

Anzenna Launches Access Control for AI Usage giving Enterprises Identity-Aware Control Over Shadow AI

Lets organizations block unapproved AI tools, redirect employees to sanctioned alternatives, and conditionally permit access based on corporate identity

REDWOOD CITY, CA, UNITED STATES, June 30, 2026 /EINPresswire.com/ -- Anzenna announces the launch of [AI Access Control](#), a new capability that gives security teams precise, identity-aware control over how employees interact with AI applications. As generative AI tools proliferate across the workplace, organizations face mounting risk from unsanctioned "shadow AI" usage that can expose sensitive data and undermine compliance. Anzenna's new offering is designed to close that gap without slowing employees down.

AI Access Control gives administrators three core enforcement modes:

1. Block unapproved sites. Anzenna prevents access to unsanctioned AI applications outright, keeping employees within trusted, approved environments and eliminating a major source of uncontrolled data exposure.
2. Redirect to approved tools. Rather than simply blocking and frustrating users, Anzenna can automatically route employees from an unsanctioned tool to a sanctioned alternative, preserving productivity while keeping usage inside governed boundaries.
3. Conditionally allow access by identity. Anzenna applies granular, identity-based rules so that AI tools are accessible only through verified corporate accounts. Logins from personal or non-corporate identities can be restricted, ensuring sensitive data stays tied to managed, accountable users.

"AI has become part of how people work, but most organizations still lack the controls to govern it safely," said Chinmaya Sharma, Head of Product at Anzenna. "Blanket bans don't work as employees just find another tab. Our approach is to give security teams a precise dial: block what's risky, steer people toward what's approved, and tie access to corporate identity. You get security and productivity at the same time."

The capability is built for environments where [AI adoption](#) is outpacing governance. By distinguishing between corporate and personal identities, Anzenna helps prevent sensitive data from flowing into unmanaged accounts while giving security and IT leaders clear visibility and control over AI usage across the organization. Access Control for AI Usage is available now. To learn more or request a demonstration, visit <https://www.anzenna.ai>

About Anzenna

Anzenna is an activity governance solution for AI and human identities, the first to unify [AI Usage Control](#) and Insider Risk Management in a single product. It monitors and governs what every AI agent, non-human identity, and employee is actually doing across the full enterprise surface: browser extensions, MCP servers, IDE and coding agents, OAuth-authorized AI apps, and file and data movement. Its Identity-Data-Action graph links AI activity back to the human behind it, fusing behavioral signals with HR context, data sensitivity, and departure status to catch threats that access control alone cannot see. Anzenna remediates in real time through existing endpoint and identity infrastructure like CrowdStrike, Microsoft Defender, Okta, and others with no second agent to deploy, and generates autonomous, evidence-backed investigation reports instead of alerts in under two minutes. For more information visit <https://www.anzenna.ai/usecases/ai-access-control/>

Marketing Team

Anzenna Inc.

[email us here](#)

This press release can be viewed online at: <https://www.einpresswire.com/article/922481495>

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.