Anzenna

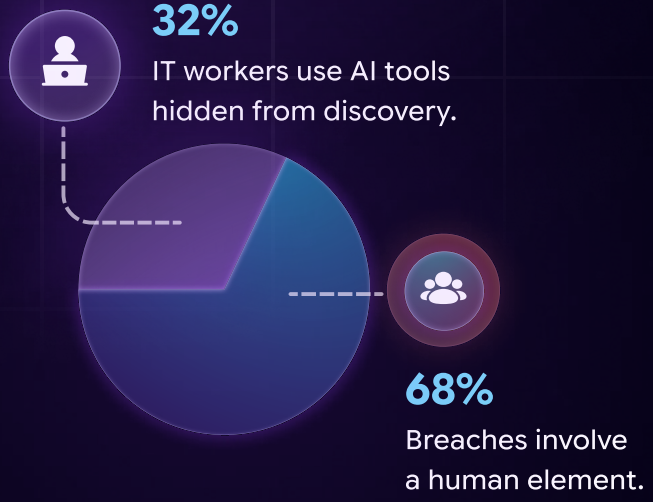
Your Insider Risk Program, Accelerated

Autonomous insider risk investigations, remediation, and operations.
The execution gap, closed. Deployed in minutes, always on.

Anzenna deploys AI agents that autonomously investigate, correlate, and remediate insider risk, acting as your AI insider risk analyst without human intervention. Anzenna builds a deep AI context graph across users, systems, and data.

This allows the platform to eliminate false positives and alert noise at the source, surfacing only **verified threats that truly require analyst attention.**

When human action is required, most of the work is already done. Each investigation includes **a complete evidence report and a recommended action.**



From Thousands of Alerts to Only What Matters

Security teams don't have a detection problem; they have an execution problem. Thousands of alerts, most of them noise. Anzenna cuts through it, resolving benign activity automatically so your analysts see only confirmed, pre-investigated risks with full context and one-click remediation ready to go.

Zero-Noise Threat Surface

The platform investigates, correlates, and resolves every alert, separating real risks from noise so only actionable incidents reach your team.

Deployed in Minutes, Always On

No endpoint agents, no professional services, no new hires. Live in minutes, operating autonomously 24/7.

One Platform, Full Coverage

Detection, investigation, correlation, and response across SaaS, cloud, identity, code, email, and endpoints, consolidated into a single autonomous platform.

Customer Experiences

90%

Alert noise eliminated

Benign activity, approved workflows, and false positives are resolved before they reach an analyst, reducing alert volume by 90%.

70%

Reduction in TTR

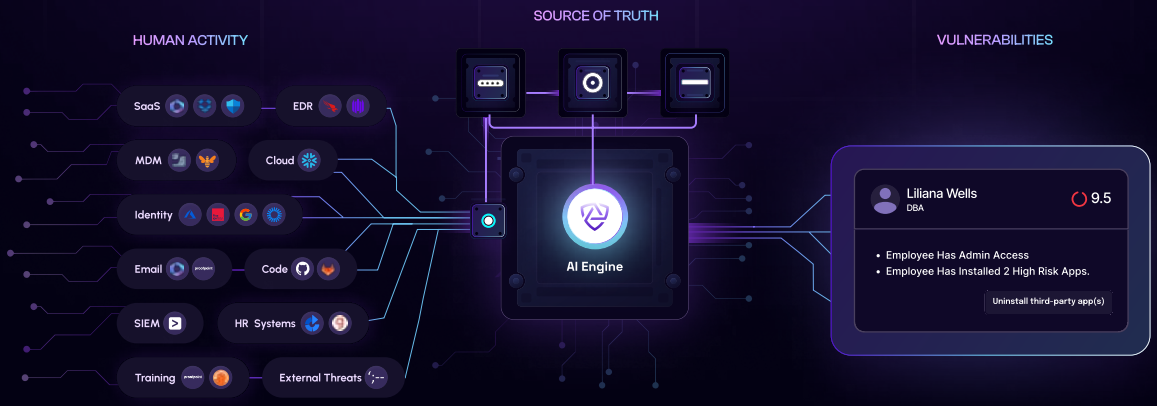
Investigations arrive fully assembled with correlated evidence, context, and recommended actions, ready for single-click resolution.

60%

Reduction in analyst workload

AI handles triage, investigation, and correlation end-to-end; analysts focus only on confirmed incidents requiring human judgment.

How Anzenna's AI Agents Work



Platform Benefits

Every alert is investigated automatically
Correlating activity across SaaS, cloud, identity, email, code, and device signals to determine if a threat is real.

False positives and approved behavior are resolved before they reach an analyst
No time wasted on noise from tools that flag benign or pre-approved activity.

Analysts see a clean, prioritized queue
Real insider risks with full evidence, not thousands of raw alerts.

Investigations arrive fully assembled
When a threat reaches an analyst, cross-system correlation, timeline, context, and impact are already compiled.

Single-click remediation
Analysts determine the best course of action and execute it with one click; TTR drops from hours to minutes.

Zero deployment friction
No endpoint agents, no months-long rollouts. Operational from day one with no additional headcount.

Threat Coverage

Data & IP Exfiltration	Cloud Data, AI, Salesforce, Source Code
AI Usage	Careless/Unsanctioned AI Use, AI Agents, uploads/file access
Compromised Insiders	Account Takeover, Identity threats, credential theft
Employee Watchlists	Disgruntled & Departing Employees, Sensitive Data Access
Privilege Misuse	Excessive / Unrevoked Access
Device & Application Threats	Malicious apps, hidden ransomware, and session hijacking

About Anzenna

Anzenna's agentic security platform works alongside your SOC and Insider Risk teams, deploying AI that continuously monitors and remediates risky signals across 130+ enterprise tools. From identity providers and endpoints to cloud platforms,

collaboration apps, and AI usage, Anzenna connects behavioral signals that would otherwise go unnoticed and acts on them before they become incidents. Anzenna is building a future where insider risk management is proactive, autonomous, and always on.

SOC2 Type certified.

Microsoft 365 security certified.

www.anzenna.ai

info@anzenna.ai