harmonic | AI Usage Intelligence

Understand What Your Organization Is Actually Doing With AI

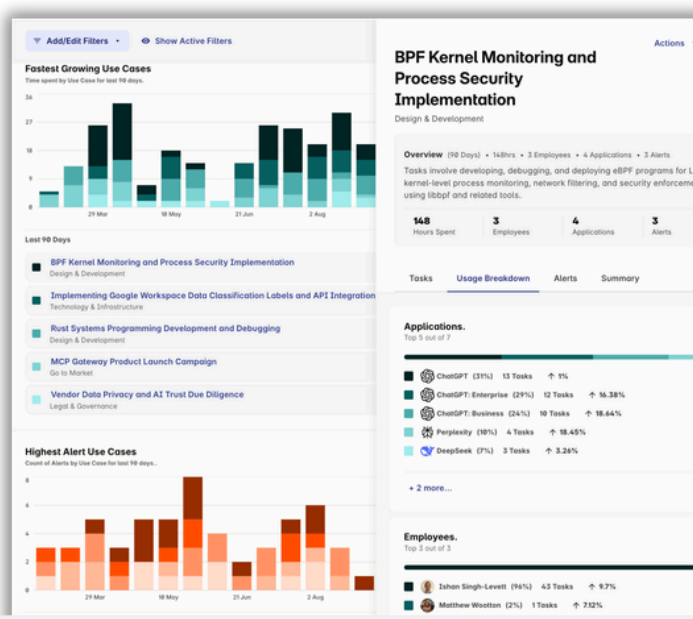
Usage Explorer moves you past app-level analytics to understand the work happening inside AI tools — the use cases driving adoption, the sensitive data being shared, and where risk and value actually exist. Not generic. Not prompt-level. Your organization's AI activity, classified into the business use cases that matter to you.

How it works

Interactions - Individual prompt/response exchanges, captured via the browser extension.

Tasks - Groups of related interactions forming one coherent piece of work. Each task receives an AI-generated summary. No raw prompts are surfaced — leaders see what people were working on, not what they typed.

Use cases - Clusters of similar tasks across employees, apps, and time. Unique to your organization. A law firm sees "contract review" and "case summarization." A retailer sees "inventory planning" and "customer complaint responses."



Key capabilities

Automatic use case discovery
Emerges from your actual data — not a predefined taxonomy. Reflects how your business uses AI, not how Harmonic thinks it should.

Two classification layers
9 functional categories (Go to Market, Legal) and 5 value categories (Risk & Compliance, Revenue & Growth, etc.) give a shared language across stakeholders.

Adoption and risk simultaneously
See where AI is delivering value and where it's creating exposure. A sensitive data alert in a board prep use case carries a different risk profile than the same alert in general drafting.

Department and function breakdowns
Slice by team, app group (approved vs. unapproved), employee, or time range. Spot which departments lead adoption and where employees are turning to unsanctioned tools.

Built for every team with a stake in AI

Usage Explorer gives security leaders, IT leaders, and AI committees a shared view of how AI is actually being used, without each team needing a different tool. Security can prioritize risk by workflow rather than raw alert volume. IT can rationalize licenses with real usage data instead of estimates. AI committees can track adoption, spot emerging use cases, and identify where employees are turning to shadow AI because sanctioned options fall short.

What you can see

Hours spent using AI — Total time across all use cases, sliceable by employee, department, or app

Fastest-growing use cases — Where traction is building; useful for tracking known internal AI projects

Use cases with highest alerts — Identify risky workflows; drill in to see which employees and apps are involved

Approved vs. unapproved breakdown — Time spent on sanctioned tools vs. shadow AI, by use case

Per-use-case app list — See when employees accomplish the same work across different tools (consolidation signal)

CSV export — Take use case data into board decks, AI committee reporting, or leadership reviews

Privacy controls included

- No raw prompts in the UI — task summaries only
- Employee exclusion list for sensitive roles
- Employee masking carries over from platform settings
- RBAC: Read Use Cases / Read Tasks / Delete Use Cases
- Personal conversations filtered out during processing

Requirements
"Store request content" setting enabled + 29-day minimum data retention.

Coverage
Coverage: ChatGPT, Claude, Gemini, Copilot, Perplexity, Copilot in M365, DeepSeek.

> "We needed to understand not just which AI tools were being used, but how they were being used. That's a completely different question—and it's the one that actually matters."
>
> **Neil Patel,**
> **Global Head of IT, Apax**

harmonic

Governance for how AI actually gets used at work. Every employee, every agent, every interaction.

harmonic.security