

TURNING AI AMBITION INTO TRUSTED PRODUCTION WITH CONTROL-M



Customers have moved beyond the question of whether to experiment with AI. The question now is more practical: once an AI agent can interact with a production workflow, how do you give it access while maintaining the control and confidence to stand behind the outcome?

That question sits at the heart of the October Control-M release and reflects what we're hearing across the market. New AI capabilities are easy to introduce. Running them reliably alongside the critical work the business already depends on is the harder challenge. AI's value doesn't come from intelligence alone. It comes from connecting that intelligence to governed action across the systems and workflows the business depends on, where orchestration becomes essential.

What teams need in production

This release responds directly to that daily pressure. AI agents, automation, and hybrid environments are now part of how work gets done, and teams need a unified way to bring them into production, rather than creating a second operating model alongside the first.

Intelligence needs to meet people where they work, without compromising enterprise control. Operators need answers in the context of their workflows, while AI agents need governed access to act. And as automation expands, trusted data, secure credentials, and operational resilience must scale with it.

What changes in October

New AI monitoring capabilities help operators investigate jobs and workflows using natural language, turning production context into clear insights on what happened and why.

The Control-M MCP Server is now generally available on Control-M SaaS, providing a governed path for AI agents to interact with Control-M, from accessing job information and logs to taking approved actions, all within existing security, permissions, and audit controls.

Execution is only as reliable as the data behind it. Control-M Data Assurance is now native on Control-M SaaS, embedding data quality checks directly into workflows to catch issues before they propagate downstream and impact critical business outcomes

Security and resilience advance further in this release. Expanded vault support across SaaS and self-hosted environments strengthens secrets management, while Multi-Region Disaster Recovery provides U.S. SaaS customers greater business continuity through regional failover

Managed File Transfer / Enterprise strengthens resilience for self-hosted customers with a centralized database architecture, simplifying high availability, disaster recovery, and failover across sites while expanding database flexibility.

On Control-M SaaS, a refreshed web experience makes monitoring more intuitive and insightful. A new Gantt view brings the day's workflows into a single visual timeline, making it easier to spot delays, failures, and anomalies in the broader context of how work is progressing.

New integrations extend Control-M orchestration across ERP, cloud infrastructure, containers, messaging, and AI platforms, replacing custom scripts with native connectivity to Oracle JD Edwards EnterpriseOne, AWS Auto Scaling Groups, Argo Workflows, SAP Build Process Automation, IBM MQ, GCP Managed Instance Groups, Amazon Bedrock AgentCore, and Workato.

Together, these advances reinforce a unified approach to enterprise orchestration: greater intelligence for operators, governed access for AI agents, stronger security and resilience, and broader orchestration across the enterprise.

The technology landscape may change, but the need for trusted orchestration does not. As AI moves from experimentation into enterprise operations, Control-M provides the foundation to run critical work with the control, reliability, and flexibility enterprises require.

Read more on the BMC New Product Innovation announcements:

<https://www.bmc.com/blogs/delivering-predictable-outcomes-ai-era/>