Sola Docs

Getting Started

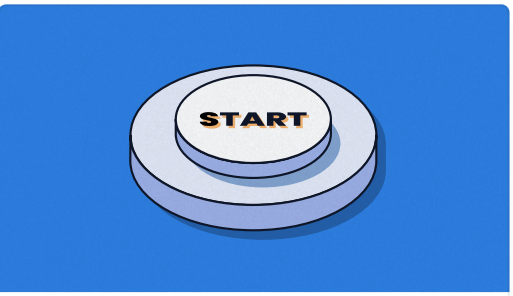
Welcome

From security questions to solutions in minutes

Sola is an AI-powered security solution that connects to your tech stack, automatically builds your complete security system, and uncovers what matters most.

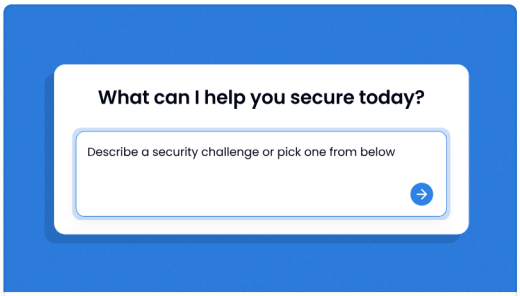
How can we help?

Ask your question in the search above, and our AI assistant will guide you.



Quickstart

No fluff, just actions

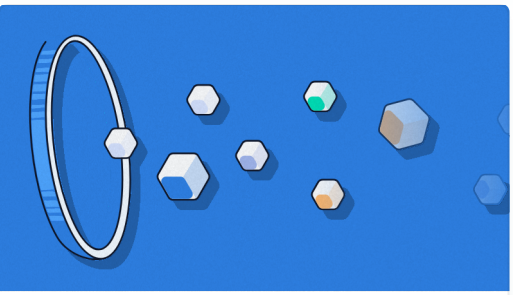


Sola AI

Build your security app, fast

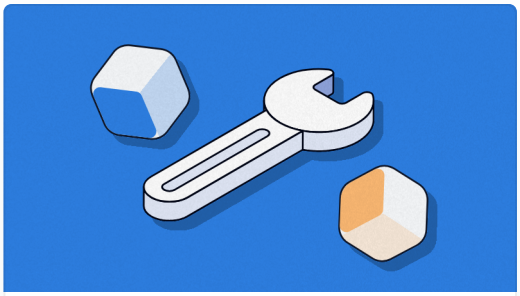
What's New

Stay up to date



Data Sources

Plug in your data

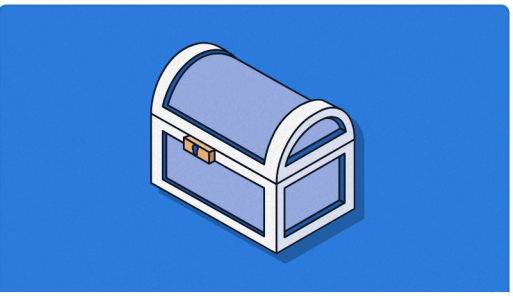


Connectors

Act on findings

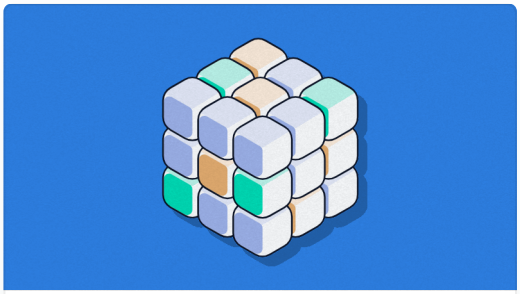
FAQs

You're in good company



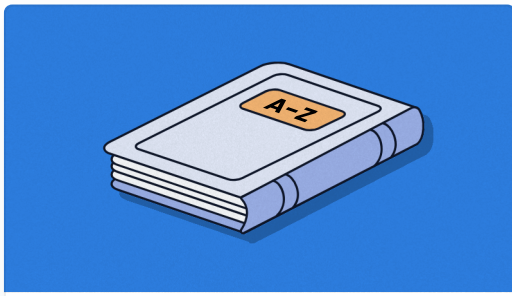
Security and Privacy

We practice what we preach



App Gallery

Start with a template



Glossary

Jargon, decoded

Quickstart

Create your own security solutions

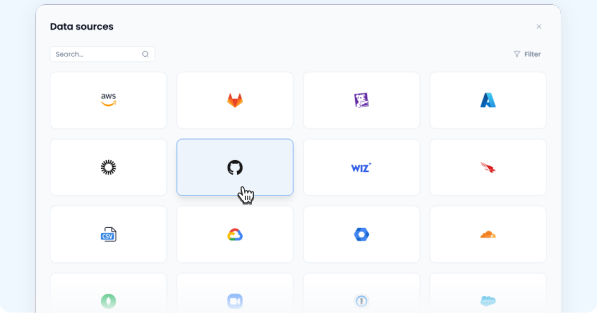
Sola makes it easy to get security done, your way. Follow these steps to get up and running.

Step-by-step guide

1 Connect your data sources

You'll need them to answer your questions.

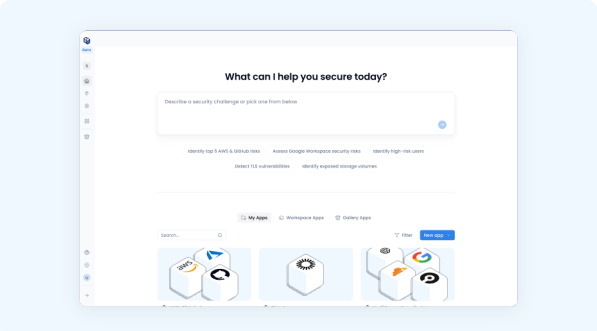
> Don't have access to connect your data now? Skip this step and complete it later.



2 Build your app with Sola AI

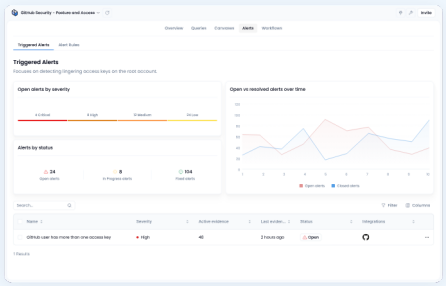
Describe your security challenge in your workspace home. Sola AI will build an app for you, complete with queries, alerts and dashboards.

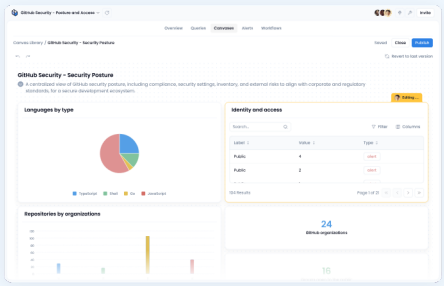
> **Pro tip:** Use our ready-made prompts to easily get started.



3 Explore triggered alerts and canvases in your app

See what Sola uncovered, and start reviewing to investigate and resolve issues.





Overview

Security is now simple

Welcome to Sola!

Sola is an AI-powered cybersecurity platform that allows practitioners of all skill levels generate security solutions in minutes.

Here you can create the security space that you need.

Answer security questions

From **everyday risks to large-scale threats**, every security solution begins with a question.

Create your own security solution by asking questions.

Cover missing security gaps

Even with the best-of-breed security tools, there's always going to be a **missing piece**!

Create your own security solution by defining what's missing.

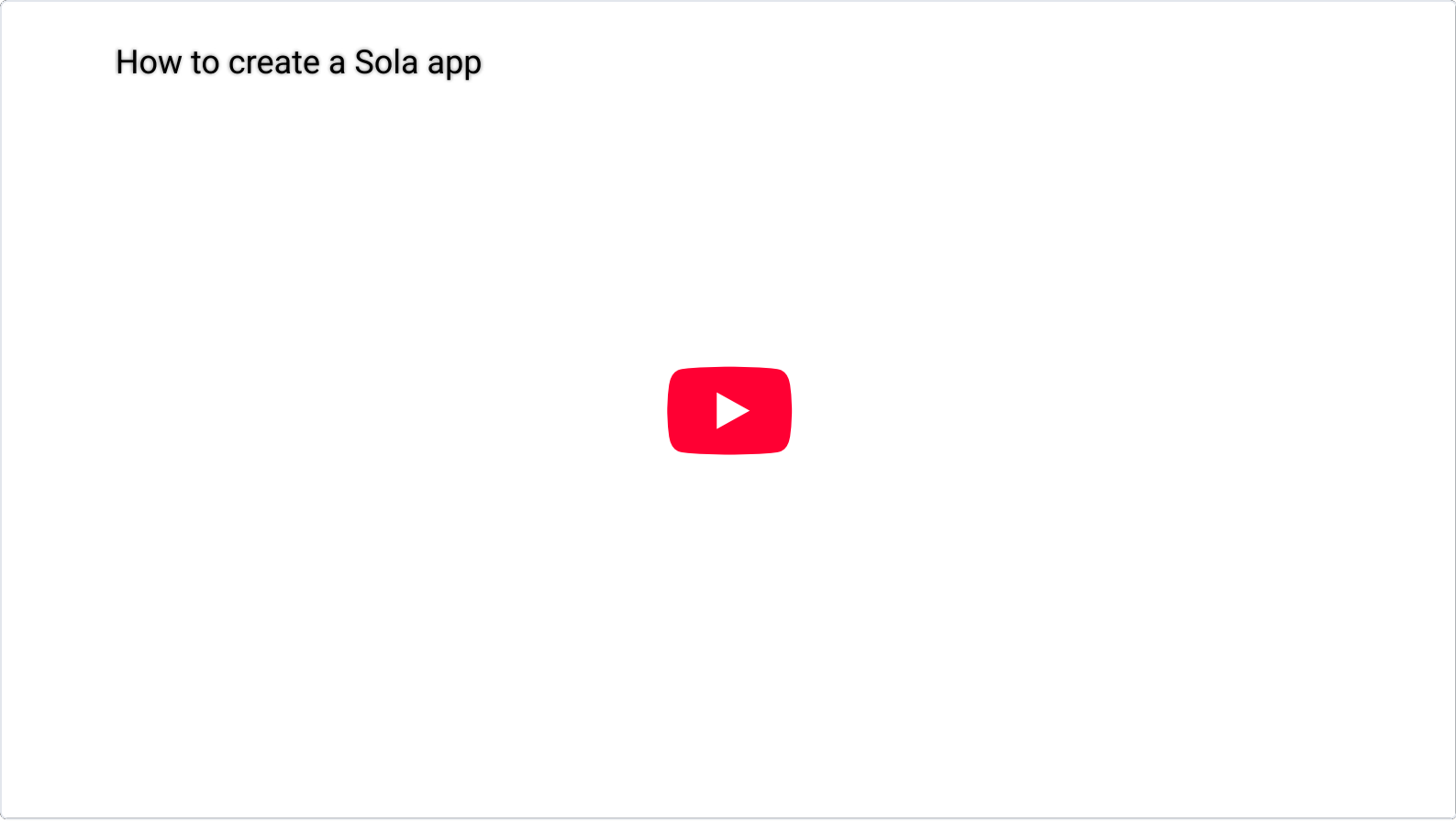
Discover expert-built security solutions

You don't have to start from scratch.

Create your own security solution by using ready-to-use security apps, and customize them to fit your needs.

This is where Sola comes in.

Sola provides you with a studio to get answers to your security questions, and build your custom security tool. All within an easy to use, collaborative environment that incorporates AI tools throughout.



How to build a Sola app

How Sola works

Sola users create and customize their own unique security solutions their way, without any barriers that large-scale security solutions have.

As part of the Sola studio, Sola apps are used to create custom security solutions for specific security use cases.

Apps are composed of 4 building blocks.

Queries for data inquiry. Use queries to **create**, **view**, and **share data insights** that answer your cyber security questions.

