Supported	Limited (reboot required for each enablement/ disablement)	iDRAC10 supports the ability to enable/disable USB port changes in just 4 steps and 9 seconds, with only one scheduled reboot upfront. In contrast, IPMI requires 8 steps and 4 minutes, 25 seconds per change, along with a server reboot for every adjustment. Across 100 servers, this adds up to a time savings of 7.1 hours, while reducing the risk of unauthorized access, ensuring faster implementation of security policies.
Two-Factor Authentication via RSA	Supported	Not supported	iDRAC10 provides enterprise-grade security with RSA SecurID two-factor authentication for server management, ensuring consistent and robust access control across environments and reducing the risk of unauthorized access. IPMI supports RADIUS-based two-factor authentication only and lacks RSA integration, limiting consistent access control across the environment and creating potential gaps in security standardization.
BIOS Live Scanning	Supported	Not supported	iDRAC10 identifies threats before they escalate by continuously scanning the BIOS during normal operation, enabling early detection of firmware tampering without causing downtime. IPMI lacks continuous integrity checks, leaving environments more exposed to undetected vulnerabilities.
Credential Management	Supported	Not supported	OME helps secure servers with centralized credential management and automated iDRAC password rotation via CyberArk integration. SSM lacks these features, increasing vulnerability to breaches.
Scope-Based Access Control (SBAC)	Supported	Not supported	OME supports both SBAC and RBAC, which provide precise, server group-specific permissions, reducing security risks. The broader SSM RBAC-only model can increase exposure to over-permissioning as environments scale.
Centralized Identity and Access Management	Supported	Not supported	OME integrates with OpenID® Connect (OIDC) providers like PingFederate and Keycloak, enabling SBAC for secure, scalable access control. SSM lacks OIDC and SBAC support, complicating scalable access control and audits and increasing security vulnerabilities.

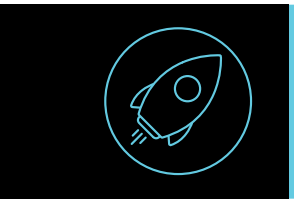
Ease of Use Features: Streamlining Work at Scale

As IT environments expand in size and complexity, management tools must simplify configuration, maintenance, and consistency across server environments. Platforms that optimize these workflows not only reduce administrative overhead but also improve operational efficiency, enabling IT teams to scale effectively while minimizing downtime. The following sections highlight the most impactful ease of use features for businesses. For additional details on the ease of use features we tested, see **Appendix C: Testing Data**.

Full-System BIOS Configuration

Staging BIOS changes through iDRAC10 lets administrators push configuration updates from the management console and apply them automatically at the next scheduled reboot, eliminating most manual console work, reducing restart oversight, and improving configuration consistency.

iDRAC10 supports more than 100 configurable BIOS settings directly from the management interface. In contrast, IPMI exposes only a single system information view, forcing administrators into manual BIOS access for most changes. In our tests, staging a BIOS change with iDRAC10 required 5 steps and 17 seconds, making it 15x faster than using IPMI, which required 4 steps, a reboot, and 4 minutes, 26 seconds for the same tests. At a 100-server scale, the Dell workflow saves more than 6.9 hours of administrative time while reducing configuration variability across the environment.



Configure BIOS settings **15x faster, reducing maintenance downtime and improving configuration consistency** with iDRAC10 vs. IPMI

Automatic Firmware Updates

As server infrastructure grows, keeping firmware up to date can quickly become a time sink. Automating the process can eliminate repetitive manual work and reduce the chance of missed updates.

With iDRAC10, you can define your update policy once and schedule and automate firmware updates across many servers at once, taking just 13 seconds per server. OME supports automated firmware and driver updates that eliminate the need for you to manually locate update files and upload them to each system, taking only 68 seconds one time to create the firmware repository. IPMI, by contrast, offers no automation and requires manual firmware uploads every update cycle, requiring 91 seconds per server, while SSM requires 116 seconds per server to manually source and upload firmware files for updates.

