SALT

SOLUTION BRIEF

Ask Pepper AI: The Generative AI Assistant for API Security

Introduction

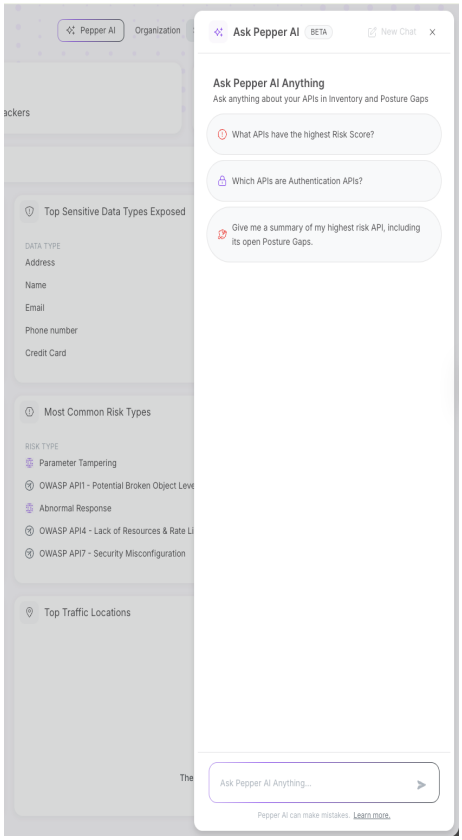
Modern API environments are vast, complex, and evolving faster than ever. With the rise of Agentic AI and Model Context Protocols (MCPs), the web of connections between services is becoming more intricate and harder to track. Security teams are often drowning in data—alert logs, inventory lists, risk scores, and posture gaps, struggling to keep pace with this new speed of innovation.

In the era of AI, security shouldn't require a manual. It should be a conversation. Ask Pepper AI transforms how teams interact with their API security data, allowing anyone to ask plain-English questions and receive immediate, actionable intelligence across their entire API lifecycle.

The Challenge: Complexity in the Age of Agents

As API portfolios grow into the thousands, finding specific answers becomes a bottleneck. Security teams face three distinct challenges, now amplified by AI:

- **The "Needle in a Haystack" Problem:** Finding the "highest risk API exposing PII" among thousands of endpoints requires multiple clicks and filters. This is made worse by Agentic AI, which creates dynamic, machine-to-machine connections that traditional dashboards struggle to visualize clearly.
- **The Skill Gap:** Junior analysts or developers may not know the specific terminology required to extract deep insights.
- **The Agentic Blind Spot:** New technologies like **MCP servers** introduce "hidden" infrastructure that connects LLMs to data. Identifying which of these connections is risky or unauthenticated often requires expert-level knowledge of the platform's query language.

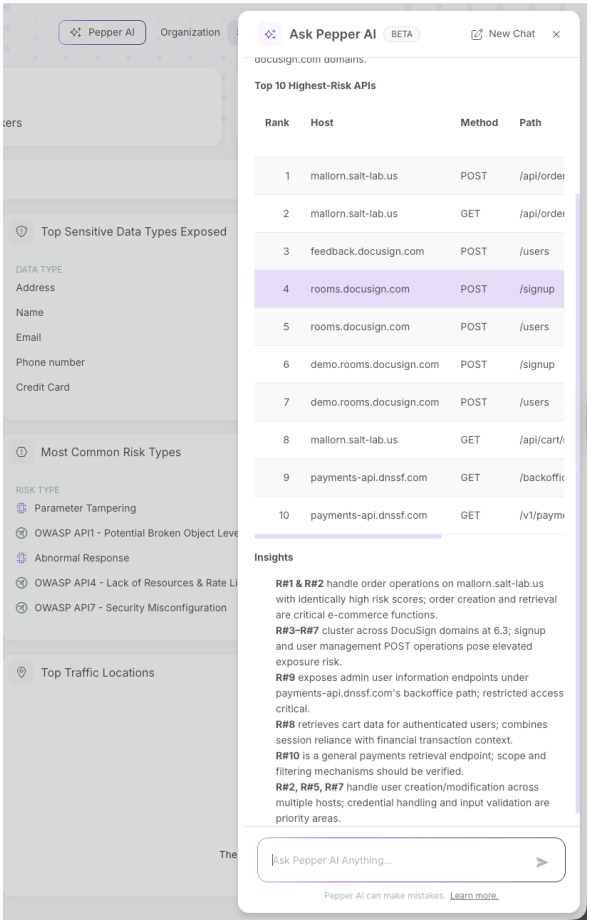


The Solution: Ask Pepper AI

Ask Pepper AI is a new, generative AI-powered natural language interface embedded directly into the Salt Security dashboard. Built on **Amazon Bedrock**, it serves as an always-on analyst that understands the context of your unique API environment.

Instead of building complex queries, you simply ask questions. Ask Pepper AI parses your intent, scans your entire data lake, spanning I**nventory, Posture, and Threat Intelligence**, and delivers a precise summary. It cuts through the complexity of Agentic AI and MCPs, turning data into dialogue.

Key Features & Benefits



- **Unified Data Querying:** Seamlessly query across all pillars of API security. Ask about **Inventory** ("How many shadow APIs do I have?"), **Posture** ("Which APIs fail our authentication policy?"), and **Threats** ("Show me APIs under attack").
- **Natural Language Interface:** No SQL or "filter hunting." Just type: "*Which MCP servers are exposing sensitive data?*" and get an instant answer.
- **Instant Risk Prioritization:** Cut through the noise by asking: "*What is my highest risk application?*" Ask Pepper AI instantly bubbles up critical issues, whether they stem from legacy APIs or new Agentic AI flows.
- **Context-Aware Insights:** It understands relationships. You can ask: "**Give me a summary of my highest risk API, including its open Posture Gaps**," and receive a consolidated report that simplifies complex attack chains.
- **Democratized Security Intelligence:** Empowers every team member, from CISO to analyst, to access deep insights without being a platform expert.
- **Powered by AWS Bedrock:** Leverages enterprise-grade security and performance to ensure safe data handling.

Conclusion

Don't let the complexity of Agentic AI slow down your security operations. Ask Pepper AI puts the power of the entire Salt platform behind a simple chat interface. By translating natural language into deep API insights, it enables teams to find risks faster, close gaps sooner, and govern their AI-driven future with confidence.