Canvases for data visualization. Create canvases to build **dashboards**, **reports**, and **interactive views** that display your insights and results in easy-to-understand **tables**, **charts**, and **graphs**.

Alerts for monitoring and alert rules. Convert your important questions into alerts to **track security risks and get notified** when important events occur.

Workflows for **automation** and **remediation**. Automate security actions to **respond faster and reduce manual effort**.

Create security solutions, your way

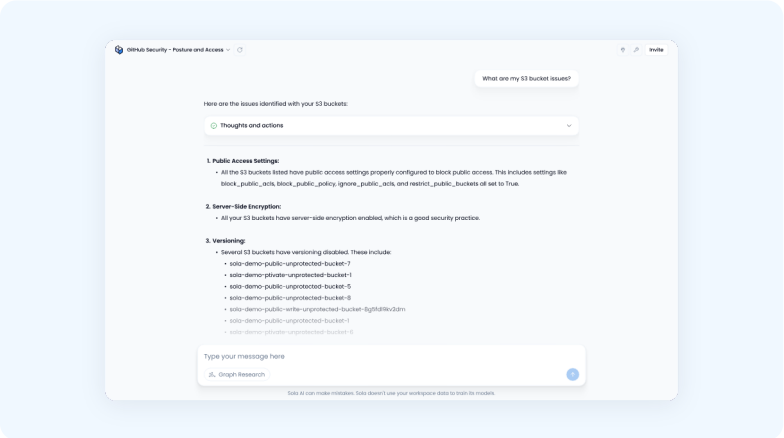
Sola AI

Build security solutions with AI security expertise

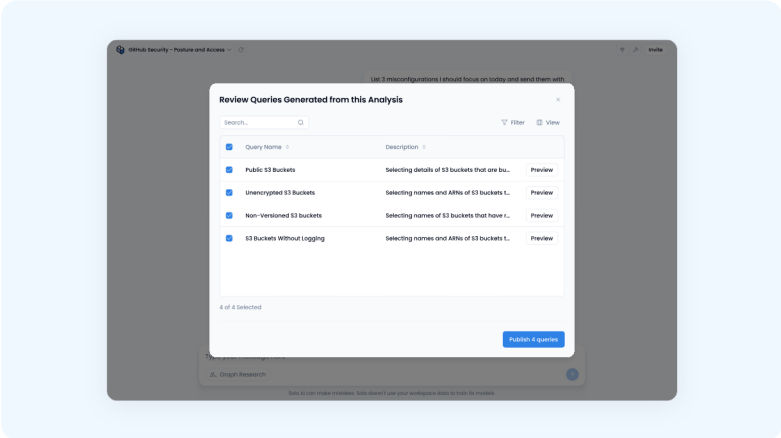
The intelligence behind your security apps

Sola AI is your built-in security expert. Use it to uncover security risks, generate insights, and build custom security apps.

Sola AI guides you as you explore your environment, and uncover what matters most.



Build apps with Sola AI



Suggested queries from Sola AI

Build security apps

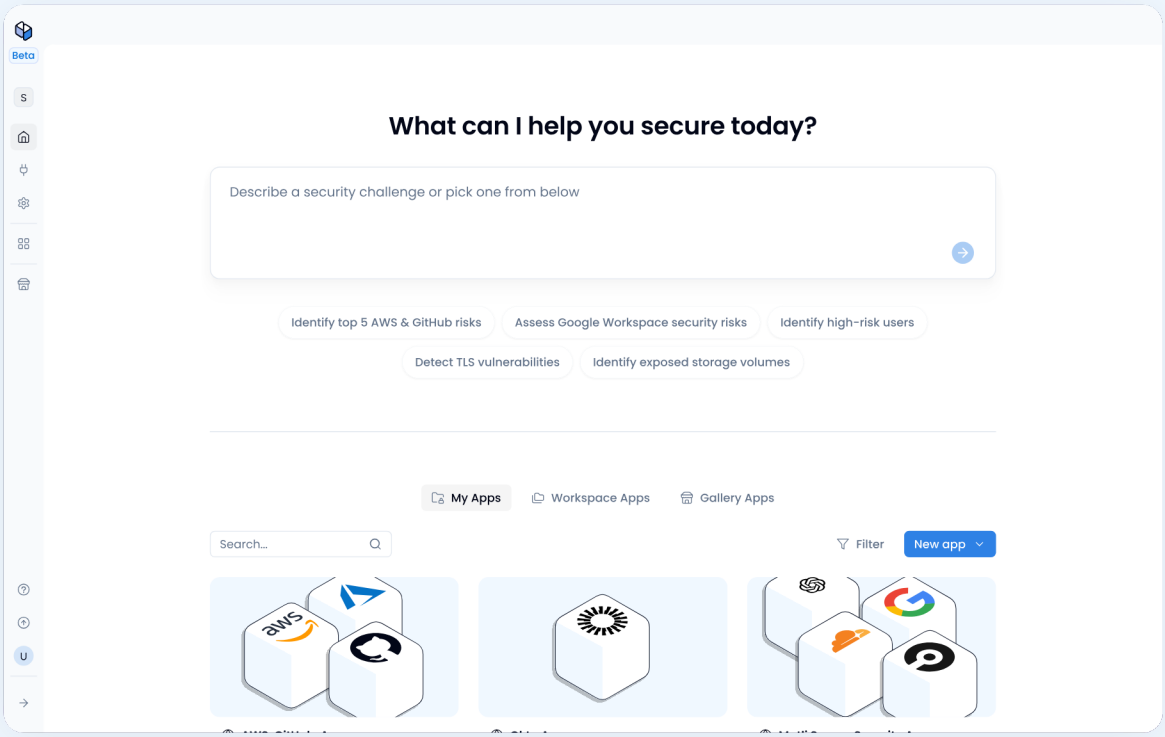
Start with a security concern and get a working app, complete with queries, dashboards, and alerts tailored to your use case, in minutes.

How it works

Go to your workspace home and submit a prompt describing your security challenge. Sola will start building a new custom app automatically and navigate you to it.

Sola AI prompt tip ✨
Use our ready-made prompts to easily get started.

Once your app is ready, you'll see a full summary of what the app monitors, why it matters, the security context, and key security insights from your environment.



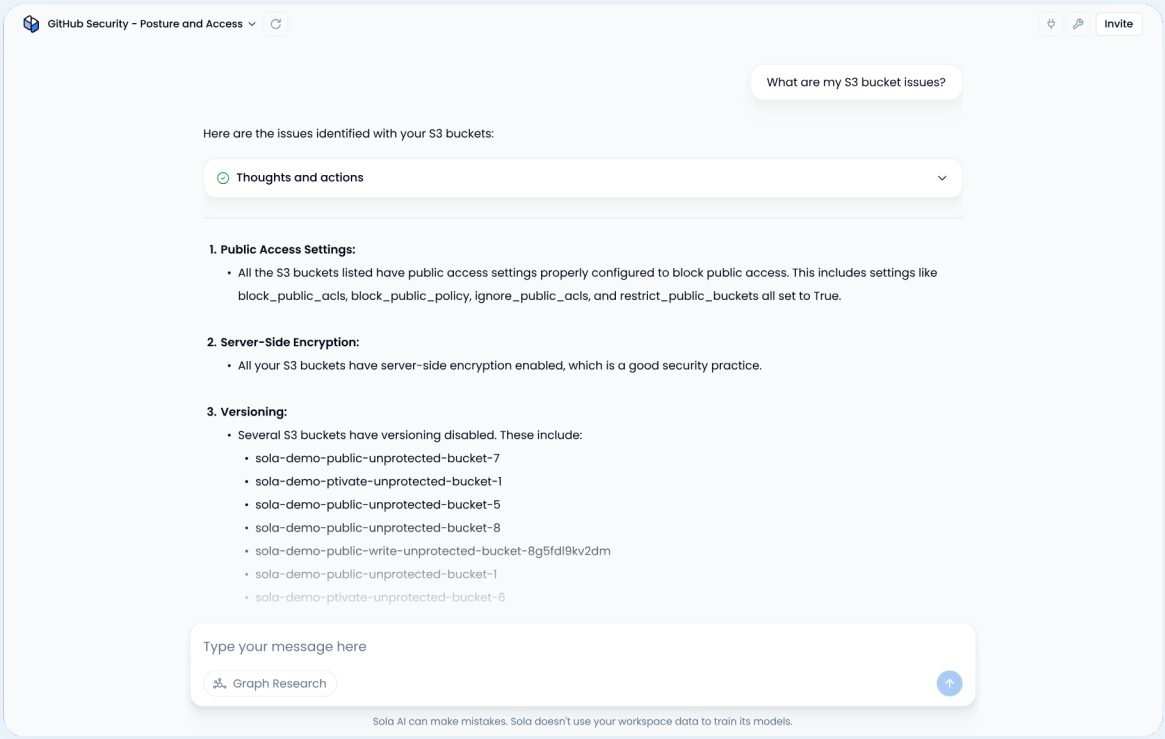
Build an app for your security needs

Gain deeper insights into your security posture

Each app includes a dedicated Sola AI copilot to help you investigate your environment and uncover security risks, gaps, and exposures across your app data sources. Sola AI provides detailed, actionable insights to help you understand and prioritize remediation.

How it works

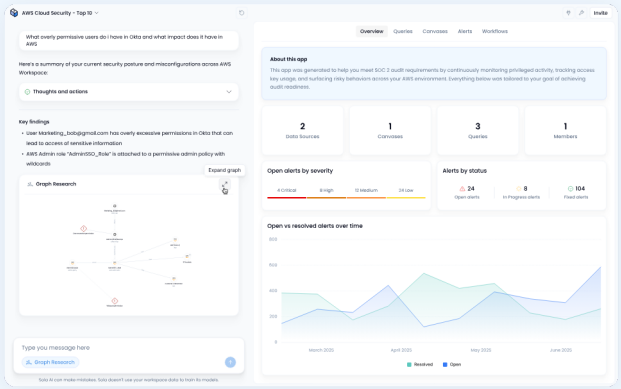
Go to your app, and ask a security question. Sola AI will analyze your connected data and provide detailed insights about what was detected, why it matters, and the queries used to generate these insights.



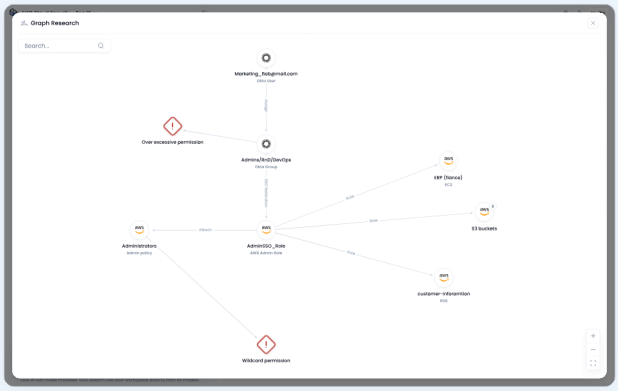
Key security insights from your environment

Graph-enhanced research

Uncover deep insights with graph research, an advanced reasoning mode in Sola AI that maps the relationships between resources, controls, and risks across your connected data. It provides complete, grounded answers to complex questions, backed by visual evidence and contextual analysis.



Graph research mode in AI copilot



Graph research visual representation

Expand your apps with new queries, canvases, alerts, and workflows

✨ Grow your app, one prompt at a time.

Use the Sola copilot to generate new queries, alerts, and canvases directly within any existing app. This allows you to add more coverage, track new risks, or build purpose-specific views

Sola AI prompt tip ✨

Ask specifically for the queries, alerts, or dashboards you want to build.

For example: “Create a dashboard for my executive team that summarizes open critical vulnerabilities.”

How it works

Go to your app and describe what you need, such as an insight, alert flow, or dashboard. Sola AI will create the new resources based on your prompt, and add them for you.

Asking for canvases or alerts also creates the required queries.