Up to **7x faster firmware updates** and **reduce update time by up to 41%** with OME and iDRAC10 vs. SSM and IPMI

Alert-Based Automated Actions

Ease of use at scale depends on reducing repeat work. OME supports alert-based automation that allows administrators to define actions once and apply them automatically when conditions are met. These policies can trigger remediation steps or scripts across groups of servers without manual intervention, reducing admin effort by up to 100% after an initial setup of 11 steps and 32 seconds.

SSM supports alert notifications but does not support automated actions in response to alerts. Administrators must review alerts and take corrective action manually on each affected system, taking 8 steps and 17 seconds per alert.

Enabling one-to-many automation reduces repetitive tasks and helps teams respond to issues more quickly and consistently across large environments.

Eliminate manual intervention and automate response time 100% with OME vs. SSM

Configuration Template Deployments

Consistent configuration is critical when deploying servers at scale. OME supports template-based deployments that include the BMC, BIOS, storage, and networking settings. Administrators can create a reusable template and apply it across multiple systems, which can help reduce setup time and configuration drift, requiring up to 98% fewer steps and up to 97% less time than SSM, which translates to 44x faster server deployment.

Supermicro management tools support templates primarily at the BMC and BIOS level, and BIOS settings must often be tailored to specific motherboard models. This limitation reduces template reuse and increases the need for manual intervention in mixed or evolving environments.

Up to **98% fewer steps** and up to **97% less time** with full-system configuration profiles with OME vs. SSM

Report Builder with Customization

Analytics are only useful if teams can easily review and share results. OME provides a built-in report builder with 52 predefined reports and options for customization, scheduling, and automated distribution. These reports cover performance, GPU activity, power usage, and inventory data, allowing administrators to generate repeatable insights without manual data extraction.

SSM provides a limited set of 13 predefined reports with no customization. This limitation increases the effort required to produce consistent analytics outputs, and it can slow planning or review processes in larger environments.

Centralized reporting allows administrators to track trends, compare systems, and support operational planning with less manual effort.

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

Ease of Use Feature	Dell	Supermicro	Business Impact Summary
Full-System BIOS Configuration	Supported	Limited	iDRAC10 streamlines BIOS configuration with access to more than 100 settings, enabling changes in just 5 steps and 17 seconds. IPMI takes 4 steps and 4 minutes, 26 seconds per server, and it mandates an immediate reboot for every BIOS change. iDRAC10 provides a time savings of 6.9 hours across a 100-server environment.
Automatic Firmware Updates	Supported	Not supported	iDRAC10 simplifies firmware updates with automated processes that take just 13 seconds per server, whereas IPMI requires manual uploads at 91 seconds per server. This time savings adds up to more than 2 hours across 100 servers (1.3 minutes per server), freeing administrators from repetitive tasks and reducing the risk of errors.
Import/Export Full Server Configuration Profile	Supported	Limited	iDRAC10 offers full server profile import/export across BIOS, storage, and network settings, saving IT administrators up to 21.5 hours per 100 servers and completing the task up to 21x faster than the limited IPMI BMC-only support.
Connection View	Supported	Limited	iDRAC10 Connection View maps server network ports to switch ports, improving troubleshooting efficiency by enabling remote cabling diagnosis. IPMI lacks this, often requiring on-site troubleshooting for multi-rack or remote setups.
Alert-Based Automated Actions	Supported	Limited/ manual	Cut admin effort by up to 100% with automated alert responses that improve response speed and consistency at scale with OME versus 8 steps and 17 seconds per alert for administrators to manually address each alert with SSM.

