Discovery

Identify the Unknown. Illuminate SaaS Risk.

The Challenge

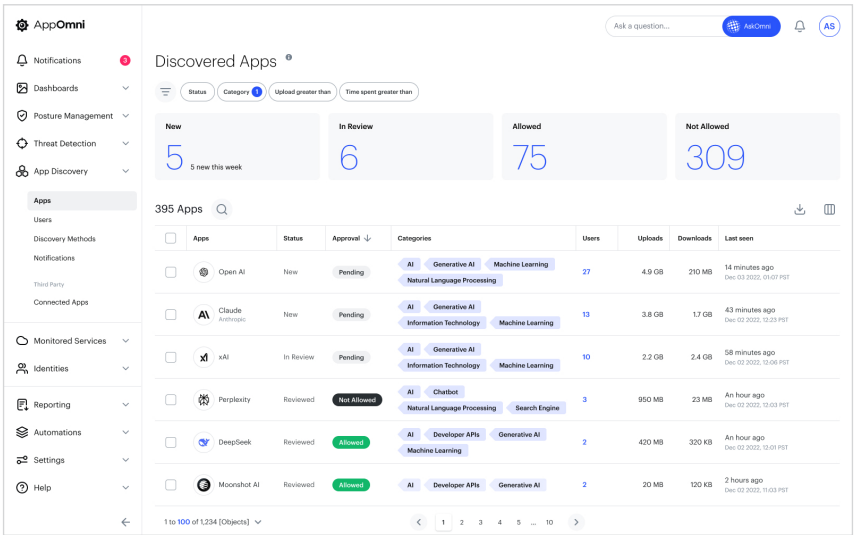
Do you know every SaaS app your employees are using? Shadow IT, AI-powered tools, and third-party apps spread faster than security can respond—creating risk, breaking compliance, and consuming time. Most discovery tools are either overly invasive, demanding access to user emails, or too shallow to act on. Without accurate, identity-level insight into app usage, security teams can't enforce policies, assess exposure, or manage their SaaS footprint confidently.

The Solution

AppOmni Discovery shines a light on what's really running in your environment—uncovering unsanctioned apps, AI tools, and risky third-party connections that would otherwise remain hidden.

It goes beyond basic visibility. By mapping usage to real users and collecting rich telemetry, Discovery gives security teams the context they need to act—whether flagging shadow IT, assessing app criticality, or making informed security decisions.

And because it's purpose-built for SaaS, Discovery fits seamlessly into how your team already works. No invasive access. No heavy lift. Just clear insight, faster investigations, and stronger governance across your SaaS ecosystem.



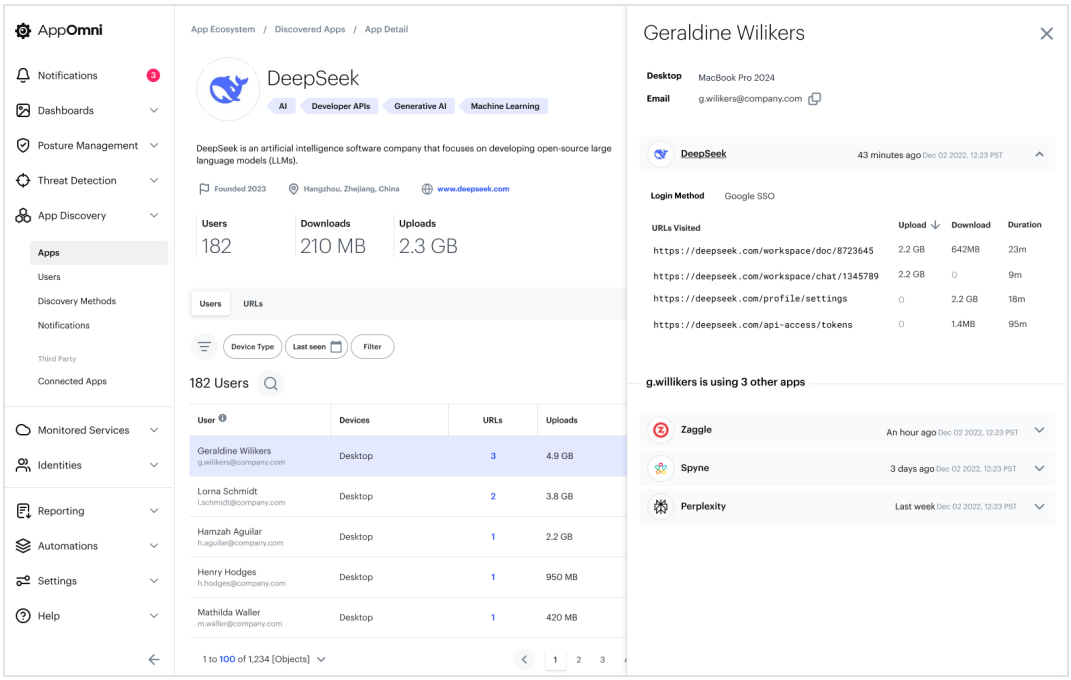
Inventory SaaS apps to include AI applications

BENEFITS

- **Faster visibility:** Instantly surface all SaaS tools, sanctioned and unsanctioned.
- **Reduced shadow IT:** Discover AI-based and unmanaged apps that increase your attack surface.
- **Third-party app governance:** Uncover browser-based connections
- **Improved SaaS governance:** Tag business use, assign owners, and build an approved app catalog

KEY FEATURES

- Browser-Based Collection
- Near Real-Time Inventory
- AI App Recognition
- App Usage Stats
- Third-Party & OAuth Insight



Connect app usage to identities

Capabilities to Identify SaaS

Capability	What It Does	Why It Matters
Browser-Based Collection	Captures app usage (time, data transfer, URLs) via a lightweight extension	Offers real-time insight without agents, email scraping, or overreach.
AI-Powered App Recognition	Cross-matches usage against a dynamic SaaS and AI app library	Automatically surfaces emerging risks and trending tool usage.
Third-Party & OAuth Insight	Identifies connected apps and OAuth scopes	Uncovers shadow integrations that expand your threat surface.
SaaS Inventory	Continuously updated list of discovered apps	Enables timely triage, blocking, or approval workflows.

Why AppOmni

- **Purpose-Built for SaaS:** Enable SaaS governance with usage insights, ownership tagging, and criticality scoring
- **Least Privilege Approach:** No inbox access, email scraping, or excessive permissions
- **Depth, Expertise & Integration:** Enterprise-scale with deep context and integrated workflows across posture, threat, and identity

> Discovery confirmed what we always suspected—our employees were using far more SaaS applications than we had visibility into. Now, we can finally see and manage the full scope of our SaaS environment.
>
> **Chief of Security,**
> **Global Technology Firm**

About AppOmni

AppOmni, the leader in SaaS Security, helps customers achieve secure productivity with their applications. Security teams and owners can quickly detect and mitigate threats using unmatched depth of protection, continuous monitoring, and comprehensive visibility. Trusted by the world's largest enterprises, AppOmni specializes in securing diverse SaaS environments. Learn more at appomni.com.