Use this to:

- Build multiple canvases in a single prompt. For example: "Create a comprehensive security dashboard for my CISO, and a high-level one for my CEO"
- Keep everything you need in one app.
- Add use-case-specific dashboards for different teams.
  For example: DevOps, Engineering, Executives
- Expand existing apps as your risk coverage grows.

Sola AI in queries

Access Sola AI from within any query in the queries tab to explain, refine, or optimize individual queries as you build. It can help you identify the right tables and columns that contain the data you need or refine SQL syntax for more accurate results.

Graph Research

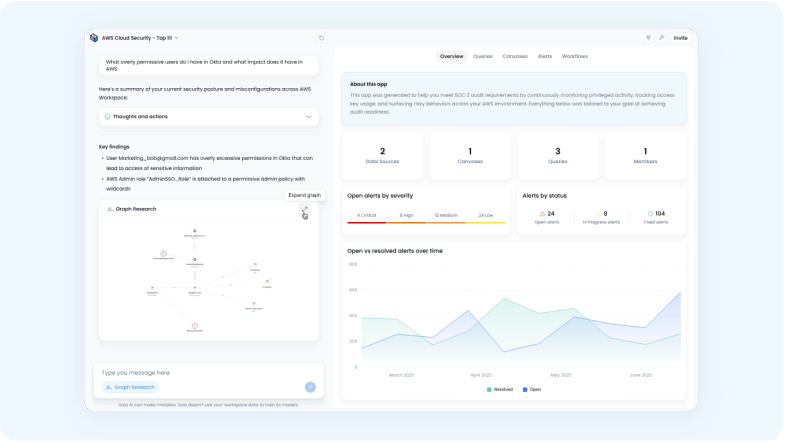
AI with unparalleled visibility into your environment

Graph research is an **advanced reasoning mode in Sola AI**. In this mode, Sola AI maps the relationships and connections between resources, security controls, and risks across your app data sources.

It uses **Sola's proprietary security graph** based analysis infrastructure and framework, to answer complex questions with a holistic view, contextualized data, and visually-backed responses.

This allows Sola to surface deep insights, providing:

- **Enterprise-grade reasoning** - Responses are grounded in a security graph built from Sola's domain expertise.
- **Valuable insights for complex cross-environment analysis** - Each insight is traceable to relationships across entities and controls.
- **Security intelligence built-in** - Combines context-aware reasoning with proven knowledge of risk, exposure paths, and misconfigurations.
- **Natural conversation, intuitive results** - Ask your security question, Sola AI will analyze, map and generate a visual representation of your assets, identities, and security controls.



Graph research mode in AI copilot

Graph research visual representation

What graph research reveals

Graph research goes beyond basic analysis to provide you with contextual, robust, precise responses, with additional insights that are based on your connected data.

Each answer is complete and grounded in real security context, validated through identified connections between assets and controls.

- **Connection insights** - Surface previously unseen connections and dependencies between different types of environments and assets
- **Toxic combinations** - Detect risky interdependencies across platforms (e.g. overly permissive GitHub access combined with exposed AWS assets).
- **Blast radius for critical issues** - Understand the full scope of impact from a single misconfiguration or compromised entity.
- **Security impact on infrastructure** - Trace how issues in one part of your environment affect services, workloads, and teams elsewhere.

Visual representation of graph research

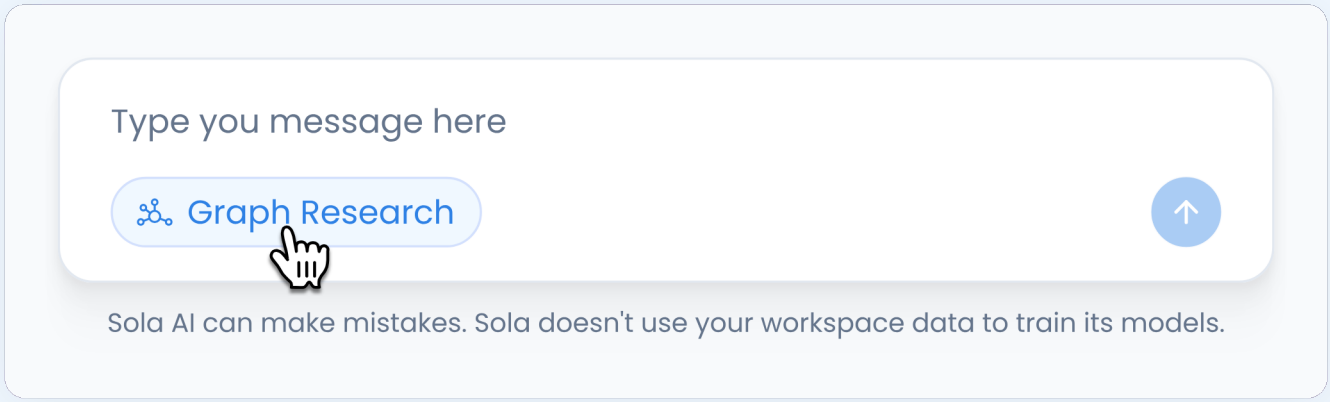
Sola AI provides a visual representation of relationships between assets and security controls.

The response includes a dynamic visual graph that illustrates:

- How different systems, users, and controls are connected
- Where risks originate and how they can spread
- Which assets are impacted and how they relate to one another

How it works

When the graph research mode is enabled, Sola AI automatically decides when to activate it.



For simple queries like “Who are my admin users?”, standard analysis is enough. For deeper, cross-system questions, Sola turns to graph research to generate an accurate response grounded in security knowledge and contextual data.

Sola's graph is built from proprietary knowledge of cybersecurity architecture and risk patterns, that maps the connections between a wide range of asset types, security controls, and their relationships.

This knowledge is combined with your organization's connected data sources to create a graph of real-time entities (such as users, roles, buckets, workloads, and more) and security controls (such as IAM, access levels, encryption, MFA, and more).

When analyzing a question, Sola AI:

- Identifies relevant asset types.
- Discovers meaningful relationships and connections across systems.
- Generates grounded traceable insights based on entity interconnections.

FAQs

What is graph research in Sola AI?

Graph research is an advanced reasoning mode in Sola AI that analyzes relationships between assets, identities, and security controls. It generates contextual answers based on how risks, misconfigurations, and dependencies connect across your environment.

When is graph research activated?

Graph research activates automatically when Sola AI determines that a question requires deeper, multi-system reasoning. For example, it may come into play to answer questions like "What issues exist across my AWS and GitHub and their relationship?"

What makes graph research different from regular analysis?

Graph research leverages Sola's proprietary security graph that maps entity relationships, revealing paths of risk, cross-platform dependencies, and high-impact security controls.

Can I turn off graph research?

Graph research is an optional mode. You can enable or disable it from the Sola AI copilot chat. Disabling Graph Research helps keep responses quick when deep reasoning isn't necessary.

Prompt Guide

Tips, ideas, and best practices for building with Sola AI

Sola AI helps you build, explore, and investigate your security posture. A clear prompt gives Sola the context it needs to deliver the right output, faster and with better focus.

This guide explains how to write effective prompts for Sola AI. It shares practical tips and examples, drawn from real usage in the field, to help you get better results.

For now, the focus is on **building canvases with Sola AI**. More best practices will be added over time.

> **Prompting with Sola AI is a collaborative process.**
>
> Start with a clear direction, refine with follow-ups, and use the recommendations Sola provides to shape the right app, canvas, or insight.

How to use this guide

Prompting in Sola AI can serve different goals, from creating new apps, to building canvases, to investigating risks, and creating workflows.

This first version focuses on canvas best practices. The recommendations are not strict rules, but tips you can apply as needed to get better results.

Canvas best practices

These best practices are grouped into three themes: Start, Refine, Expand, and Troubleshoot.

1. Start

Begin with broad prompts to set the direction.

✨ Start broad, then iterate

Provide Sola AI with a general theme and refine your prompt step-by-step until the output matches your needs.

For example,

- “What are my top AWS security issues?”
- “Show me insights on GitHub access risks.”

✨ Keep prompts short and clear

Sola AI works best with concise prompts. While prompts can be up to ~3000 characters, shorter inputs are more effective and easier to refine.

For example:

- **Less effective**: “Create a canvas with detailed breakdowns of all services, including every AWS account, Okta user, GitHub repo, permissions, vulnerabilities, and historical changes...”
- **Better**: “Show me my top AWS security issues, grouped by account, with a chart of failed logins.”

✨ Reference your data

Start with referencing specific queries and ask Sola AI to create a canvas based on these queries or app data.

For example,

“Create a canvas based on the queries for inactive Okta users and failed logins.”

> ⓘ As a best practice, before starting a new canvas, make sure relevant queries already exist for what you want to build. If any are missing, Sola AI will complete them automatically as part of the canvas creation.

2. Refine

Shape Sola’s output to better match your needs.

✨ Add layout and structure early

Include any layout or style that you have in mind as early as possible, even in the first prompt. The earlier you set expectations, the better Sola can match your vision.

For example,

- “Show me my top AWS security issues, split into sub-pages by logical grouping, and make it Star Trek themed.”

✨ Give Sola context

Use Sola terminology, such as “canvas”, “app”, “app queries”, and “integrations”, to help Sola AI understand your intent.

Be specific about chart types or views if you want them.

For example,

- “table of admin users”
- “bar chart of open vulnerabilities by repo”

✨ Use interactive elements

Sola canvases can include interactive features to make insights more actionable.

For example:

- Add links to view the underlying data or queries.
- Highlight data trends with arrows and colors.
- Include toggles or tabs for different views.
- Add insights that summarize trends automatically.

3. Expand

Grow and explore beyond the basics.

✨ Invite clarification

Ask Sola AI to confirm before building. This helps align expectations and save time

For example,

- "Before you start building, make sure everything is clear. Ask me any clarification question you might have"

✨ Ask the Sola AI copilot

When in doubt, ask Sola AI what it can do. This will help you discover new directions.

For example,

- “What kind of canvases can I build from this app?”
- “What insights can I generate from this data?”
- “How do workflows work?”
- “What can I do with canvases?”

4. Troubleshoot

Fix issues and polish your canvas.

Even with clear prompts, canvases may need some adjustments. With Sola AI, if something doesn’t look right, you have the tools to fix it.

✨ Refine the prompt

Re-run with a smaller scope or clearer instructions.

✨ Tweak the layout

Resize charts, adjust text, or move elements directly in the canvas editor.

✨ Check for UX issues

Adjust overflowing text, small buttons in tabs, or charts that don’t fit well.

Use queries as building blocks

If a visualization isn’t working, make sure the underlying query returns the data you expect.

✨ Iterate with Sola AI

Ask the copilot to adjust or fix issues, such as:

- “Make the chart labels shorter.”
- “Increase the tab button size.”
- “Move the legend to the right side.”

Advanced ideas

Once you’re comfortable with the basics, try creative prompts to push canvases further:

- “Build a CISO dashboard and a separate engineering dashboard, each on its own tab.”
- “Make a canvas themed for executives with high-level summaries and traffic-light colors for risk.”
- “Add a toggle that switches between today’s results and 30-day trends.”
- “Show MFA adoption over time with arrows indicating increases and decreases.”
- “Add links from charts to the queries powering them.”

This guide will continue to grow with more best practices.