Ease of Use Feature	Dell	Supermicro	Business Impact Summary
HTML5-Based Management Interface	Supported	Limited	OME uses an HTML5-based interface for all management functions, including console access. SSM relies on a hybrid Java® Runtime Environment (JRE) and HTML interface, increasing access friction and maintenance overhead and slowing down workflows for administrators.
Preconfigured Virtual Appliance Deployment	Supported	Limited	OME is provided as a preconfigured virtual appliance available in 7 form factors for easy deployment on major hypervisors, tailored to different environments; SSM installs on Windows® or Linux® and requires manual configuration, adding complexity and increasing ongoing maintenance.
Heterogeneous Server Monitoring	Supported	Not supported	OME monitors multi-vendor servers in a single interface, reducing admin effort and streamlining operations. SSM only supports Supermicro servers, requiring extra tools for any servers from other manufacturers, which adds complexity and inefficiency.
Third-Party Integration Support	Supported	Limited	OME provides 5 third-party integrations and a VMware vCenter® plugin with 18 features for more centralized workflows and a more unified, time-saving management experience. SSM provides only 3 integrations and a vCenter plugin with just 8 features, limiting efficiency.
Mobile Integration	Supported	Not supported	OME enables administrators to monitor and perform basic management tasks directly from their mobile devices; SSM lacks comparable mobile management capabilities, limiting flexibility.
Configuration Template Deployments	Supported	Limited	OME template-based deployments for BMC, BIOS, storage, and networking ensure consistent server management while reducing admin effort, requiring up to 98% fewer steps and up to 97% less time than SSM, which translates to 44x faster server deployment.
Firmware and Driver Updates	Supported	Limited	OME automates firmware and driver updates, eliminating manual file uploads. Pre-staged workflows reduce update time by up to 41% with up to 98% fewer steps across 100 servers compared to manual updates with SSM.
Report Builder with Customization	Supported	Limited/ manual	OME offers 52 customizable, automated reports, 4x more than the 13 static reports offered by SSM. This reduces admin effort while providing deeper insights into performance, GPU activity, power, and inventory.

Analytics Features: Improving Visibility and Insight

Strong analytics features can help administrators understand system behavior, identify emerging issues, and make better decisions at scale. Our testing examined the depth and accessibility of the analytics capabilities available through iDRAC10 and the broader Dell portfolio, compared to the tools Supermicro offers. The results show meaningful differences in visibility and operational value. For additional details on the analytics features we tested, see **Appendix C: Testing Data**.

Telemetry Streaming

Broad telemetry access allows teams to collect detailed server data and analyze trends over time. iDRAC10 supports automatic telemetry streaming through a built-in configuration workflow, and it provides 32 reports across 12 categories with 285 metrics. Administrators can stream sensor, thermal, and hardware data to external analytics platforms for real-time monitoring or historical analysis.

By contrast, IPMI supports limited telemetry streaming only, which consists of administrators pulling a limited set of telemetry metrics via custom scripting. As a result, teams using Supermicro tools must rely on data collection or limited built-in views with just 10 reports across 3 categories with 17 metrics, which can restrict their ability to centralize data and perform deeper analysis at scale.

GPU Metrics and Visibility

Clear visibility into GPU activity is essential for environments running AI, machine learning (ML), or high-performance computing (HPC) workloads. iDRAC10 exposes 33 GPU-related metrics, including inventory data, utilization, thermal readings, and device health indicators. These metrics give administrators detailed insight into how GPUs behave under load.

IPMI exposes just 9 GPU-related values. This reduced visibility can make it harder to identify bottlenecks, detect abnormal behavior, or optimize GPU-intensive workloads. For organizations planning or operating AI infrastructure, the difference in available metrics can directly affect monitoring accuracy and tuning efficiency.

More than **3.7x the GPU metrics** and **deeper accelerator visibility** with iDRAC10 vs. IPMI

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

Analytics Feature	Dell	Supermicro	Business Impact Summary
Telemetry Streaming	Supported	Limited	iDRAC10 telemetry streaming provides 32 reports across 12 categories with 285 metrics, enabling centralized analysis of sensor, thermal, and hardware data. IPMI offers 10 reports across 3 categories with 17 metrics.
GPU Metrics and Visibility	Supported	Limited	iDRAC10 provides visibility into 33 GPU metrics, enabling more accurate monitoring of AI and HPC workloads. IPMI offers only 9 GPU metrics, limiting insight into accelerator behavior.

Sustainability Features: Managing Power and Efficiency at Scale

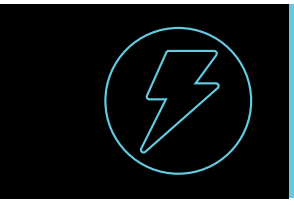
As server environments grow, power consumption and thermal management become operational constraints, not abstract sustainability goals. Administrators must understand how systems consume energy, identify inefficiencies, and apply controls consistently across hundreds of servers. Management tools that expose accurate power data and automate corrective actions can help teams reduce waste, manage capacity, and plan infrastructure growth more effectively. For additional details on the sustainability features we tested, see **Appendix C: Testing Data**.

