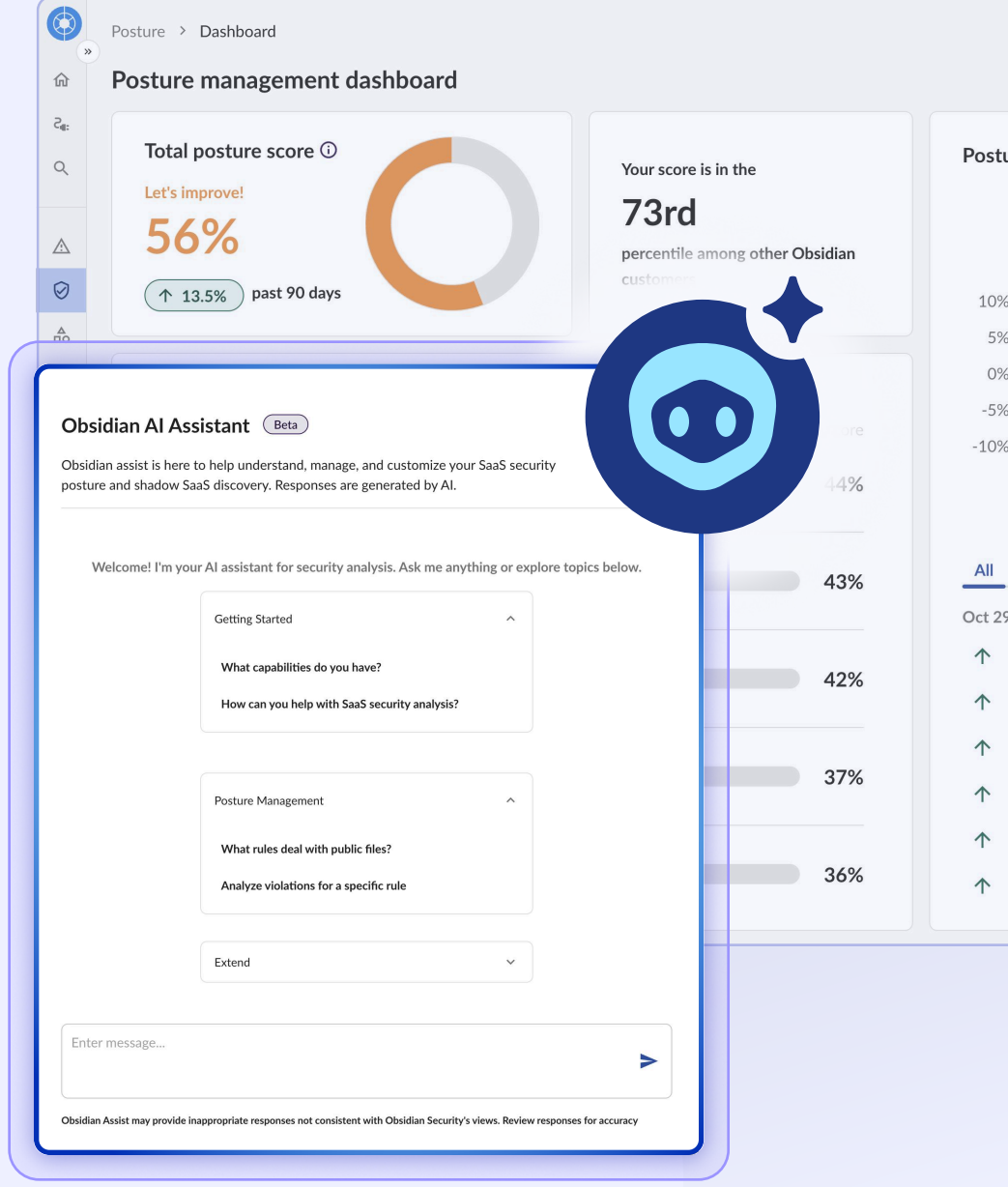
OBSIDIAN

Extend your security teams with Obsidian AI Assistant

Clarity, speed and confidence for security teams, built on the Obsidian Knowledge Graph

Obsidian AI Assistant is the tool to boost your security team's productivity.

Security teams today are stretched thin with countless posture violations and manual triage processes in the middle of SaaS and AI sprawl. Existing tools are able to capture the data but rarely connect the dots. Security teams don't need another noisy tool, they need an assistant they can trust. Obsidian AI Assistant, built on the powerful Obsidian Knowledge Graph, acts as an extension of your security team: explaining complex rules, triaging threats and managing exceptions for SaaS apps and AI Agents.



Extend your security teams with Obsidian AI Assistant

Explore what you can do with Obsidian AI Assistant.

Unlike generic copilots, Obsidian AI Assistant intelligently orchestrates across specialized agents across the Obsidian platform, ensuring every query is routed to the right capability. The result: stronger posture, faster investigations and confidence in every security action.

See what you can ask: real prompts that deliver real answers, organized by your use case:

Get clarity on technical rules and terms

Make policies understandable in plain language. Onboard your analysts faster, simplify collaboration with non security teams and cut through all the data to get what you need in seconds.

- Explain what this posture rule means on Salesforce “Salesforce sites with clickjack protection disabled”
- Show me all posture rules related to privileged accounts in Google Drive.

Spot posture violations that matter most

Surface posture violations that truly impact business risk and compliance within seconds and get prescriptive next steps to act safely and with confidence. Prioritize, triage and remediate the most critical violations first, improving posture while cutting wasted effort.

- Summarize all violations related to inactive accounts in the last 30 days for Snowflake
- Which posture violations in Okta are the most critical at this point?

Use AI Assistant as your first line of triage

Filter noise and use playbook driven reasoning to triage alerts step by step to reduce false positives and cut your mean time to resolution.

- Show me user identities with the most number of suspicious alert patterns
- Walk me through the reasoning for this suspicious token reuse #26 on ServiceNow.

See and control all SaaS

Uncover shadow SaaS, quickly summarize risk, and follow guided remediation steps to secure them.

- What are the riskiest shadow SaaS applications in my environment?
- how can I secure Perplexity from unfederated usage?

Get audit-ready evidence on demand

Show how posture rules are enforced, their exceptions and how they map to regulatory frameworks. Compliance teams get full clarity, speeding up audit prep timings.

- Show me which rules in Google map to SOC2 requirements
- Explain how our SaaS posture supports HIPAA compliance for protected health data for Okta