App Gallery

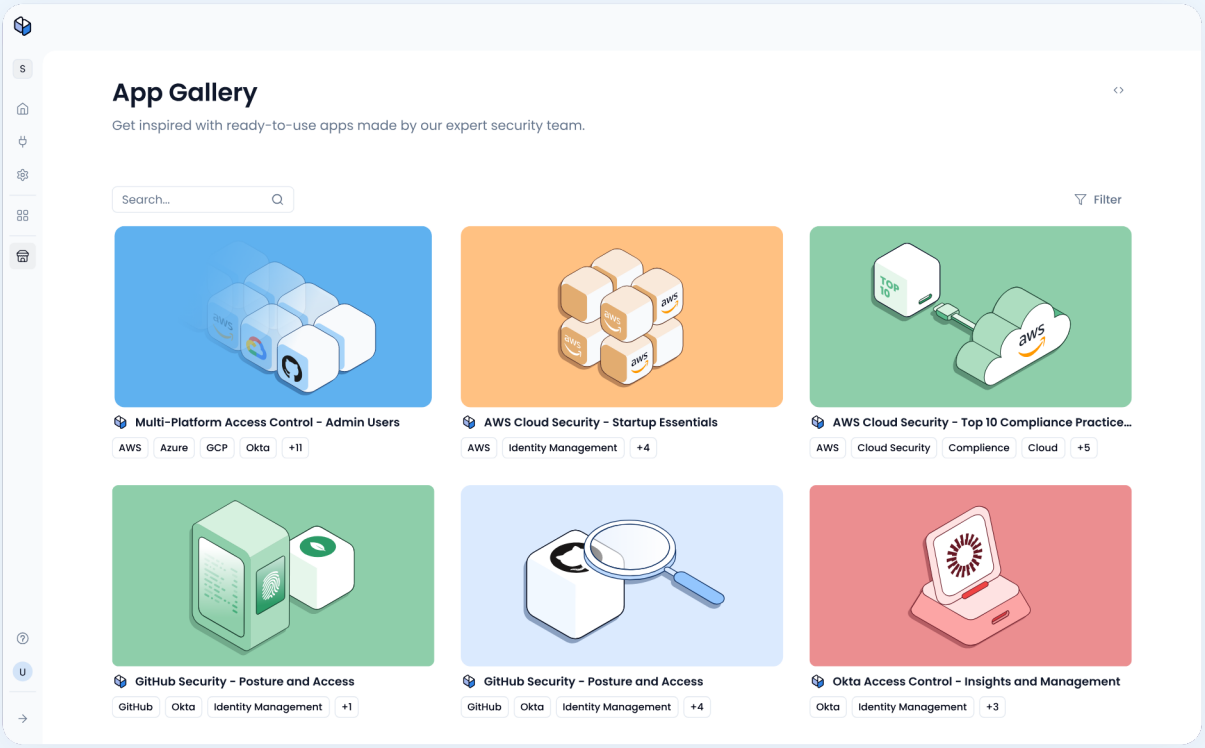
Get inspired with ready-to-use apps made by our expert security team

Explore expert-built security apps

Browse ready-made apps designed by security experts.

Each app is built to help you answer critical security questions, track risks, and strengthen your security posture—without starting from scratch.

Start exploring the app gallery ↗.



Sola App Gallery

Customize to make it your own

Every app in the gallery can be customized. Start with a template, modify queries, adjust dashboards, and set up alerts to tailor it to your specific security needs.

Start exploring the app gallery ↗.

How it works

1 ## Browse the gallery and install an app

Find an app that aligns with your security focus, and add it to your workspace.

2 ## Connect the app to your data

Add your data sources to gain insights on your environment.

3 ## Customize your app

Adjust queries, visualizations, and alerts, to fit your needs.

What's New

Release notes: Get the latest updates, features, and news from Sola

September 17, 2025

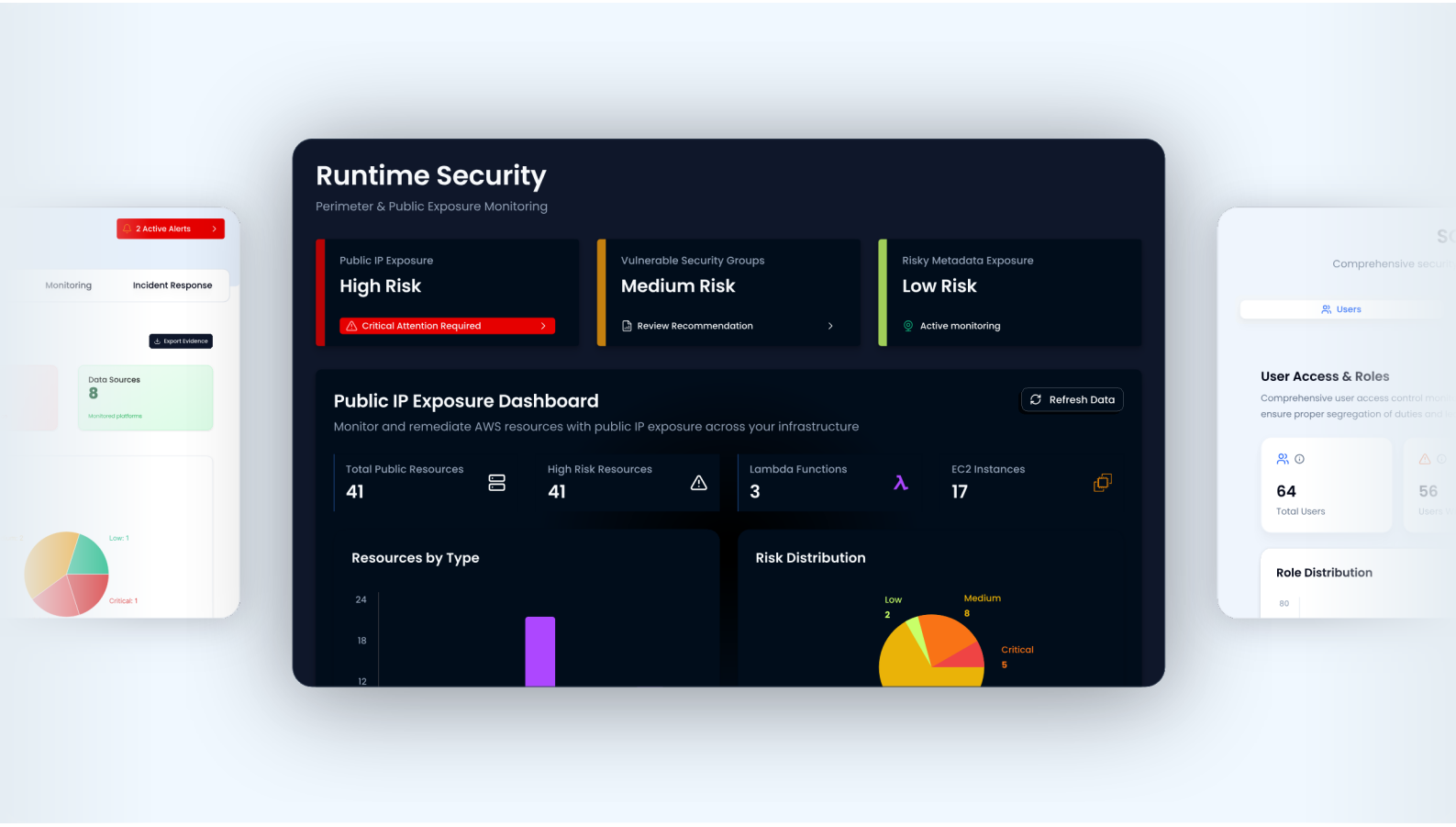
Here's the latest on what's new and improved at Sola.

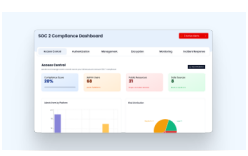
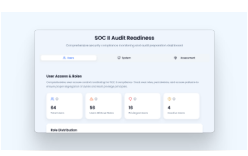
✨ *New*: Vibe canvases

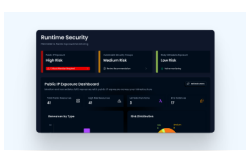
Transform security data into fully customizable interactive interfaces.

Vibe canvases let you create dynamic charts, tables, and guides with natural language prompts, giving you unlimited flexibility in layout, style, and use cases, from monitoring cloud posture to building executive reports, and more.

ⓘ See the Prompt Guide ↗ for tips and examples to refine your prompts and get the best results.



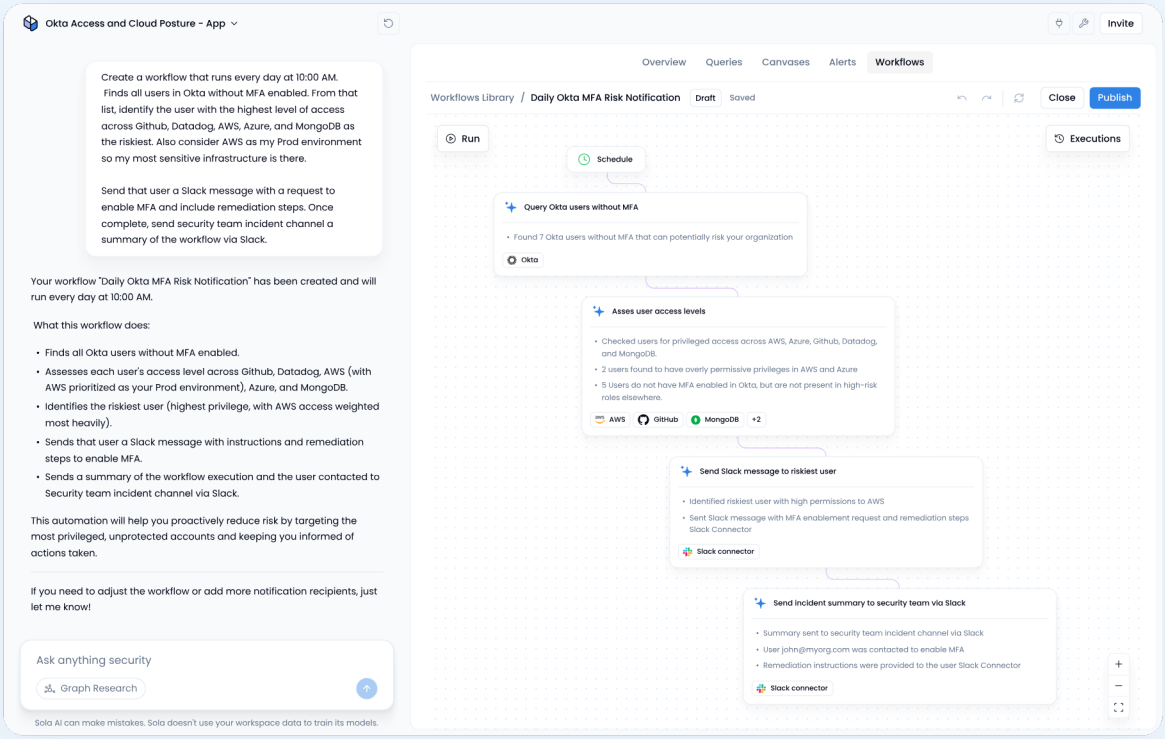




✨ *New*: Agentic workflows

Structure and automate security operations with AI-native flows.

Agentic workflows bring intelligent step-by-step orchestration to your apps, enabling investigations, remediation, and reporting across data sources and connectors. Built with Sola AI, workflows combine reasoning with automation for flexible, transparent, and resilient execution.