Power Management Reporting

Reporting turns raw data into actionable insight. OME includes more than 27 built-in reports specific to OME Power Management, with options to customize, schedule, and automatically distribute those reports. These reports support tasks such as energy planning, capacity analysis, and long-term optimization without requiring manual data extraction.

SSM provides only 2 basic power-related reports and does not support comparable customization or automation. This limits its usefulness for organizations that need repeatable reporting to support planning or compliance initiatives.

With OME Power Management, administrators can generate consistent sustainability reports across large server environments with minimal effort, reducing manual work and improving decision-making.



Access more than **13x the built-in power and energy reports** and **repeatable sustainability reporting** with OME Power Management vs. SSM

Power Usage Metrics and Visibility

Effective sustainability management depends on visibility. OME Power Management exposes 22 power- and energy-related metrics at the individual server level, including power consumption, thermal data, system utilization, and component-level measurements. These metrics provide administrators with a fast means of seeing how resources are used across the infrastructure.

SSM exposes only 3 power metrics, limiting insight into server behavior and reducing the ability to diagnose inefficiencies.

OME Power Management also provides quick access to 8 dashboard views that surface key sustainability data without requiring report creation. Administrators can quickly identify power and temperature offenders, underutilized racks, idle servers, and available headroom directly from the interface. SSM provides only 4 summary views and requires additional navigation to access comparable information.

This difference in accessibility matters at scale. When sustainability data is immediately visible, administrators can act sooner and with greater confidence.

OME Power Management **turns real server energy data into carbon emissions insights with configurable factors**. SSM offers no native equivalent.

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

Sustainability Feature	Dell	Supermicro	Business Impact Summary
Power Management Reporting	Supported	Limited	OME Power Management provides more than 27 built-in, customizable reports for detailed energy planning and sustainability tracking, whereas SSM provides only 2 basic, less-flexible power-related reports.
Power Usage Metrics (Per-Server Visibility)	Supported	Limited	OME Power Management provides more than 7x more power and energy metrics per server (22 versus 3) and 2x more dashboard views (8 versus 4) compared to SSM, offering significantly greater visibility into system inefficiencies and usage.
Carbon Emissions Analysis and Capacity Planning	Supported	Not supported	OME Power Management offers carbon emissions analysis from actual server energy use with configurable factors. SSM lacks native, real-world carbon emissions analysis.
Automated Power and Thermal Management Policies	Supported	Limited	OME Power Management offers static power capping and temperature-triggered automation for individual or group servers. SSM only supports basic power threshold policies, lacking temperature-triggered automation.
Power and Thermal Data	Supported	Limited	OME Power Management dashboards provide comprehensive quick access views into power and thermal conditions, including power offenders, temperature offenders, idle servers, underutilized racks, and available headroom. SSM provides fewer summary views, requiring more time to identify and address sustainability-related issues.

AIOps: Scaling Operations Through Centralized Analytics

As server environments grow in size and complexity, administrators need more than per-system monitoring to maintain performance, efficiency, and control. Centralized analytics tools can help teams aggregate telemetry, identify patterns, and surface issues that are difficult to detect when systems are managed individually. By extending visibility beyond the management console, centralized analytics platforms can reduce manual analysis, improve decision-making, and support proactive operations at scale. Additional details on the AIOps features validated in this report are provided in **Appendix C: Testing Data**.

Performance Metrics with Anomaly Detection

Monitoring performance metrics is most effective when tools can identify abnormal behavior automatically. AIOps analyzes performance data across CPU, memory, storage, and network resources and applies anomaly detection to highlight deviations from normal operating patterns. This approach reduces the need for administrators to manually define thresholds or review metrics server by server.

By identifying unusual behavior early, analytics with anomaly detection can help teams investigate issues before they escalate into outages or performance degradation.

