



Broadcom Unveils AI-Ready Data Foundations in VMware Tanzu Platform to Power Secure Enterprise AI Cloud

August 31, 2026

New Capabilities Pair Governed AI Agents with Governed Data Inside the Private Cloud to Solve Security, Accuracy, and Operational Cost Challenges

LAS VEGAS, Aug. 31, 2026 (GLOBE NEWSWIRE) -- **VMware Explore 2026** -- Today at VMware Explore, Broadcom Inc. (NASDAQ: AVGO), a global technology leader that designs, develops, and supplies semiconductor and infrastructure software solutions, announced new AI-ready data foundations for the VMware Tanzu Platform, the official agent platform for VMware Private AI Cloud. The update delivers a complete, end-to-end framework enabling enterprises to transition safely from initial AI pilots to fully production-ready AI agents inside their own secure private clouds.

As organizations adopt agentic AI, business leaders face critical trust and security hurdles. Unlike traditional software, AI agents act autonomously and query data independently, creating significant risks around data leakage, unexpected cloud egress fees, and inaccurate outputs caused by uncurated information.

The latest VMware Tanzu Platform release solves this agent trust problem in two ways: securing the agent and securing the data. Agents run in hardened sandboxes leveraging services from a curated marketplace, so every agent operates with isolated credentials and explicit connections to the services it uses. Data is governed for access, context, and lineage. Access means agents reach the right data and only the right data. Context means data is prepared efficiently before agents consume it, improving accuracy and lowering token costs. Lineage means every agentic decision can be traced to exactly what data was used and where it came from.

Key capabilities introduced in the VMware Tanzu Platform include:

- **Hardened Agent Sandboxes:** Enforces a "deny-by-default" security containment model that completely isolates credentials, helping to prevent prompt injection attacks and unauthorized network access.
- **AI-Ready Data Foundations:** Processes structured and unstructured enterprise data on-site, delivering high-precision context to AI agents to improve accuracy, reduce hallucinations, and lower token costs.
- **Out-of-the-Box Developer Harness:** Accelerates build times with pre-approved skills, step-by-step workflow buildpacks, human-in-the-loop controls, and integrated memory services.
- **Curated Marketplace:** Operates a centralized catalog where developers and agents can safely discover and connect to vetted AI models, tools, and data products.
- **Auditable Agent Governance:** Integrates an AI gateway to monitor, rate-limit, and log every action an agent takes for strict compliance and auditing.

Supporting Quotes

"As part of an integration phase that began in 2019, BDC used VMware Tanzu Platform to support the deployment and operation of selected internal business applications. During this phase, the platform helped standardize how applications were deployed and managed across teams, reducing manual processes and differences in how applications were run. As our use of data and AI evolved, this also helped our platform teams support these applications and related services without requiring additional specialized expertise. This helped reduce day-to-day operational overhead for our technology teams."

– **Marie-Claude Potvin, Assistant Vice President, Infrastructure Services, Business Development Bank of Canada (BDC)**

"Enterprises aren't hesitant about agents because of what they know can go wrong; it's the unknown unknowns, the unintended consequences nobody can enumerate in advance. Much of that risk lives where agents meet enterprise data. Platforms that make data access governed, curated, and auditable by default turn that fear into something manageable."

– **Rachel Stephens, Research Director, RedMonk**

"Enterprises do not have an AI ambition problem. They have an agent trust problem. You cannot let software make decisions on data you do not govern, running on infrastructure you do not control. Tanzu Platform for Agents pairs governed agents with governed data inside the customer's own boundary, so businesses can move fast with agents without giving up control."

– **Purnima Padmanabhan, vice president and general manager, Tanzu Division, Broadcom**

Availability

Capabilities announced here will be generally available in Tanzu Platform in Fall 2026.

For More Information

Read more about Tanzu Platform for agents in the announcement blogs:

- [Introducing AI-Ready Data Foundations in Tanzu Platform](#)

- [Scaling the Agentic Enterprise: Production-ready AI Agents with Tanzu Platform](#)
- [Summary of all Tanzu Platform announcements at VMware Explore 2026](#)

About VMware Explore

VMware Explore is the established cloud event for IT professionals to advance their skills and credentials. VMware Explore 2026 will connect attendees with technology experts and solution architects who are solving real-world challenges. Focused technical sessions, Hands-on Labs, and certification opportunities will enable attendees to apply their learnings and deliver greater value back to their organizations. Attendees will leave with the training, tools, and strategies to build and operate a modern private cloud that is AI-native—running any workload while keeping data local and secure. To learn more about VMware Explore, please visit: <https://www.vmware.com/explore>

About Broadcom

Broadcom Inc. (NASDAQ: AVGO) is a technology leader that designs, develops, and supplies semiconductors and infrastructure software for global organizations' complex, mission-critical needs. Broadcom combines long-term R&D investment with superb execution to deliver the best technology, at scale. Broadcom is a Delaware corporation headquartered in Palo Alto, CA. For more information, visit www.broadcom.com.

Broadcom, the pulse logo, and Connecting everything are among the trademarks of Broadcom. The term "Broadcom" refers to Broadcom Inc., and/or its subsidiaries. Other trademarks are the property of their respective owners.

Media Contact:

John D'Avolio
Tanzu Division, Broadcom
+1. 503. 308.3096
john.davolio@broadcom.com