[Try them now in your apps ↗]

[📣 Read the full release notes]

September 17, 2025

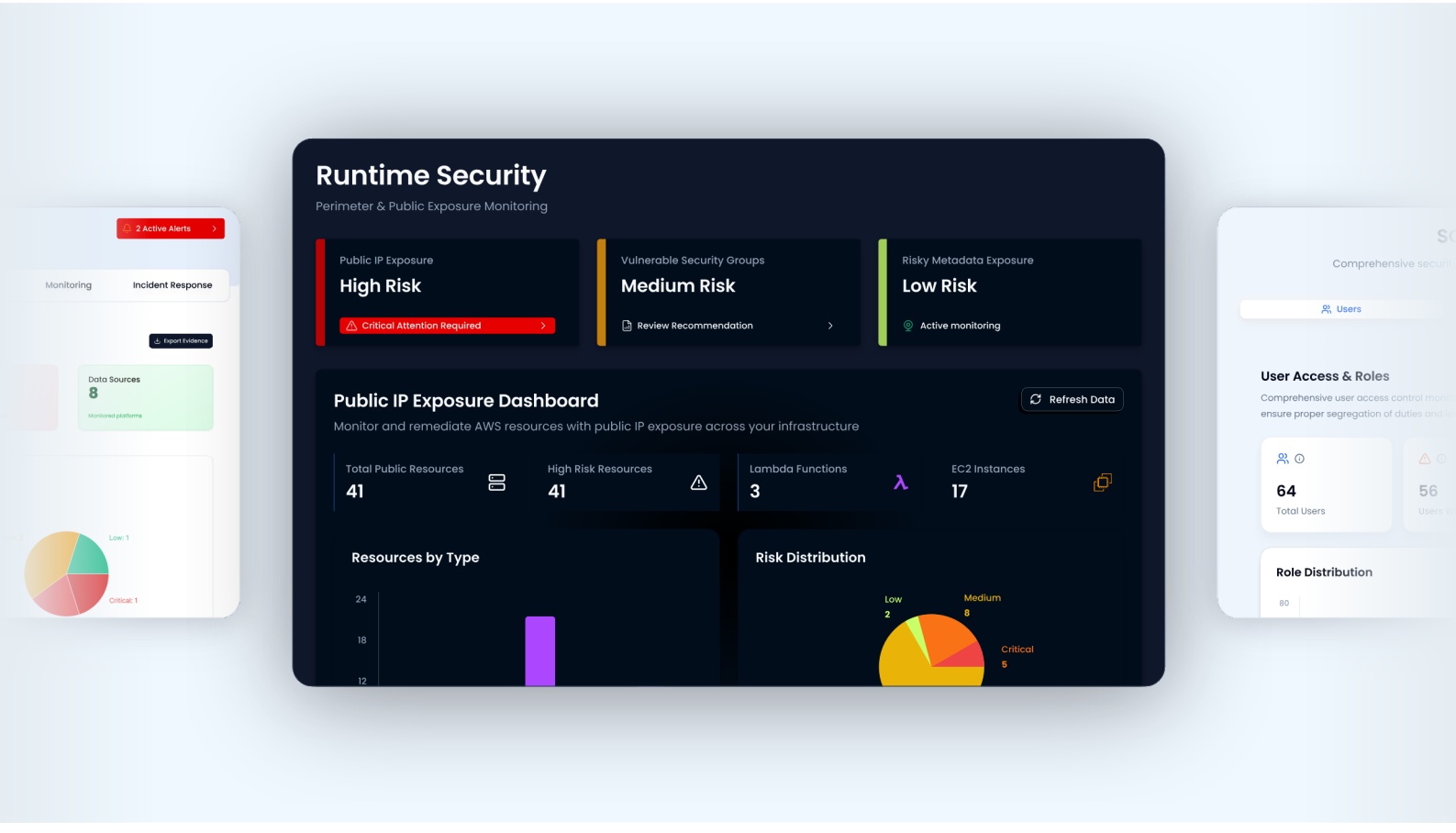
Release notes

✨ *New*: Vibe canvases

Transform security data into fully customizable interactive interfaces.

Vibe canvases let you create dynamic charts, tables, and guides with natural language prompts, giving you unlimited flexibility in layout, style, and use cases, from monitoring cloud posture to building executive reports, and more.

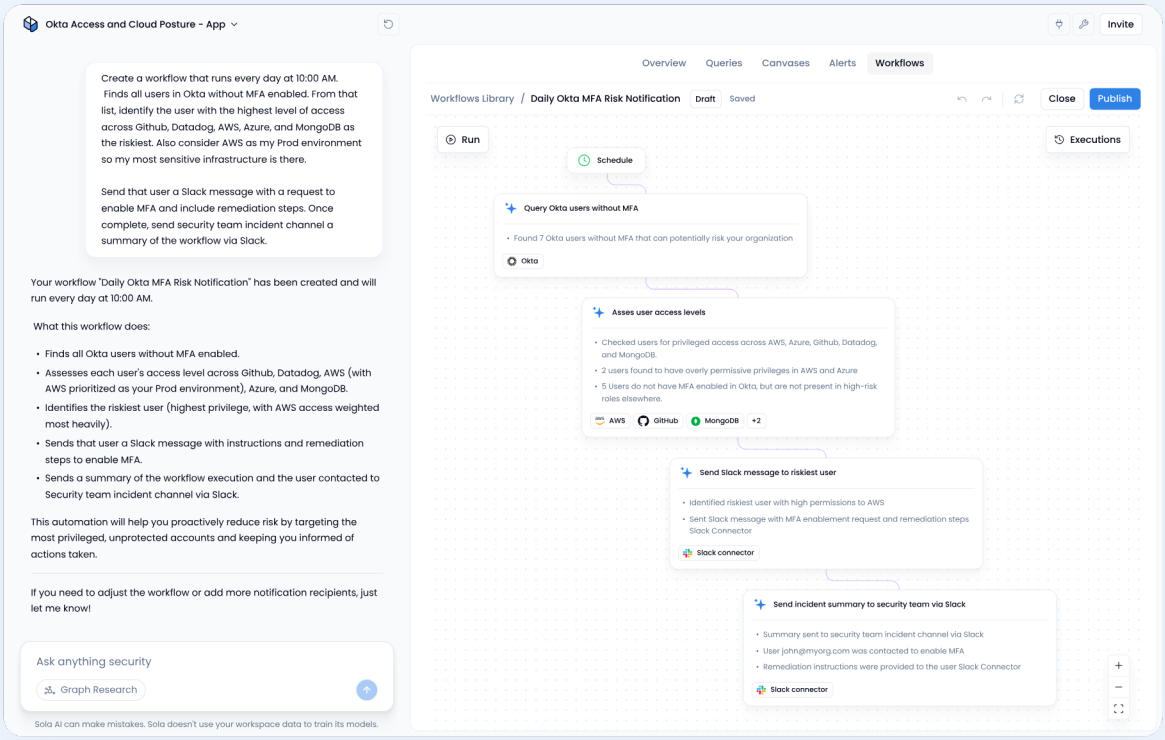
ⓘ See the Prompt Guide ↗ for tips and examples to refine your prompts and get the best results.



✨ *New*: Agentic workflows

Structure and automate security operations with AI-native flows.

Agentic workflows bring intelligent step-by-step orchestration to your apps, enabling investigations, remediation, and reporting across data sources and connectors. Built with Sola AI, workflows combine reasoning with automation for flexible, transparent, and resilient execution.



Notes and reminders

Stay tuned for more coming soon! 🚀

—

The Sola Team

September 10, 2025

Release notes

✨ Sola AI

Send CSV to Slack

Send any CSV export from Sola AI directly to Slack as part of a message, making it easier to share data with your team in real time.

Try it now ↗

Sola Studio

Explore data over time with historical snapshots

Access historical snapshots of your data in Sola to explore the history of your data, investigate changes in posture and configurations, using queries or by asking Sola AI. To activate, include "*snapshots*" in your prompt or toggle on "Include historical snapshots" in the SQL query window.

For example, ask Sola AI to:

- Show AWS EC2 inventory across multiple data snapshots.
- Investigate snapshots of Github users granted admin access in the last few days.
- Find Okta role or policy that has changed in the last 3 days across snapshots and how.

Integrations

Data Sources

***New*: SentinelOne**

Integrate SentinelOne to monitor endpoint agents, threat detections, vulnerabilities, installed applications, and security policies.

***New*: Jira Cloud**

Integrate Jira Cloud to surface issue and project data, enabling visibility into remediation projects, tasks, sprints, boards, users and more.

New Apps

Now available in the App Gallery ↗:

- AWS Security Posture Rule Set ↗

Notes and reminders

Stay tuned for more coming soon! 🚀

—

The Sola Team

August 10, 2025

Release notes

Here’s the latest on what’s new and improved at Sola.

✨ Sola AI

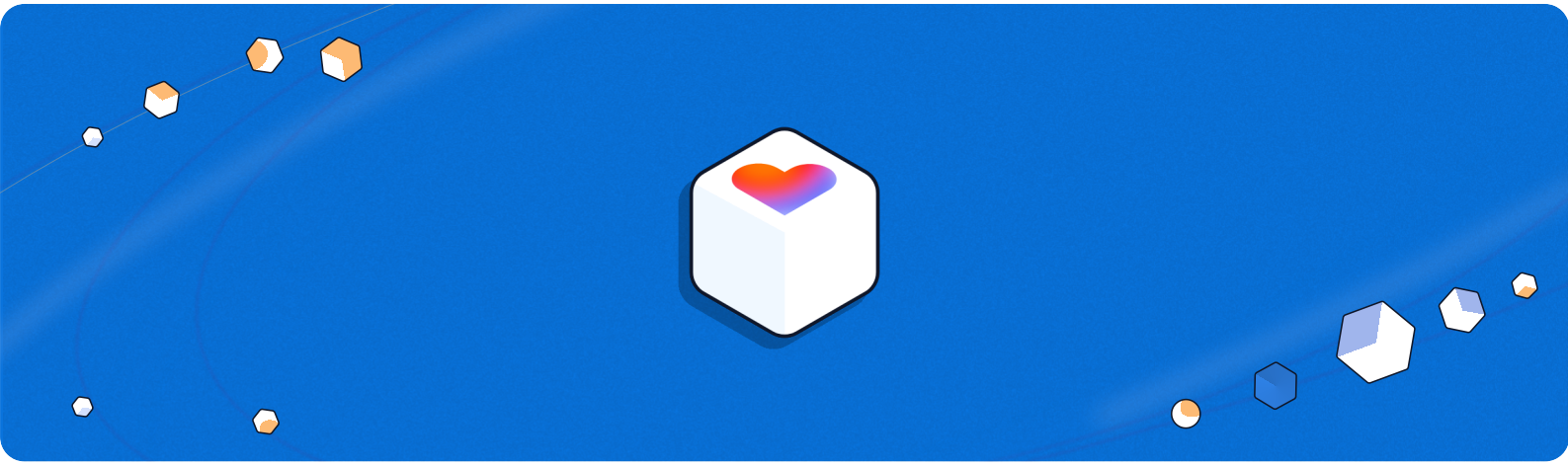
Build queries, alerts, and canvases, one prompt at a time

Sola Copilot now lets you build canvases, alerts, and queries directly within existing apps. Expand coverage, add new use cases, and generate full dashboards, all from a conversation with the copilot.

Create multiple canvases in a single request, each tailored to different teams or goals. This update makes it easier than ever to grow and evolve your apps with natural language.

Try it now ↗

Integrations



Data Sources

***New*: Lovable App Scanner**

Connect Lovable to monitor and assess the security posture of your Lovable applications, including vulnerabilities, misconfigurations, and hidden exposures that traditional tools may overlook.

New Apps

Now available in the App Gallery ↗:

- Lovable App Scanner - Security Posture ↗

Notes and reminders

Stay tuned for more coming soon! 🚀

—

The Sola Team

July 23, 2025

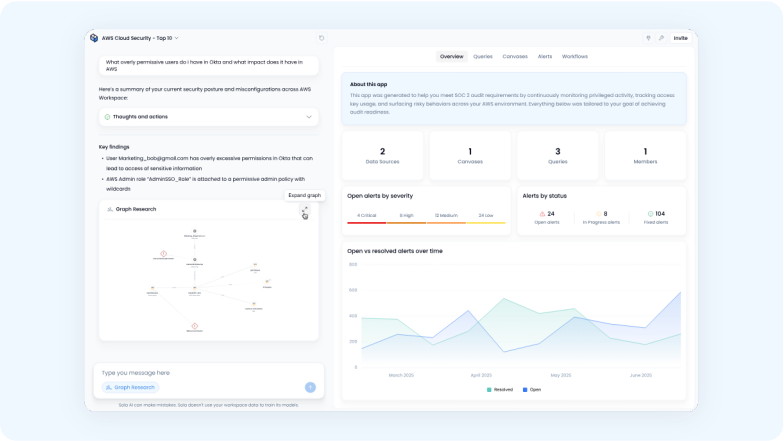
Release notes

Here’s the latest on what’s new and improved at Sola.