Server-Level GPU Utilization

GPU resources are increasingly critical and expensive, making efficient use essential. AIOps provides server-level GPU utilization metrics that show how accelerators are consumed across workloads and over time. These metrics help administrators identify underused resources, detect imbalances, and understand utilization patterns without relying on per-system inspection.

Surfacing GPU utilization clearly at the server level can help teams get more value from accelerator investments in complex environments.

Carbon Footprint Analysis

Linking energy usage with carbon impact is critical for credible sustainability reporting and planning. AIOps provides built-in carbon footprint analysis, presenting a summary and system- and workload-level views of energy consumption and associated emissions so teams can see exactly how power usage translates into environmental impact across their data centers.

By consolidating energy and carbon metrics in a single interface, Dell helps organizations assess impact more clearly, track progress against sustainability goals, and make informed capacity and investment decisions as environments scale.

Table 6 | AIOps capabilities

Feature Area	Feature	Business Impact Summary
Security	Cybersecurity Advisories	AIOps offers centralized security and configuration visibility with advisory insights, reducing risks across your data center.
Security	Policy-Based Security Configuration (PBSC)	AIOps enables PBSC, ensuring consistent infrastructure protection and rapid issue resolution.
Ease of Use	Multiple Performance Reports	AIOps offers extensive performance reporting for environment visibility and faster decisions.
Ease of Use	Generative AI (GenAI) Assistant	AIOps features a GenAI assistant that streamlines analytics and boosts usability, helping administrators find insights faster and reducing interface learning time.
Analytics	Performance Metrics with Anomaly Detection	AIOps tracks CPU, memory, storage, and network metrics, using built-in anomaly detection.
Analytics	Server-Level GPU Utilization	AIOps provides server-level GPU utilization metrics that help administrators understand how accelerators are being used across workloads. This visibility supports better resource planning and tuning.
Sustainability	Carbon Footprint Analysis	AIOps provides near-real-time, audit-ready carbon footprint analysis by correlating live energy data with system- and workload-level emissions, reducing reliance on static estimates or external audits.

Business Value

In this report, Dell demonstrates broader capability coverage, more efficient workflows, and deeper visibility than the Supermicro server management tools examined.

Together, Dell server management tools form an integrated server management portfolio that supports embedded control, data center–level operations, and analytics at scale. While both Dell and Supermicro offer enterprise-ready management tools, our testing showed that Dell delivers greater automation, broader telemetry access, and more consistent operational workflows across the server lifecycle.

Across the areas validated in this report, Dell's server management portfolio delivers the following operational benefits:

- **Security:** iDRAC10, OME, and AIOps support layered security controls, including dynamic USB port management, two-factor authentication with RSA, BIOS integrity verification, centralized visibility, and policy-based configuration. These capabilities can help reduce risk, limit configuration drift, and apply safeguards more consistently across large environments.
- **Ease of use:** iDRAC10 and OME reduce repetitive administrative work through staged BIOS configuration, automated firmware updates, reusable configuration templates, and alert-based automation. When applied across environments of 100 servers or more, these efficiencies can save hours of administrative time and improve operational consistency.
- **Analytics:** iDRAC10 and AIOps provide broad telemetry access, richer GPU metrics, anomaly detection, and environment-level analytics that extend visibility beyond individual systems. Supermicro's tools expose fewer metrics, and Supermicro does not offer an equivalent tool to AIOps, which limits insight at scale.
- **Sustainability:** OME Power Management and AIOps deliver deeper power and energy visibility, automated power and thermal policies, carbon emissions analysis, and robust reporting. These capabilities help organizations understand and manage energy use more effectively as environments grow.

We found that these strengths position Dell to help organizations manage server environments more efficiently, reduce operational overhead, and maintain consistent control as infrastructure scales.

FAQ

1. Who should read this report?

The intended audience for this report includes server administrators and IT decision-makers (ITDMs) in enterprises and also in upper- and mid-market organizations who are evaluating server platforms and management solutions. In addition, business decision-makers (BDMs) will find the report useful because they have IT-purchase authority and can influence platform selection based on cost, operational efficiency, and risk.

