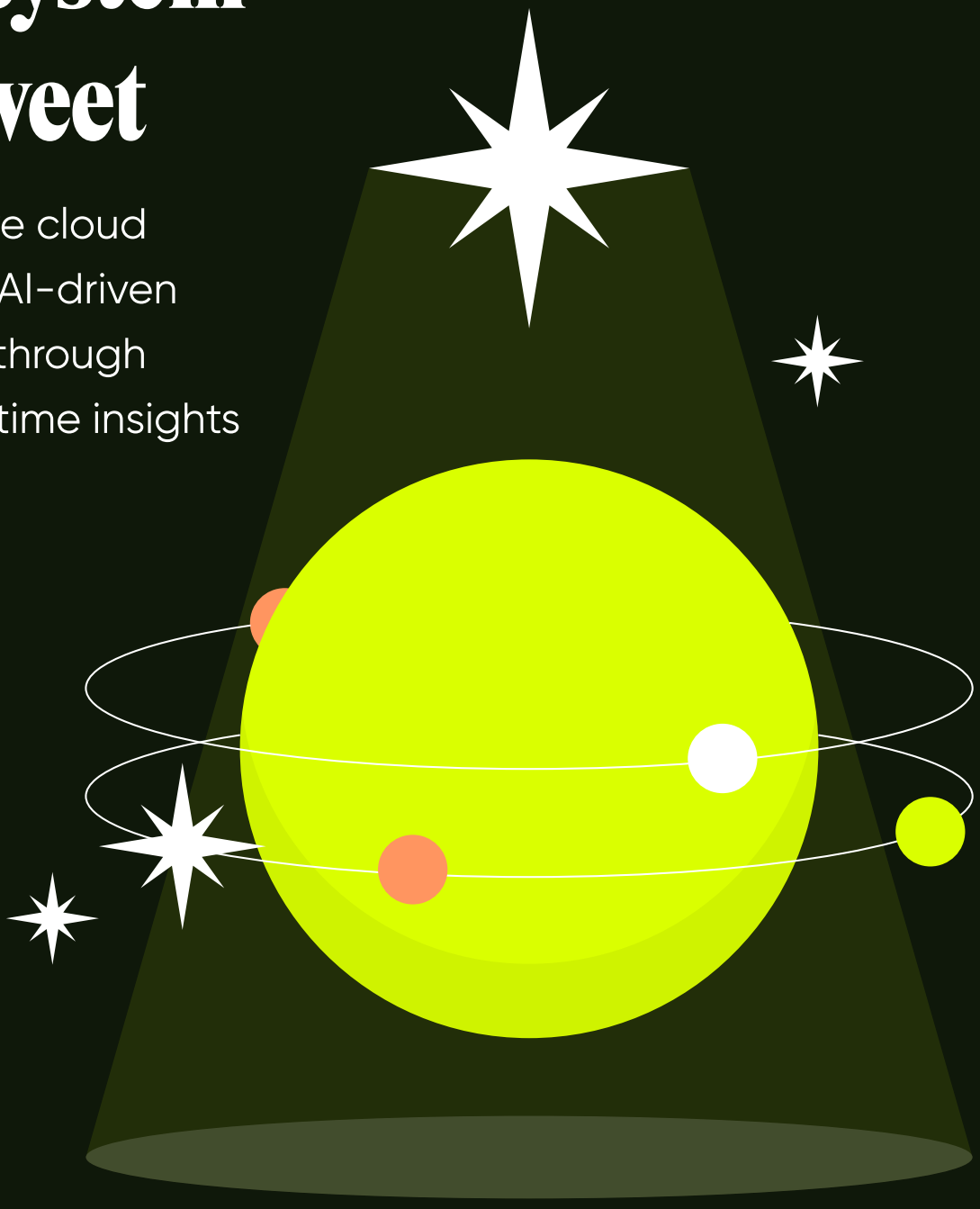
sweet.

Secure Your AI Ecosystem with Sweet

Comprehensive cloud protection for AI-driven environments through advanced runtime insights



www.sweet.security

From identifying AI agents to detecting sensitive data, Sweet ensures your AI models and their connected systems remain secure.

Comprehensive Visibility

Gain a clear view of all AI-related assets and their data flows.