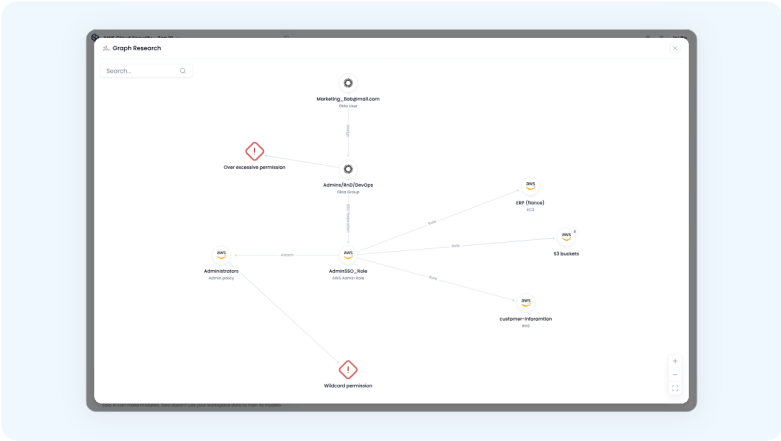
✨ Sola AI

Graph-enhanced research in Sola AI

Sola AI now includes graph-enhanced research, a deep analysis mode that uses **Sola’s proprietary security graph** to answer complex questions with rich context and clarity. It maps relationships between resources, controls, and risks to deliver **grounded**, **complete responses** backed by visual evidence and cross-environment reasoning.



Graph research mode in AI copilot



Graph research visual representation

[Try it now in your workspace home ↗]

Notes and reminders

Stay tuned for more coming soon! 🚀

—

The Sola Team

July 21, 2025

Release notes

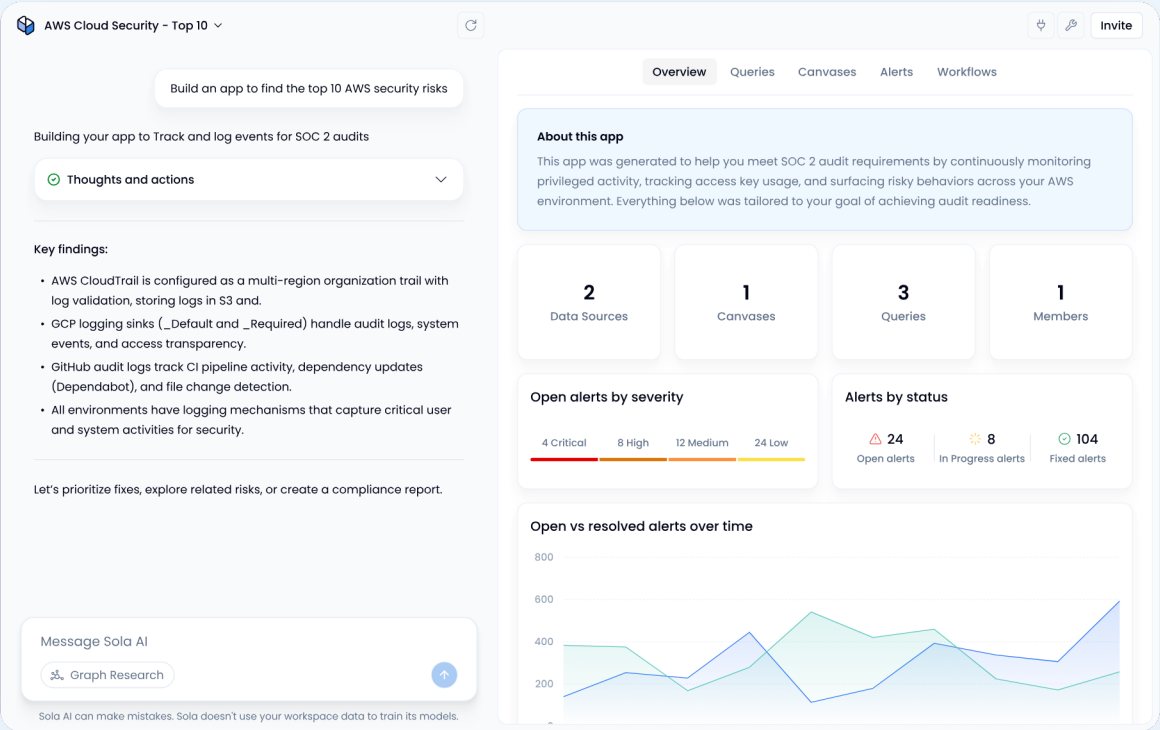
Here’s the latest on what’s new and improved at Sola.

✨ Sola AI

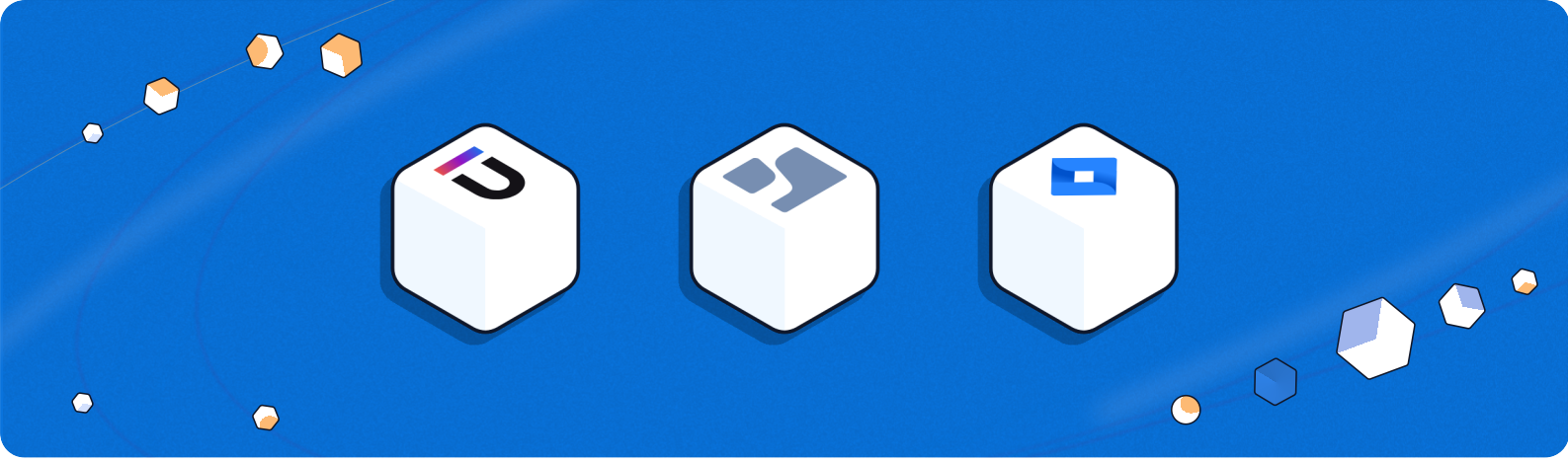
Your AI Security Copilot: AI-First Sola app layout

Sola AI is now integrated throughout your security apps.

The new design lets you ask questions, explore data, and investigate issues while viewing alerts, dashboards, and queries.



Integrations



Data Sources

New: Upwind

Integrate Upwind to surface cloud security data from Upwind, including threat policies, threat detections, and vulnerabilities.

New: Jamf Pro

Connect Jamf Pro for Apple device management on enrolled devices, configurations, user associations, and security posture across your Apple fleet.

Connectors

New: Jira

Bring Sola AI into your Jira projects to create and track issues directly from in-chat conversations and streamline remediation workflows.

Sola Studio

Export canvas as PDF

Download your canvas as a PDF to share insights or report on findings. The file includes all widgets and layout.

Export alert tables as CSV

Export triggered alerts and alert evidence tables with Sola apps directly to CSV files. Exported files reflect your customized view (filters, sorting, and selected columns).

New Apps

Now available in the App Gallery ↗:

- EntraID - Security and Access Insights ↗

Notes and reminders

Stay tuned for more coming soon! 🚀

June 30, 2025

Release notes

Here's the latest on what's new and improved at Sola

Connectors: Real-time actions from in-chat AI copilot

Sola now supports Connector integrations that let you interact with external services in real time, directly from Sola AI conversations.

Use the new Slack connector to share findings during analysis, escalate issues for remediation, and offload insights to the right stakeholders or channels across your organization.

✨ Sola AI

Ask AI copilot about triggered alerts

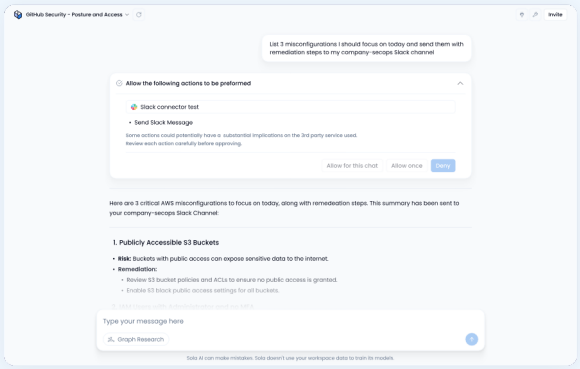
Sola AI can now help you review and investigate triggered alerts.

Get on-demand insights into triggered alerts to help you prioritize and take action.
Ask questions like ***"What alerts should I focus on today?"*** or ***"How can I remediate these issues?"*** to get a structured summary of relevant alerts, key findings, and recommended next steps directly from the Sola AI copilot.

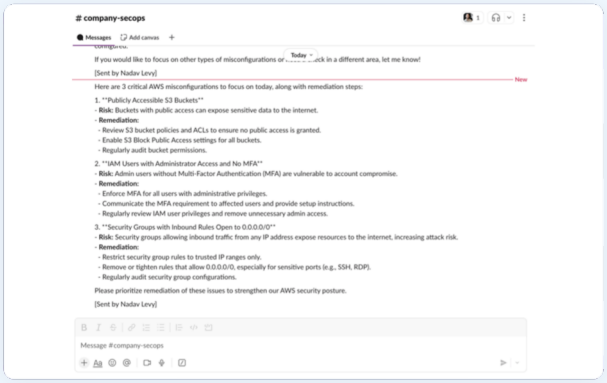
Ask AI copilot to send to Slack

Sola AI can now share findings, insights, or summaries directly to Slack.

Use prompts like ***"Send this to my SecOps channel"*** or ***"Notify the team in Slack"*** to streamline collaboration and keep stakeholders informed without leaving the conversation.