2. What was the primary goal of this report?

The main goal of this report was to compare the practical server management capabilities of Dell and Supermicro tools. Prowess Consulting's analysis focused on how each vendor's tools affect day-to-day administration across four core areas: security, ease of use, analytics, and sustainability. Rather than catalog every feature, the report highlights where differences in design and automation change how much effort administrators must invest to manage server environments at scale.

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

On the Dell side, we evaluated iDRAC10, OME, and AIOps as part of the broader Dell server management portfolio. On the Supermicro side, we examined IPMI for embedded management and SSM for one-to-many management. Our comparisons focused on validated features that directly affect routine administration, such as USB control, BIOS configuration, firmware updates, telemetry, and GPU visibility.

4. What testing methodology did Prowess Consulting use?

We used hands-on testing that measured the number of steps and the time required to complete common administrative tasks on each platform; in addition, we also reviewed documentation for the various tools. For each validated scenario, we documented the workflows in the actual management interfaces, and we then extrapolated the measured effort from a single server to an environment of 100 servers. This approach emphasizes operational scale and helps illustrate how small per-server differences can add up to significant time savings or additional effort in larger environments.

5. Why does the report include AIOps if Supermicro has no direct equivalent?
AIOps is part of the Dell server management portfolio and plays an important role in how customers can monitor and analyze server environments at scale. Even though Supermicro does not offer a comparable platform, excluding AIOps would under-represent the capabilities available to Dell customers. In this report, AIOps is presented as an additional analytics and visibility layer for Dell environments, and we validated its capabilities independently rather than using it for head-to-head claims.

6. What were the key findings of the comparison between Dell and Supermicro server management tools?
Across the areas tested, we found that Dell's tools delivered broader security coverage, more efficient configuration workflows, and deeper analytics than the Supermicro tools we examined. At the embedded management layer, iDRAC10 enables faster USB control, stronger authentication options, and BIOS integrity verification. At the one-to-many management layer, OME simplifies BIOS configuration, firmware updates, and server profile deployment across environments. For analytics, AIOps extends visibility with telemetry streaming, richer GPU metrics, and environment-wide insights that are not available in Supermicro's server management portfolio.

7. How do these findings benefit IT administrators and decision-makers?
For IT administrators, our findings show where they can reduce repetitive work, shorten maintenance windows, and gain better visibility into system behavior. Features such as full-system BIOS configuration from the BMC, scheduled automatic firmware updates, and full server profile import/export can save hours of manual effort across an environment. For decision-makers, these efficiencies support stronger security postures, more consistent operations, and better ROI and TCO, which can influence long-term infrastructure planning and platform selection.

8. How does this report relate to AI, GPU workloads, and modern analytics needs?
Many organizations now run GPU-intensive workloads for AI, ML, and HPC. iDRAC10 exposes a broad set of GPU-related metrics that can help administrators monitor accelerator health and utilization at the server level. AIOps extends this visibility across environments by aggregating telemetry, surfacing performance trends, and providing additional tools, such as a built-in GenAI assistant to help administrators navigate analytics and interpret platform data more efficiently. Supermicro's tools expose fewer GPU metrics and do not offer an equivalent tool to AIOps or the GenAI assistant, which can limit GPU-specific visibility and analytics at scale.

Appendix A: Glossary

Automatic telemetry streaming is a feature in iDRAC10 that sends detailed server data, such as sensor readings, thermal metrics, and event logs, to external analytics tools. IPMI does not support automatic telemetry streaming.

Baseboard management controller (BMC) is the embedded controller that provides out-of-band management functionality for a server. iDRAC10 and IPMI both operate as BMCs, though they offer different feature sets.

BIOS live scanning is a security feature in iDRAC10 that verifies the integrity of the BIOS image during normal system operation. It helps detect tampering or corruption without requiring a reboot.

Connection View is a visualization feature in iDRAC10 that maps server network ports to the upstream switch ports. It helps administrators diagnose cabling issues without requiring on-site inspection. Supermicro tools do not provide a comparable view.

Dell Artificial Intelligence for IT Operations (AIOps) is a cloud-based analytics and observability layer for Dell environments. It centralizes health, performance, and configuration data across multiple sites to help administrators identify issues earlier and maintain awareness of distributed server environments. Supermicro does not offer an equivalent platform.

