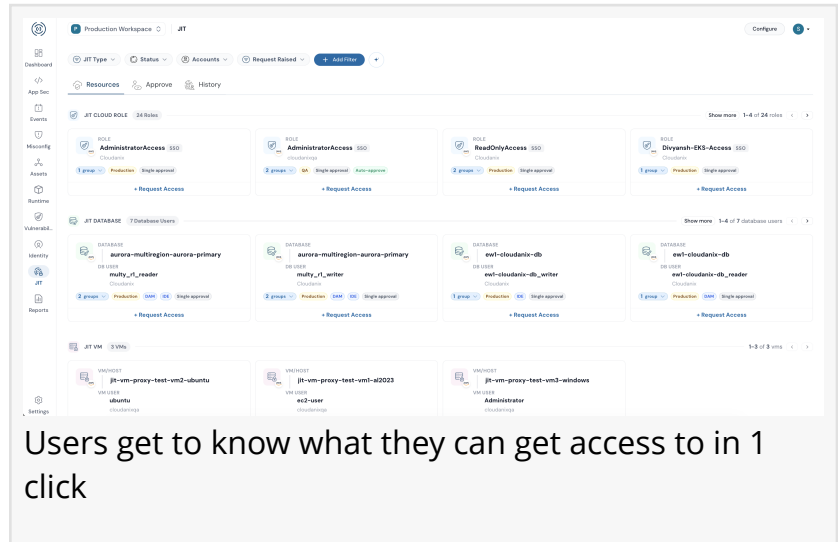


Cloudanix Achieves AWS Security Competency Status for Its CNAPP+ Platform and Just-in-Time Access Engine

The recognition validates Cloudanix's customer success - and Just-in-Time that replaces standing privilege across cloud, workloads, db, SaaS, and AI agents

SUNNYVALE, CA, UNITED STATES, August 10, 2026 /EINPresswire.com/ -- Cloudanix, an Amazon Web Services (AWS) Partner, today announced it has achieved the AWS Security Competency status, recognizing its technical proficiency and proven customer success in cloud security on AWS.



Users get to know what they can get access to in 1 click

The recognition arrives as non-human and AI agent identities increasingly outnumber humans in the cloud — turning standing privilege into one of the largest unmanaged risks security teams face. It is the risk Cloudanix is built to remove: granting privileged access only when it is needed, and taking it away the moment the work is done.

“

Managing privileged access to our AWS environment was once one of our biggest security concerns. With Cloudanix JIT, access is now temporary, audited, and automatically revoked”

Okesh Badhiye, Head of Technical Engineering, Finfinity (Customer)

The AWS Security Competency recognizes AWS Partners with demonstrated technical proficiency and proven customer success in security software. Cloudanix is also a member of the AWS ISV Accelerate Program and is available in AWS Marketplace, where customers can purchase it against their existing AWS commitments. Built on AWS, Cloudanix delivers continuous posture management, identity controls, and Just-in-Time access that customers run in their own AWS environments.

A platform play: CNAPP+, not a point tool

[Cloudanix is a CNAPP+ platform](#): the five canonical pillars of a Cloud-Native Application

Protection Platform — CSPM, CIEM, CWPP, Cloud Detection & Response, and Code Security — plus four capabilities classic CNAPP leaves out: Just-in-Time access for human, machine, and AI agent identities; code-to-cloud lineage; compliance as a first-class data object; and data-aware controls. Code, Cloud, Identity, and Data security run on one graph, with 30-minute agentless onboarding.

One Just-in-Time engine, seven access surfaces

At the center of the platform is Cloudanix's Just-in-Time (JIT) access engine, which replaces long-lived standing privilege with access that is requested, scoped, identity-stamped, and automatically revoked. One policy model, one approval flow, and one correlated audit trail cover human, machine, and agent identities alike — [delivered in flavors built for each layer of the stack](#):

Cloud JIT — time-boxed AWS, Azure, and GCP console access through an organization's existing SSO.

VM JIT — keyless, recorded SSH to any virtual machine, with no bastion and no shared keys.

Kubernetes JIT — ephemeral, scoped kubeconfig for any cluster, including fully private ones.

Database JIT — audited, keyless query access from the IDE a team already uses.

SaaS JIT — time-boxed entitlements across the SaaS catalog, with automatic off-boarding.

Agentic JIT — zero standing credentials for CI/CD pipelines, Kubernetes pods, services, and AI agents.

Coding Agent JIT — brokered, approval-gated access for AI coding agents such as Kiro, Claude, Cursor, and any MCP-based agent — the task gets the access, not the keys.

Each grant ties to a real human, machine, or agent identity and lands in the customer's own audit trail — giving security and compliance teams the exact who, what, when, and why behind privileged actions, and the evidence audits demand.

Executive perspective

"Earning the AWS Security Competency status validates what our team and our customers have built together. Cloud security has moved past posture management — the hard problem now is access. As machines and AI agents become the majority of identities in the cloud, standing privilege is the blast radius. With CNAPP+ and our Just-in-Time engine, customers replace that standing access with privilege that is granted on request and gone when the work is done."

— Sujay Maheshwari, Co-founder & CEO, Cloudanix

"We built one Just-in-Time engine for seven surfaces — cloud consoles, VMs, Kubernetes, databases, SaaS, CI/CD, and AI coding agents — with zero standing credentials and the same SSO, terminal, and kubectl engineers already use. Each action is identity-stamped to a real

human, machine, or agent and audited in the customer's own cloud. The AWS Security Competency reflects that engineering depth, and the outcomes our customers see."

— Purusottam Mupunu, Co-founder & CTO, Cloudanix

Customer perspective

"Managing privileged access to our AWS environment was once one of our biggest security concerns. With Cloudanix JIT, access is now temporary, audited, and automatically revoked — giving us a 100% reduction in privileged-access exposure without slowing our engineering team down. As a marketplace connecting more than 50 financial institutions, that level of confidence is essential."

— Okesh Badhiye, Head of Technical Engineering, Finfinity

Availability

Cloudanix is available now, including in AWS Marketplace. Organizations can connect an account and see findings rooted in identity, asset, and blast radius in under 30 minutes. To request a demo or a free assessment, visit cloudanix.com.

About Cloudanix

Cloudanix is a CNAPP+ cloud security platform that unifies Code, Cloud, Identity, and Data security on a single graph. Beyond the five canonical CNAPP pillars, Cloudanix adds Just-in-Time access for human, machine, and AI agent identities, code-to-cloud lineage, compliance-led design, and data-aware controls including Database Activity Monitoring. More than 140 organizations use Cloudanix to monitor over 100 million assets across AWS, Azure, and GCP, with 30-minute agentless onboarding, 1,000+ security checks, and coverage for 15+ compliance frameworks.

Cloudanix is backed by Y Combinator and has offices in Sunnyvale, California and Pune, India.

Learn more at cloudanix.com

Sujay Maheshwari

Cloudanix Inc

sujay@cloudanix.com

Visit us on social media:

[LinkedIn](#)

[YouTube](#)

This press release can be viewed online at: <https://www.einpresswire.com/article/933049107>

EIN Presswire's priority is source transparency. We do not allow opaque clients, and our editors

try to be careful about weeding out false and misleading content. As a user, if you see something we have missed, please do bring it to our attention. Your help is welcome. EIN Presswire, Everyone's Internet News Presswire™, tries to define some of the boundaries that are reasonable in today's world. Please see our Editorial Guidelines for more information.

© 1995-2026 Newsmatics Inc. All Right Reserved.