Send to Slack from AI copilot

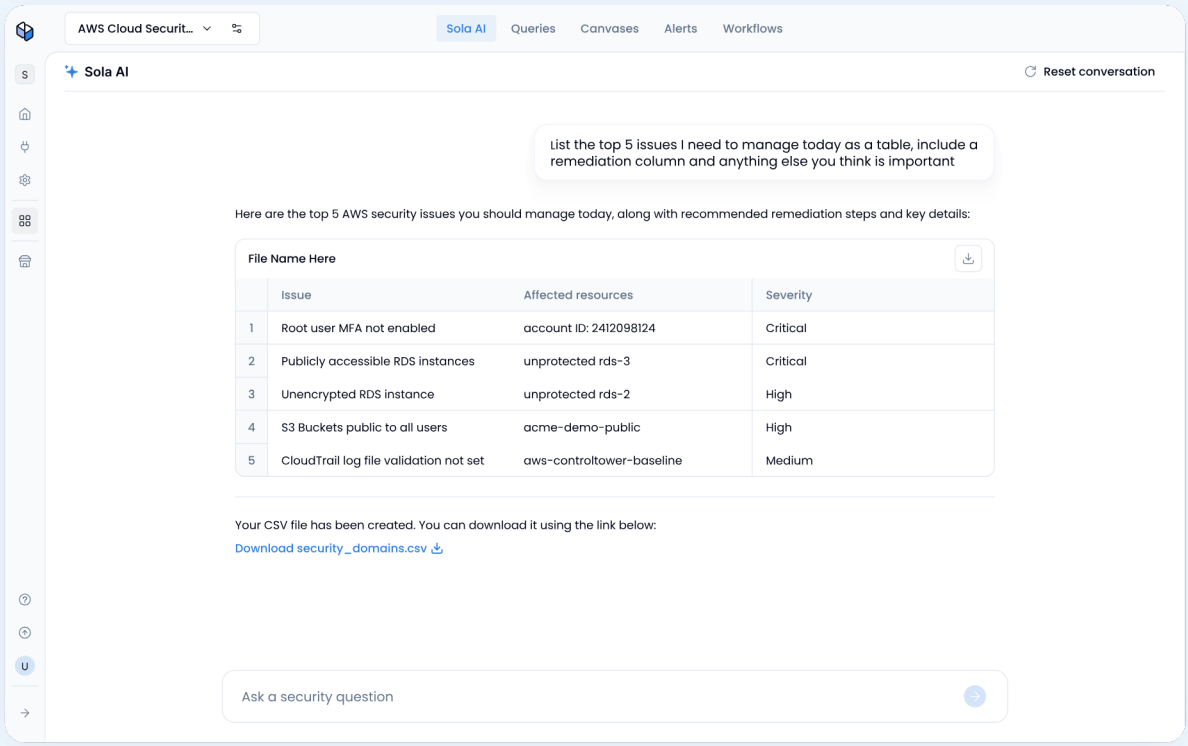


Slack Sola Agent

Export AI-generated tables as CSV

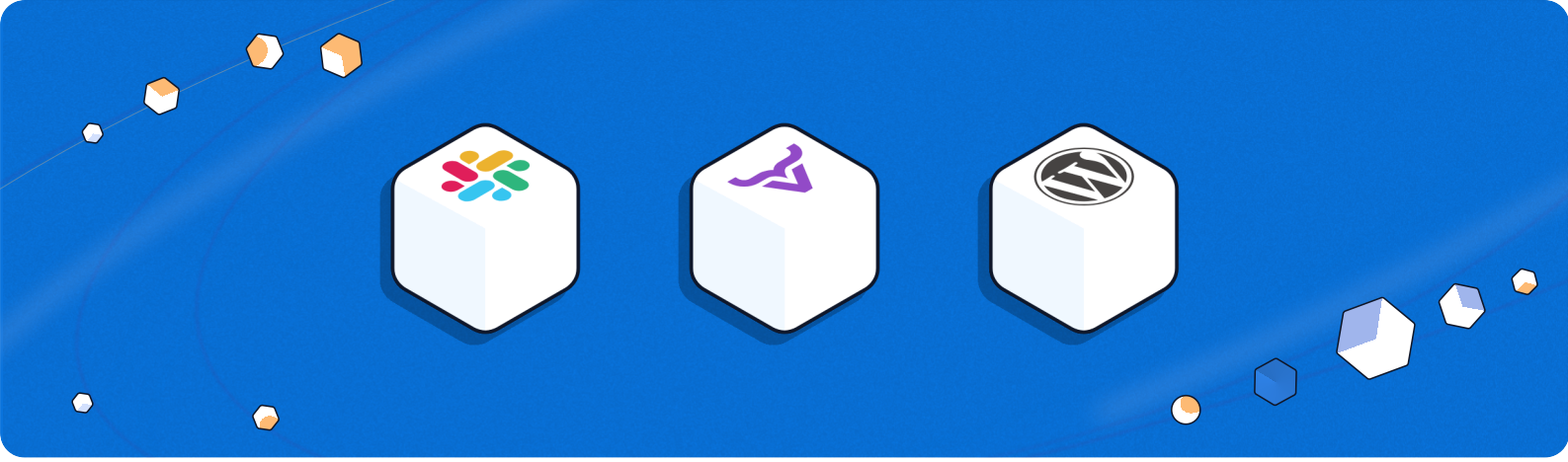
Sola AI can now export tables it generates during a conversation as CSV files.

Ask the copilot to export any result table, such as investigation findings, user lists, or issue breakdowns, for easier sharing, reporting, or deeper analysis in external tools.



Export CSV from AI copilot

Integrations



Data Sources

New: OX Security

Connect Ox Security to monitor code vulnerabilities, secrets exposure, container risks, SBOM insights, and more.

New: WordPress Scanner

Integrate WordPress to surface publicly exposed sites, and potential security risks across your web infrastructure.

Improved: Cloudflare

Now supports custom firewall rule sets and rules at both Account and Zone levels, providing deeper visibility into web application protection and access control configurations.

Improved: Google Workspace

Now includes Google Directory, enabling insights into organizational structure, user status, and access visibility.

Connectors

New: Slack

Send findings, summaries, alerts and more directly from Sola AI copilot to Slack.

Sola Studio

Export query results to CSV file

Export query results directly to CSV files. Exported files reflect your customized view (filters, sorting, and selected columns).

Filter canvas widgets

Apply filters to individual widgets in your canvas, in both edit and view mode, to focus on specific data slices. This lets you refine the scope and create multiple widgets from a single query, without duplicating or modifying the original query.

New Apps

Now available in the App Gallery ↗:

- CrowdStrike - Hosts and Alerts Insights ↗

Notes and reminders

Stay tuned for more coming soon! 🚀

—

The Sola Team

May 20, 2025

Release notes

Here’s the latest on what’s new and improved at Sola.

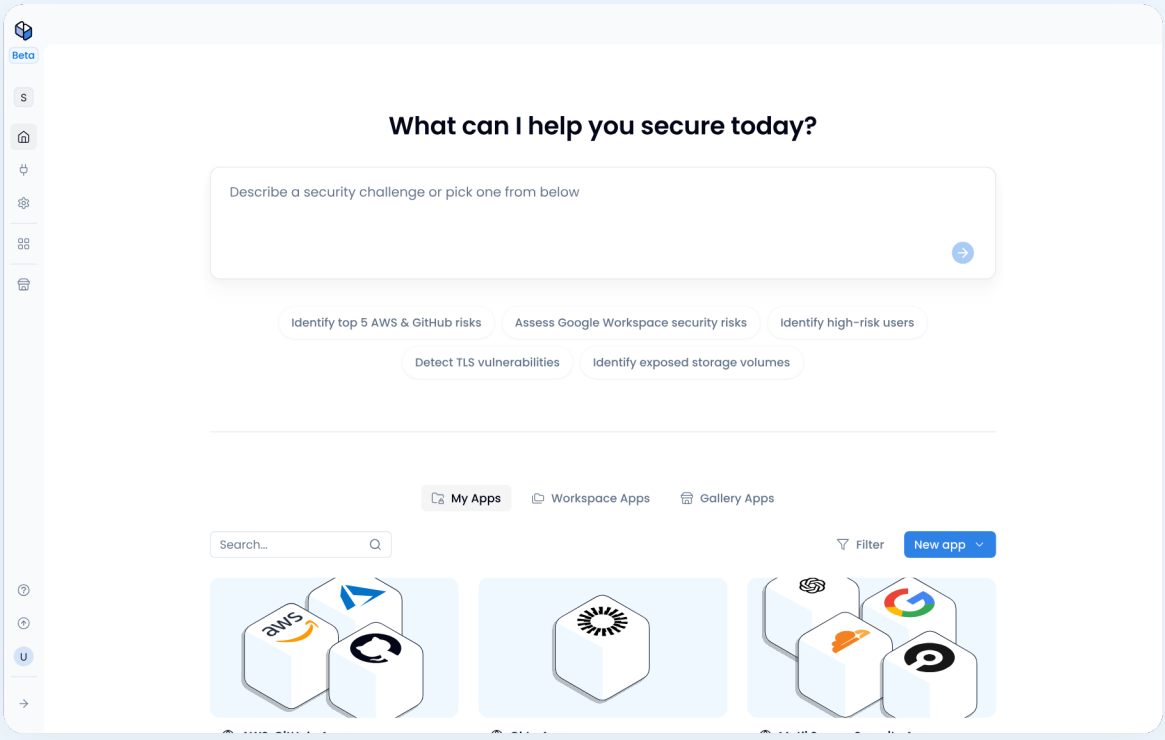
✨ Sola AI

From prompt to app, powered by Sola AI

Sola AI now builds complete security apps from a single prompt.

Whether you’re tackling a known issue or exploring new risks, Sola AI turns your prompt into a working security solution in minutes.

Just describe the security use case you want to investigate, and Sola AI will generate a full app, complete with tailored dashboards, alerts, and key insights from your connected data.



Build an app for your security needs

[Try it now in your workspace home ↗]

Notes and reminders

Stay tuned for more coming soon! 🚀

—

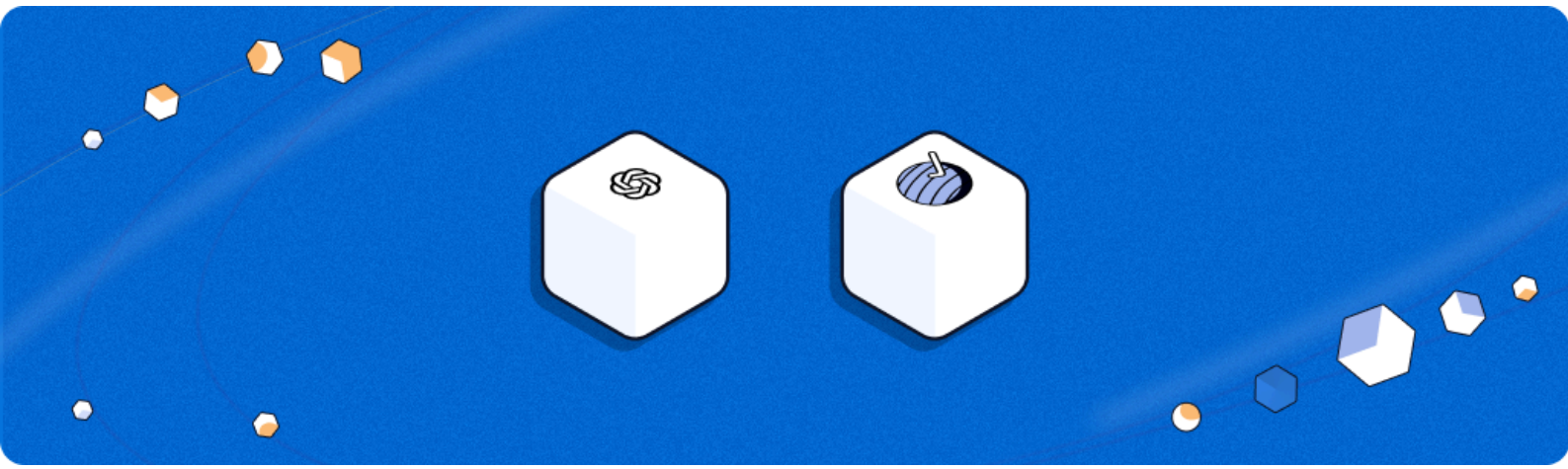
The Sola Team

May 14, 2025

Release notes

Here's the latest on what's new and improved at Sola.

Integrations



New: Open AI Platform

Connect your OpenAI account to monitor users, API keys, projects, audit activity, and more, to uncover potential risks across your OpenAI environment.

New: Sola Web Checker

Add domains, URLs, or host endpoints to uncover hidden risks, and continuously monitor the security posture of your public assets.

New Apps

Now available in the App Gallery:

- Google Workspace ↗
- Sola Web Checker ↗

Sola Studio

Alert email notification

Add members or valid email addresses to receive email notifications when a new alert is triggered.

Canvas widget overview

Expand widgets in your app canvases to easily view a detailed overview of the query and data results.

Filter queries in alert creation

Apply an additional filter layer on top of a selected query when creating alert rules. This lets you refine the scope and create multiple alert rules from a single query, without duplicating efforts.