Dell OpenManage Enterprise (OME) is the Dell one-to-many management console for Dell PowerEdge™ servers. It offers centralized configuration, reporting, firmware management, and integration with AIOps.

Firmware update scheduling is a feature in iDRAC10 that automates firmware updates on a set schedule. It reduces repetitive manual work and helps maintain consistent patch levels across a server environment. IPMI does not support automated scheduling.

GPU metrics are a set of measurement values exposed for PowerEdge servers by iDRAC10 that describe GPU health, temperature, utilization, inventory, and performance. IPMI exposes only a limited subset of these metrics.

Import/export server configuration profile is a capability in iDRAC10 that allows administrators to apply complete server configuration profiles (including BIOS, storage, and network settings) to one or more servers. IPMI supports backup and restore only for BMC settings.

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

Supermicro Intelligent Platform Management Interface 2.0 (IPMI) is Supermicro's embedded management controller interface. It provides remote access and basic configuration capabilities but supports fewer settings and automation workflows than iDRAC10.

Supermicro Server Manager (SSM) is Supermicro's one-to-many management tool for monitoring and basic administration. It offers fewer configuration and analytics capabilities than OME.

Two-factor authentication is an additional security verification method that requires a second proof of identity in addition to a password. iDRAC10 supports two-factor authentication through RSA SecurID; Supermicro tools support two-factor authentication via RADIUS only.

Appendix B: Test Configurations

Feature	Dell	Supermicro
Server Model	PowerEdge R770	Supermicro SuperServer® SYS-222HA-TN
CPU	2 x Intel® Xeon® 6767P	2 x Intel Xeon 6980P
Storage	2 x 447.13 GB NVM Express® (NVMe®) 6 x 1,489.88 GB NVMe	1 x 960 GB NVMe solid-state drive (SSD) 1 x 400 GB NVMe M.2
Memory Size	2,048 GB	512 GB
Memory	32 x 64 GB 5,200 MHz	8 x 64 GB 6,400 MHz
BMC Version	iDRAC10 v1.20.60.50	IPMI 2.0 v1.21.1
Software Version	OME v4.6.0	SSM v6.3.0

Appendix C: Testing Data

Feature/Action	Dell Steps and Time	Supermicro Steps and Time
Dynamic USB Ports	iDRAC10: 4 steps, 9 seconds	Supermicro: 8 steps, 4 minutes and 25 seconds
Two-Factor Authentication via RSA	iDRAC10: Supports RSA-based two-factor authentication	Supermicro: Supports two-factor authentication, but does not support RSA-based authentication
BIOS Live Scanning	iDRAC10: Verifies BIOS integrity when live scanning is enabled without requiring a server reboot	Supermicro: Does not provide continuous BIOS integrity verification

