# Anzenna Launches AI DLP, Bringing Data Loss Prevention to AI Prompts and Agent Activity

*Stops sensitive data heading into sanctioned and shadow AI tools, then scores against the identity behind it before acting*

REDWOOD CITY, CA, UNITED STATES, July 30, 2026 /EINPresswire.com/ -- Anzenna announces AI DLP, a capability that detects and stops sensitive data from reaching AI tools. Source code and customer records now leave the enterprise through channels existing DLP was never built to inspect: sensitive data pasted into a personal ChatGPT prompt , an OAuth grant to an AI app with access to sensitive data, sensitive data exfiltrated via an MCP server connected to an approved AI solution, a coding agent working inside the IDE. Anzenna covers those paths and reasons about what each movement means before it acts.

Legacy DLP grew up around files moving through email and endpoint. However, they generate a ton of alerts without context and are blind to newer ways of AI exfiltration. Anzenna's AI DLP is focused on detecting newer AI threats while surfacing only a small number of legitimate cases instead of a mountain of benign alerts.

Anzenna's AI DLP works in four stages:

1. Anzenna correlates identity and data signals across the enterprise surface to find sensitive content heading toward AI tools, sanctioned and shadow alike, covering prompts, file uploads, MCP, OAuth grants, and agent activity.

2. Each movement is scored against the employee's behavioral baseline, their role and peer group, and the sensitivity of the data itself, rather than against a static rule.

3. Each violation is then investigated in context, resulting in a prioritized case file carrying the identity, the data type, the destination tool, and the reasoning behind the verdict, which is why customers see roughly 90 percent fewer alerts than existing DLP tooling puts in front of them.

4. Security teams can block the transfer, quarantine the data, revoke access, or coach the user, with a full audit trail on every action.

The same sensitive data paste can mean three different things, and Anzenna is built to tell them

apart. A support agent using a sanctioned assistant inside normal working patterns gets allowed through. Someone reaching for a personal account to move faster gets coached. A departing engineer pulling sensitive data they have never touched gets escalated to the security team with the evidence already assembled.

"Employees are putting real company data into AI tools every day, and most of them are just trying to do their jobs," said Chinmaya Sharma, Head of Product at Anzenna. "Existing DLP either misses that moment entirely or buries it under thousands of false positives nobody has time to read. We look at who moved the data and whether that behavior fits the person, which is what lets us stop the dangerous transfers without getting in everyone else's way."

“We have over 1000 alerts a day coming out of our legacy DLP and it’s missing AI coverage. Anzenna helps reduce alert volume by 90% while filling the AI DLP coverage gap” - Director of Security, Healthcare.

AI DLP is available now and leverages the endpoint and identity infrastructure customers already have. 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

Contact:
Marketing Team https://www.anzenna.ai

Marketing Team
Anzenna Inc.
email us here
Visit us on social media:
LinkedIn
X

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.