Anzenna

WHITE PAPER

How Anzenna + VS Code Work Together

The Anzenna and VS Code integration delivers real-time visibility into the AI tools developers rely on most without requiring new agents or disrupting workflows. VS Code enables rapid extension adoption, but with that speed comes risk. Anzenna monitors extension usage across developer environments, leveraging endpoint telemetry to detect risky or malicious plugins. It enriches that data with publisher trust, user behavior, and application risk, surfacing the insights that security teams need most.

Together with VS Code, Anzenna empowers teams to spot blind spots, flag dangerous extensions, and support safe developer practices without slowing anyone down.

The Problem

Developer environments are a blind spot. These users often have elevated privileges, access to sensitive IP, and install their own tools, including risky VS Code extensions.

The VS Code marketplace's lenient publishing process makes it easy for malicious actors to push extensions that quietly exfiltrate data or run scripts in the background.

Security teams are often unaware of what extensions developers are using or whether they're risky, due to disconnected systems and lack of real-time insight.

Common Challenges

- **High-risk users with unmonitored admin access**
- **Malicious VS Code extensions with deep permissions**
- **Lack of application inventory and metadata**
- **Security perceived as a blocker to developer productivity**
- **Siloed tools: no link between identity, device, and dev tools**
- **Manual research and triage processes that don't scale**

Visual Studio Code

Visual Studio Code is a lightweight yet powerful source code editor developed by Microsoft. Widely adopted by developers across the globe, it supports a vast ecosystem of extensions and integrations, enabling everything from debugging and version control to AI-powered coding assistance. With real-time collaboration, built-in terminal, and cross-platform support, VS Code is trusted by individual developers and enterprise teams alike to streamline development workflows and boost productivity.

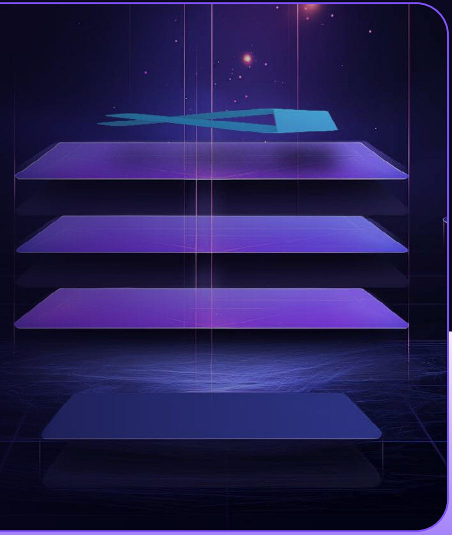
Anzenna

Anzenna is an agentless Insider Risk Management platform that integrates seamlessly with VS Code environments. Using advanced Agentic AI, Anzenna fills critical gaps in extension visibility, maps risky plugins to individual users, and enriches extension data with publisher trust, behavioral signals, and automated risk scoring—all without disrupting developer workflows.

Anzenna + VS Code Integration

Gain the full picture by layering AI-driven context over your development environments.

Anzenna turns extension metadata and device telemetry into identity-aware, developer-specific risk intelligence, allowing security teams to prioritize what matters and reduce noise. With automated insights, explainable risk scores, and deep integration into existing tools, Anzenna gives you confidence to manage insider risks in VS Code at scale.



The Solution

Anzenna's VS Code integration offers security teams what they've lacked: deep visibility into what developers install, enriched with intelligent context, without friction.

Holistic Visibility

- See what extensions developers are using automatically.
- Pull inventory of VS Code extensions using EDRs like CrowdStrike, no new agents needed.
- View extension metadata: publisher, version, description.
- Understand extension provenance and trustworthiness using AI enrichment.

Intelligent Risk Scoring

- AI evaluates extensions and apps at scale: who published them, what they access, and how they behave.
- Scores are assigned based on publisher trust, permissions requested, and historical developer behavior.
- Helps flag truly risky items, cutting noise with a ~1–2% false positive rate.

Automated Developer-Centric Insights

- Don't block, educate.
- Security teams get context-rich insights to share with developers, reinforcing safe behavior.
- Co-pilot feature lets teams ask "why was this flagged?" and get specific answers.

Seamless Integration

- No new agents. Built on existing platforms like CrowdStrike Falcon.
- Works quietly in the background with zero disruption to developers.
- SOC2 Type II certified and enterprise-ready.

Actionable Use Cases

- Identify malicious VS Code extensions before they cause harm
- Flag high-risk packages, apps, and browser extensions
- Catch non-malicious but risky behavior like license violations
- Support just-in-time admin controls