Anzenna

# Anzenna for Developers

## Securing Developer Workflows Without Compromise

### Overview

Developers hold the keys to your kingdom. They push code, access sensitive IP, install their own tools, and operate at high velocity. That's why they're also one of the biggest blind spots in insider risk. Anzenna solves this by giving security teams deep visibility into developer environments without slowing them down. From VS Code extensions to privileged access, Anzenna tracks what matters, flags what's risky, and leaves developers free to ship.

# What Anzenna Does

### Full Developer Inventory

- Tracks applications, browser extensions, packages, and VS Code extensions
- Captures rich metadata like publisher, version, and descriptions
- Surfaces compliance risks (e.g. licensing violations)
- Detects and flags potential source code exfiltration by monitoring developer tools and workflows

### Just-in-Time Admin Access

- EPM system built on top of existing agents like CrowdStrike or Tanium
- Grants temporary elevated privileges only when needed
- Tracks what apps get installed during the session
- Helps meet insurance compliance and reduce exposure

### AI-Driven Risk Scoring

- Uses proprietary AI agents to analyze every item installed
- Flags high-risk software based on behavior, publisher reputation, and threat indicators
- Keeps false positives low (~1–2% for critical issues)

### VS Code Extension Monitoring

- Focuses on VS Code due to its massive install base and lax extension marketplace policies
- Detects malicious or invasive extensions, an area where other tools fall short
- Doesn't uninstall by default, but provides enough context for security teams to make the call

### Behavioral Context

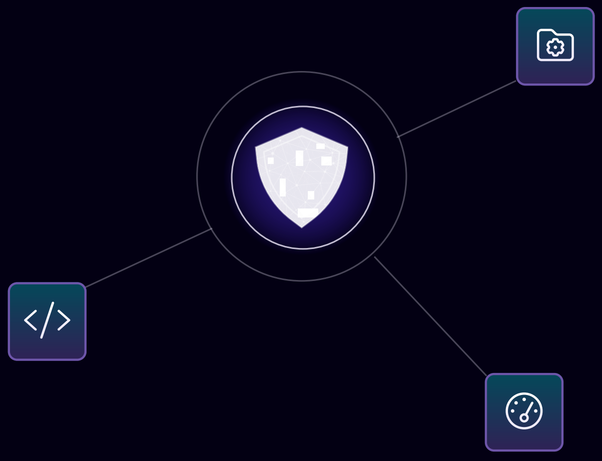
- Benchmarks user behavior against team norms
- Flags abnormal activity like large-scale data transfers or dangerous combinations of actions (e.g. MFA disabled + risky app installed)

### Co-Pilot for Security

- Natural language interface that lets security teams query the system directly
- "Why is this risky?" "Who else uses this app?" → Instantly answered with explainability

## Why Developer Risk Matters

Developers are high-permission users by design. They often run with admin rights, have access to sensitive repos and environments, and are trusted to manage their own tools. But this freedom creates security gaps:



- Accidental risk: pushing secrets to GitHub, installing sketchy extensions, ignoring MFA
- Malicious intent: IP theft before switching jobs
- Security apathy: most devs don't see security as their job and often see it as a blocker

Anzenna helps security teams meet developers where they are, giving them full visibility into what's running on dev machines and prioritizing what's actually risky.

## How It Works

### Zero Friction for Devs

- No new agents. Built to work with tools already deployed: CrowdStrike, Intune, Tanium
- Doesn't block installations or inject itself into workflows

### "Trust but Verify" Philosophy

- Lets developers move fast, but gives security full situational awareness
- Designed to educate, not punish, users when risky behaviors are spotted

### Built for the Real World

- Prioritized VS Code because of real malicious activity and a rich, structured extension marketplace
- Built by devs, for devs. Most of Anzenna's own engineers use VS Code

# Business Value

Reduces organizational risk without hurting velocity

Increases visibility for insider threat programs

Supports compliance and audit readiness (e.g. license use, access control)

Prevents high-impact, low-frequency events like IP theft or malicious exfiltration

Can unlock discounts on cyber insurance with proper privilege control

## Ready to put your insider risk program on auto-pilot?

Anzenna helps companies understand, prioritize, and act on developer risk without crushing productivity. It's a lightweight, high-impact layer of protection for the users you trust the most.

Anzenna