Enhanced Security

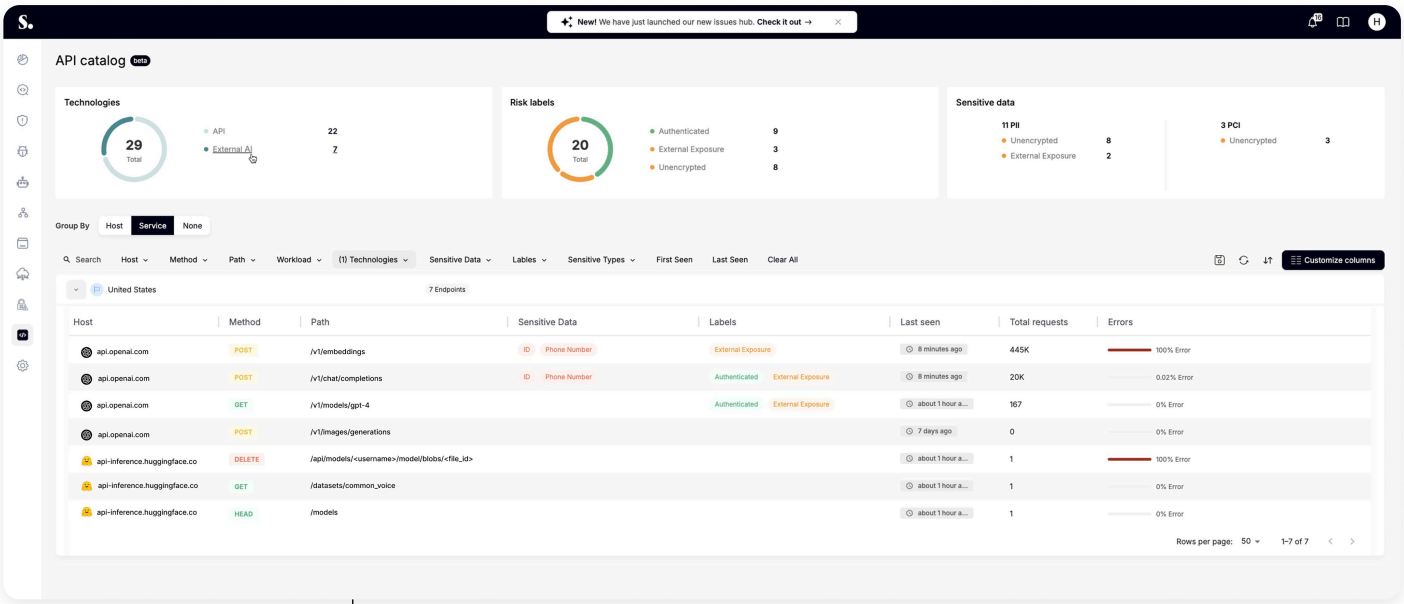
Mitigate risks across your AI infrastructure by addressing vulnerabilities and preventing sensitive data exposures before they escalate.

Real-Time Threat Detection

Continuously monitor AI infrastructure —including agents, models, and APIs —to detect and neutralize risks as they emerge.

Data Transparency

Ensure end-to-end visibility into sensitive data interactions.



Discovery of Shadow AI

Uncover and secure unauthorized or unmanaged AI systems within your environment.

Detect Shadow AI

Identify and control unsanctioned AI tools and models operating outside IT and security oversight, such as rogue APIs or unmanaged ML models.

Assess Risk Exposure

Prioritize and evaluate potential vulnerabilities and sensitive data exposure tied to shadow AI systems, ensuring the most critical risks are addressed first.

Take Control

Seamlessly integrate identified risks and insights into your existing workflows and remediation pipelines for proactive security management.

Inventory Management

Gain full visibility into all AI services and tools within your environment, both internal and external.

API-Based Discovery

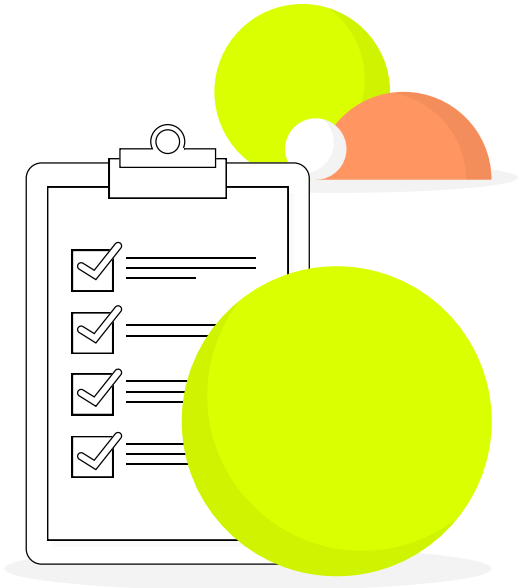
Automatically discover all AI services through API (L7) analysis, building a real-time inventory of AI agents and their data flows.

