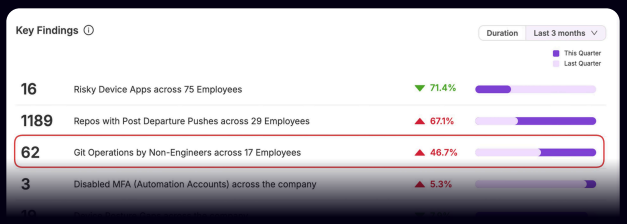
Anzenna + CROWDSTRIKE

Smarter Insider Threat Detection Starts at the Endpoint

How Anzenna + CrowdStrike Work Together

The Anzenna and CrowdStrike integration delivers real-time, contextualized insight into insider threats across your organization's endpoints—without deploying new agents or infrastructure. CrowdStrike provides world-class endpoint telemetry, detecting behavioral anomalies and emerging threats, while Anzenna enriches that data with identity context, historical user behavior, application risk, and automated remediation.

Together, they help security teams prioritize and act faster—flagging high-risk users, unknown apps, or suspicious behaviors, and responding immediately with precision



The Problem

Endpoints are often where insider threats begin—through risky app usage, credential theft, or lateral movement. But without broader context, even the best endpoint protection can miss the human element behind the breach. Who's behind the activity? Has this user or device exhibited risky patterns before? Is the behavior normal? Security teams lack that context and are overwhelmed with alerts, siloed data, and slow investigation workflows, leaving organizations exposed to internal threats. That's where Anzenna comes in.

Common Challenges

- Gaps in user-to-endpoint visibility and risk attribution
- Difficulty contextualizing threat telemetry with identity, behavior, and application data
- Reactive instead of proactive remediation
- Manual workflows that slow down the response
- Disconnected sources of truth across EDR, HR, identity, and app systems

CrowdStrike

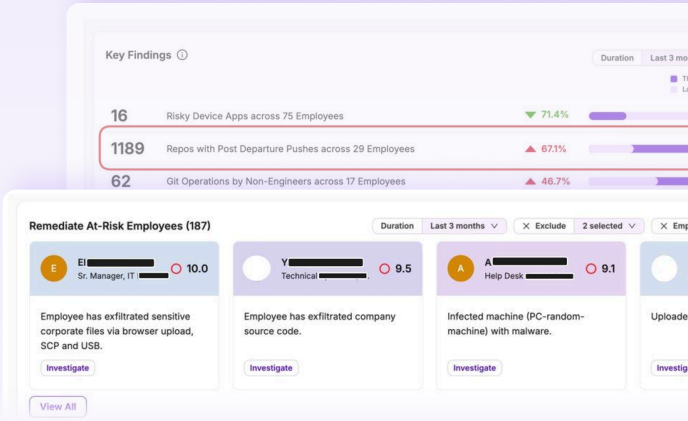
CrowdStrike Falcon is an industry-leading EDR platform delivering comprehensive visibility across endpoints. It provides real-time threat detection, prevention, and response—powered by threat intelligence and behavioral analytics trusted by enterprises worldwide.

Anzenna

Anzenna is a modern AI based platform that integrates directly with CrowdStrike. It applies Agentic AI to enrich endpoint data with user and application context, risk scoring, and automated response capabilities—giving security teams the full picture behind suspicious behavior.

Anzenna + CrowdStrike Integration

Gain the full picture by combining endpoint telemetry with context-rich, identity-centric risk intelligence. Anzenna brings intelligent prioritization and automated remediation to CrowdStrike alerts—empowering teams to act faster and reduce risk with confidence.



The Solution

Anzenna's CrowdStrike integration empowers you to uncover and act on the true source of insider risk. No agents. No silos. Just real-time insights and intelligent response built on trusted EDR telemetry.

Holistic Visibility

- Link users to devices, applications, and behaviors in real-time
- Understand the "who" & "what" behind every endpoint signal

Intelligent Risk Scoring

- Identify risky applications, usage patterns, and abnormal behaviors
- Score risk using app provenance, developer history, and user trends

Automated Remediation

- Trigger actions via CrowdStrike's native API—quarantine, isolate, or alert
- Stop risk at the source without deploying new tools

Seamless Integration

- Integrates via secure CrowdStrike APIs—no new agents needed
- Enterprise-ready: SOC2 Type II certified, Microsoft 365 pentested

Actionable Insights

- View unified data from CrowdStrike, Identity, HRIS, and more
- Prioritize insider threats with intelligent recommendations and workflows

Types of Threats Detected & Remediated

- Source code Exfiltration
- Data Exfiltration
- Risky Software and Applications Installed

Learn more at anzenna.ai

Anzenna + CROWDSTRIKE