Feature/Action	Dell Steps and Time	Supermicro Steps and Time
Credential Management	OME: Supports centralized credential management with automated rotation of iDRAC passwords, including integration with external tools such as CyberArk	Supermicro: No comparable feature
Scope-Based Access Control (SBAC)	OME: Supports SBAC	SSM: Only supports RBAC
Centralized Identity and Access Management	iDRAC10: Supports OIDC via Ping Federate and Keycloak	Supermicro: No comparable feature
Full-System BIOS Configuration	iDRAC10: Provides access to more than 100 BIOS settings; allows staging of BIOS changes in 5 steps and 17 seconds and without a reboot	IPMI: Provides access to 1 BIOS setting at the BMC level; requires 4 steps and 4 mins and 26 seconds to change (including the reboot)
Automatic Firmware Updates	iDRAC10: 13 seconds per server	IPMI: 91 seconds per server
Import/Export Full Server Configuration Profile	iDRAC10: 9 seconds to start an unattended import	IPMI: 785 seconds to manually import BMC-level settings and make changes in BIOS
Connection View	iDRAC10: Supports Connection View for remote diagnosis of cabling and connectivity issues	Supermicro: No comparable feature
Alert-Based Automated Actions	OME: 11 steps, 32 seconds for initial configuration, with no further actions required	SSM: 9 steps, 14 seconds (plus 8 steps and 17 seconds to address each alert)
HTML5-Based Management Interface	OME: Uses an HTML5-based interface for all management functions	SSM: Has a service-side JRE dependency, which must be maintained and is a potential security vulnerability
Preconfigured Virtual Appliance Deployment	OME: Delivered as a virtual appliance supporting multiple deployment form factors, including common hypervisors	SSM: Installed as an application on Windows or Linux servers or a VMware-based appliance on Linux
Heterogeneous Server Monitoring	OME: Supports monitoring servers from multiple manufacturers through a single management interface	SSM: Focuses primarily on Supermicro systems; requires separate tools for other servers
Third-Party Integration Support	OME: Supports 5 third-party plugins (Windows Admin Center, VMware vCenter, Microsoft® System Center, ServiceNow®, and Ansible®), including a VMware vCenter integration with 18 management features	SSM: Supports fewer third party integrations (VMware vCenter, ServiceNow, and Ansible) with 8 management features for VMware vCenter
Mobile Integration	OME: Supports mobile-level interaction for monitoring and selected management tasks	SSM: No comparable feature
Configuration Template Deployments	OME: Supports template-based deployments covering BMC, BIOS, storage, and networking settings; 10 steps, 34 seconds for initial setup; 0 steps, 0 seconds afterward	Supermicro management tools: Support narrower, hardware-specific templates at the BMC and BIOS level; 7 steps, 15 seconds per deployment
Firmware and Driver Updates	OME: Supports automated firmware and driver updates, removing the need for manual file discovery and repeated uploads; 17 steps, 1 minute and 8 seconds for initial setup; 0 steps, 0 seconds afterward	Supermicro management tools: Require administrators to manually locate and upload firmware and driver files; 14 steps, 1 minute and 56 seconds per component update

Feature/Action	Dell Steps and Time	Supermicro Steps and Time
Report Builder with Customization	OME: Provides 52 built-in reports and the ability to customize	Supermicro: Provides 13 static reports
Telemetry Streaming	iDRAC10: Supports 32 reports across 12 categories for telemetry streaming with 285 individual metrics	Supermicro management tools: Support 10 reports across 3 categories for telemetry streaming with 17 individual metrics
GPU Metrics and Visibility	iDRAC10: Provides 33 GPU-related metrics	IPMI: Provides 9 GPU-related metrics
Power Management Reporting	OME Power Management: Provides 27 built-in reports	SSM: Provides 2 built-in reports
Power Usage Metrics (Per-Server Visibility)	OME Power Management: Provides 22 metrics across 12 categories with 8 dashboard views	SSM: Provides 3 metrics with 4 dashboard views
Carbon Emissions Analysis and Capacity Planning	OME Power Management: Provides carbon-emissions analysis based on actual server energy usage	SSM: No comparable feature
Automated Power and Thermal Management Policies	OME Power Management: Provides 2x the options for administrators, supporting both power- and thermal-based policies	SSM: Supports power-based policies only
Power and Thermal Data	OME Power Management: Provides 16 metrics across 8 categories	SSM: Provides 5 metrics across 4 categories
Cybersecurity Advisories	AIOps: Provides centralized visibility into configuration and security-related conditions across server environments and surfaces advisory insights	Supermicro: No comparable tool available
Policy-Based Security Configuration (PBSC)	AIOps: Evaluates server configurations against defined security policies and surfaces misconfigurations centrally	Supermicro: No comparable tool available
Multiple Performance Reports	AIOps: Provides multiple built-in performance reports that present detailed views of system behavior across server environments	Supermicro: No comparable tool available
GenAI Assistant	AIOps: Includes a built-in GenAI assistant to help administrators interact with analytics and management features	Supermicro: No comparable tool available
Performance Metrics with Anomaly Detection	AIOps: Provides performance metrics and anomaly detection views	Supermicro: No comparable tool available
Server-Level GPU Utilization	AIOps: Provides server-level GPU utilization metrics to help administrators understand accelerator usage across workloads	Supermicro: No comparable tool available
Carbon Footprint Analysis	AIOps: Provides carbon footprint analysis with summary-, system-, and workload-level metrics for energy usage and carbon emissions	Supermicro: No comparable tool available

Legal Notices and Disclaimers

0626/260003