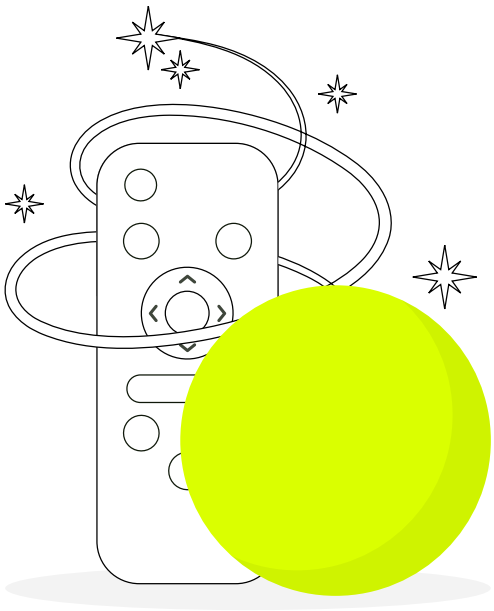
Internal and External AI Services

Detect external SaaS tools like ChatGPT and internal AI systems tied to Retrieval-Augmented Generation (RAG) databases.

Database Mapping

Identify and monitor databases feeding your AI systems to ensure data transparency and operational integrity.





AI Security Posture Management (AI-SPM)

Proactively manage and secure AI models in production.

AI Risk Detection

Identify and mitigate risks in AI workflows, such as vulnerable libraries, dependency issues, data poisoning, or adversarial inputs.

Policy Enforcement

Align AI model usage with compliance standards and organizational policies.

Risk Insights

Provide actionable insights to prioritize and mitigate risks associated with AI deployment.

Runtime Protection

Protect AI systems in real-time by identifying and mitigating security threats.

Sensitive Data Detection

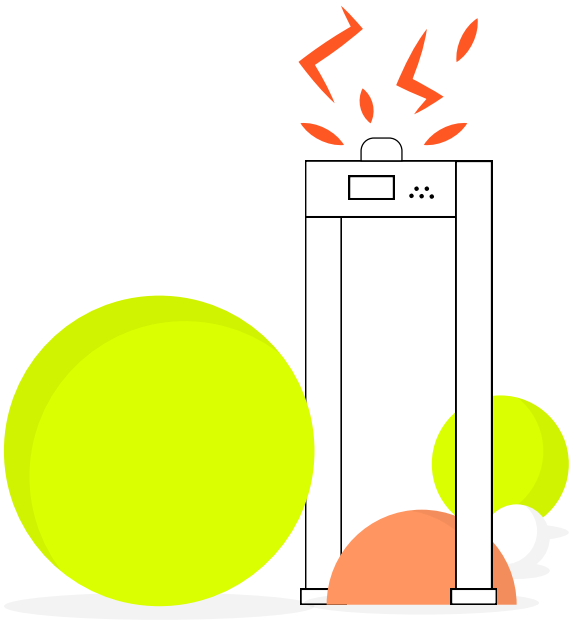
Monitor for Personally Identifiable Information (PII), secrets, and other sensitive data traversing AI workflows.

Secure Prompt Interactions

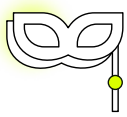
Utilize tools like LLM Guard to analyze and safeguard prompts in real time.

Incident Prevention

Stop incidents at the source with rapid detection and mitigation measures.



Empower secure AI adoption across your applications with Sweet



Shadow API Detection

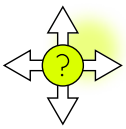
Identify hidden or unauthorized APIs that may expose sensitive data.

Sensitive Data Control

Prevent unintentional exposure of critical information through AI agents.

Compliance Tracking

Ensure AI usage aligns with regulatory and organizational standards.



Enhanced Decision-Making

Leverage runtime insights to drive secure and efficient AI deployments.