



Broadcom Delivers End-to-End Security, Identity, and Observability for Agentic AI

August 31, 2026

Together AgentMinder, VMware vDefend, and VMware Avi Load Balancer Enable Enterprises to Secure Autonomous Agents, Protocols, and AI Workloads

LAS VEGAS, Aug. 31, 2026 (GLOBE NEWSWIRE) -- **VMware Explore 2026** — Broadcom Inc. (NASDAQ: AVGO), a global technology leader that designs, develops, and supplies semiconductor and infrastructure software solutions, today announced comprehensive security, identity, and observability capabilities for agentic AI environments running on Private AI Cloud. With AgentMinder, VMware vDefend, and VMware Avi Load Balancer, Broadcom provides advanced, multi-layer cybersecurity solutions designed to govern autonomous AI agents, defend agentic workloads, and protect enterprise Private AI Cloud workloads.

Private AI Cloud delivers a more secure and cost-effective AI infrastructure to run inference workloads and agentic AI. It features the advanced security and automated compliance guardrails to help secure the workloads while helping to prevent data exfiltration and reducing cyber risk across every AI workload. Customers benefit from an agentic AI pipeline to build, run and govern trusted agents to innovate rapidly.

The enterprise attack surface expands dramatically across agents, tools, datastores, and large language models (LLMs) as organizations deploy agentic AI applications using new protocols such as Model Context Protocol (MCP) and agent-to-agent (A2A) communications. Broadcom's advanced cybersecurity solutions address these emerging blind spots by establishing trusted agent identities, enforcing Zero Trust boundaries, and providing enhanced visibility and granular control across the entire AI ecosystem.

"Enterprises need to rethink their security architecture as they operationalize their private AI cloud with agentic workloads," said Umesh Mahajan, vice president and general manager, Application Networking and Security Division, Broadcom. "With AgentMinder, vDefend, and Avi we are delivering a comprehensive set of layered security solutions for the Private AI Cloud. Enterprises can now safely operationalize agentic AI with defense-in-depth security, enforce strict guardrails, and comprehensively protect their AI environment."

Comprehensive Defense and Governance for Agentic AI

These solutions address critical agentic AI security and operational risks across three core layers: VMware vDefend, VMware Avi Load Balancer and Broadcom AgentMinder.

VMware vDefend: Agentic Zero Trust

VMware vDefend delivers Zero Trust lateral security for AI workloads running on VMware Cloud Foundation. The following new vDefend enhancements will extend its ZeroTrust lateral security to agentic AI workloads:

- **Discovery of Agentic AI Components:** Will automatically identify MCP servers, LLMs, datastores, and tools by continuously monitoring traffic flows across VMware Cloud Foundation.
- **Shadow AI Monitoring:** Will detect unauthorized AI usage and enforce strict Zero Trust policies to help maintain complete control over enterprise environments.
- **AI-Generated IDPS Signatures:** Will use an agentic AI pipeline to create Intrusion Detection and Prevention (IDPS) signatures at machine scale and speed, providing distributed virtual patching to protect workloads against the volume and velocity of AI-discovered vulnerabilities.

VMware Avi Load Balancer: Agentic Threat Defense

Avi Load Balancer, with its seamless integration with Kubernetes including VMware vSphere Kubernetes Service (VKS), multi-terabit performance, elastic scale-out operation is ideally suited to deliver AI-aware load balancing, web application security and API protection (WAAP) to agentic AI workloads. The following new enhancements will broaden its protection of agentic AI workloads:

- **Tool and Agent Misuse Prevention:** Will help restrict agents from accessing unauthorized MCP tools and inspect transaction content to block malicious execution, including remote code execution (RCE) and file injection.
- **Zero Day Attack Detection:** Will establish normal agentic traffic baselines across agents, LLMs, and tools to flag and isolate anomalous behavior in real time.
- **Sensitive Data Protection:** Will help prevent unauthorized exfiltration of credentials, personally identifiable information (PII), and sensitive financial data.

Broadcom AgentMinder: Agent Identity, Intent & Governance

Unveiled today, AgentMinder serves as the central control plane for autonomous AI agents ([read the press release](#)). As agents transition from content generation to active business process execution, AgentMinder delivers the following core governance capabilities:

- **Identity and Intent Controls:** Treats autonomous agents as enterprise-grade identities and binds their authority to a declared mission, permitted intents, approved tools, and authorized resources.
- **Runtime Policy Enforcement:** Features a cloud-native gateway that evaluates real-time context (identity, tool, intent, resource) and enforces least-privileged policies on every tool invocation.
- **Compliance-Grade Auditability:** Built on OpenTelemetry to deliver compliance-grade visibility into every agent session

and action, delivering chain of custody, anomaly detection, and operational insight at machine speed.

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 Contacts:

Heather Haley
Broadcom Global Communications
+1.925.856.8042
heather.haley@broadcom.com

Eloy Ontiveros
Broadcom Global Communications
+1.650.427.6145
eloy.ontiveros@broadcom.com