Filter query view

Apply table filters when viewing query results to refine the data.

Notes and reminders

Stay tuned for more coming soon! 🚀

—

The Sola Team

April 20, 2025

Release notes

Here’s the latest on what’s new and improved at Sola.

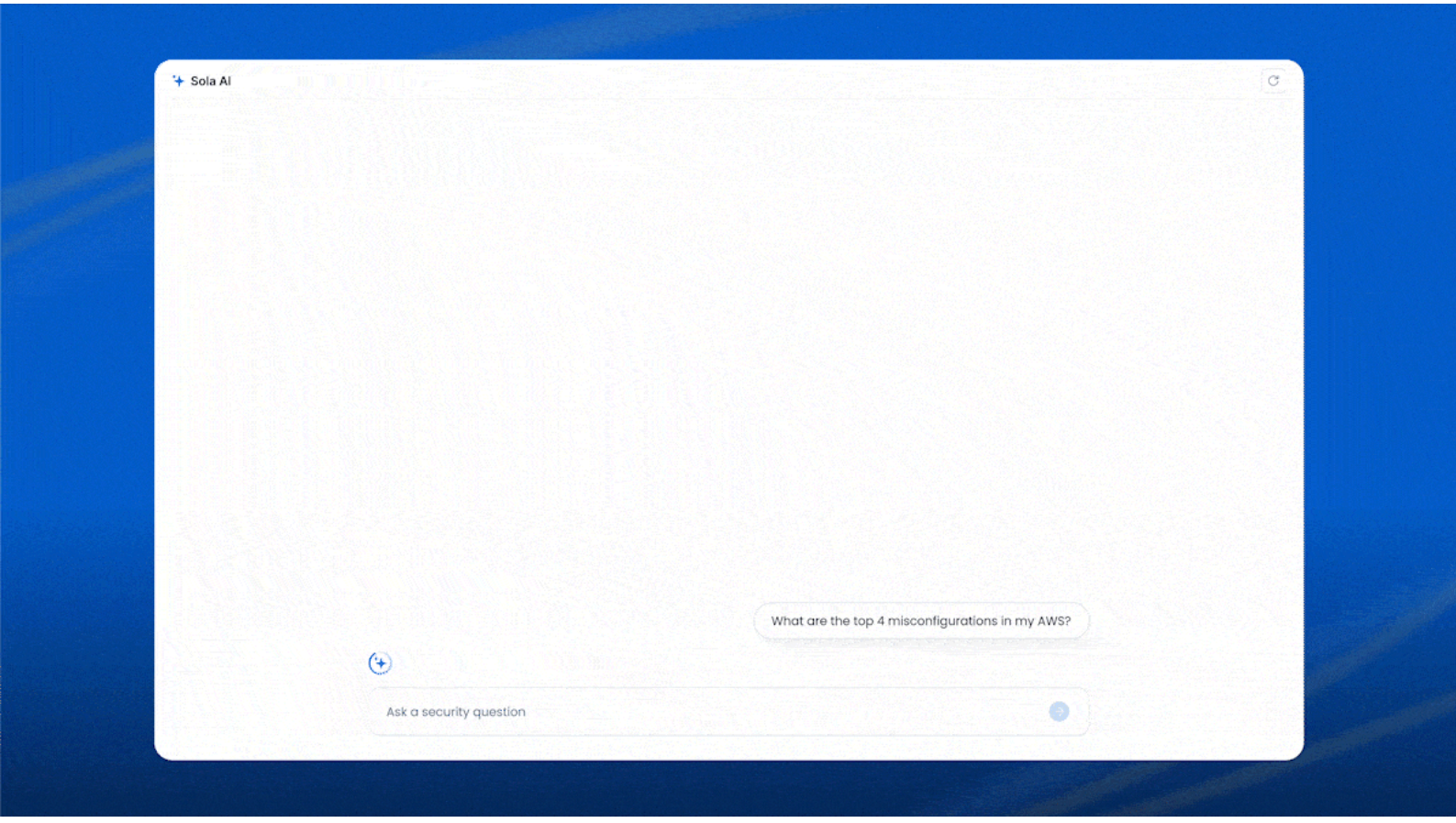
✨ Sola AI

New Sola AI insights agent

Get deep visibility into your security posture with a new AI insights agent.

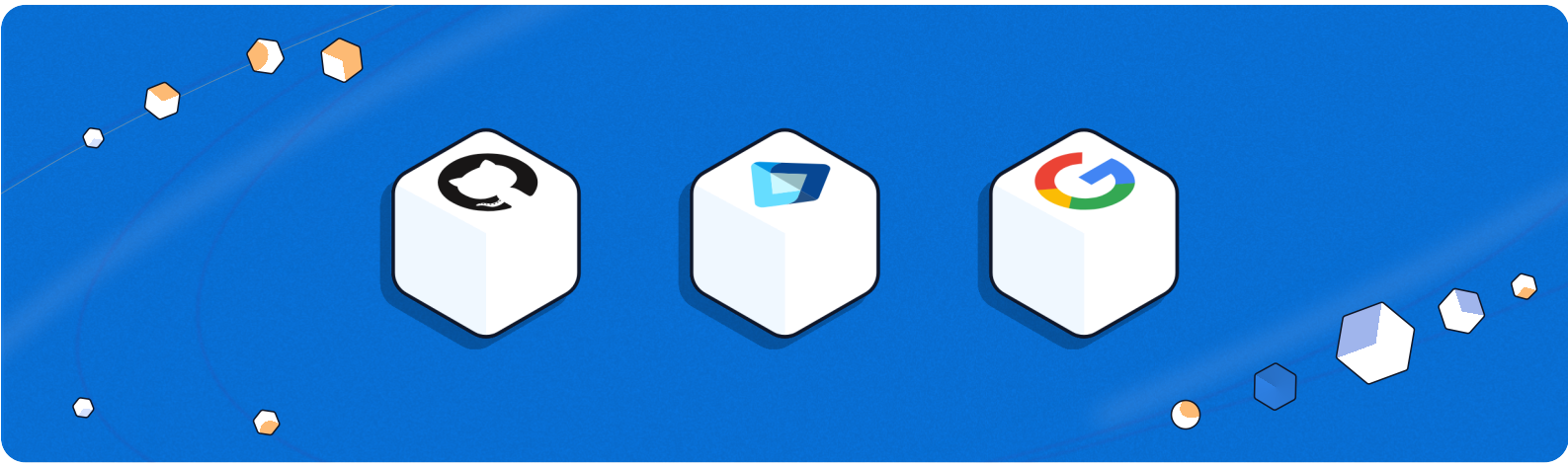
Apps now include a dedicated Sola AI tab to help you investigate your environment and uncover security risks by asking security questions. Ask specific or broad questions like “What’s my AWS security posture?” or “What are the top security issues with my GitHub repositories?”, and Sola AI will return targeted queries, generate insights, and surface what matters most.

Whether you’re exploring new risks or validating your controls, this AI-powered agent helps you dig deeper, faster.



New Sola AI insights agent

Integrations



New: Microsoft Entra ID (formerly Azure AD)

Integrate your Microsoft Entra ID environment to monitor identity and access management across your organization.

New: Google Workspace

Connect your Google Workspace accounts to gain insights and build apps around Workspace users, Gmail settings, and files in Google Drive.

Improved: GitHub Cloud - Sola GitHub App

The Sola GitHub App is now available as a fast and secure way to connect your GitHub Cloud account with your Sola workspace.

This predefined integration simplifies setup, making it easier to get started and begin analyzing your GitHub environment.

Security and Privacy

SOC 2 Type II compliance

Sola is now SOC 2 compliant, meeting the highest standards for security, availability, and confidentiality. We are committed to protecting your data with industry-leading practices and trusted security controls.

Learn more about our other key industry certifications, such as ISO 27001, and our latest security and compliance documentation, in the Trust Center ↗.

Notes and reminders

Stay tuned for more coming soon! 🚀

—

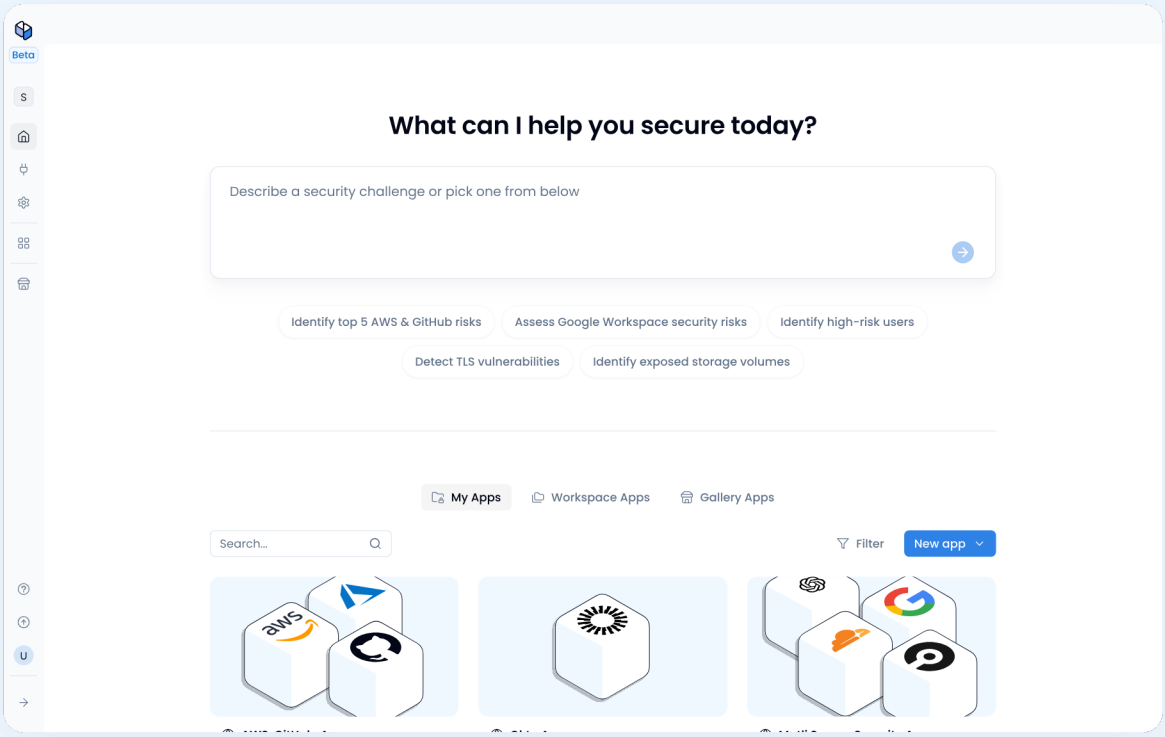
The Sola Team

Workspace

Workspace Home

Create your own security solutions

A Sola workspace is a collaborative studio environment that lets you create and share custom security apps. It is a virtual space for all apps you are a member in and can join, within an organization. You can be a member of multiple workspaces.



Sola workspace home

Your workspace is a central place where you can ideate and map out **your security gaps and use cases**, and create custom solutions to address them. Each custom solution can cover a specific use case.

Key components you'll need:

1. **Data sources** - Secure connections to the data of services used within your organization.
2. **Apps** - Customizable tools designed to address specific cyber security use cases or needs.

Pro tip: Start by connecting your data sources.
This will allow you to start getting answers to your security questions and create apps quickly.

Apps

Create custom security apps, your way

A Sola app is a custom security tool that you create, tailored for your specific security needs and area of interest. Each app you create is autonomous and supports its own use case. It can be limited to one or more data sources with different workspace members as creators and consumers.

The app you create can range from basic and simple use cases, to specific or complex scenarios. Apps can be shared with your team members, depending on their member roles. Public apps are open to all workspace members with the selected default role. Private apps require an invite.

Apps are connected to relevant data sources that allow you to query your data and gain security insights into your organization.

Each app is made up of 5 building blocks:

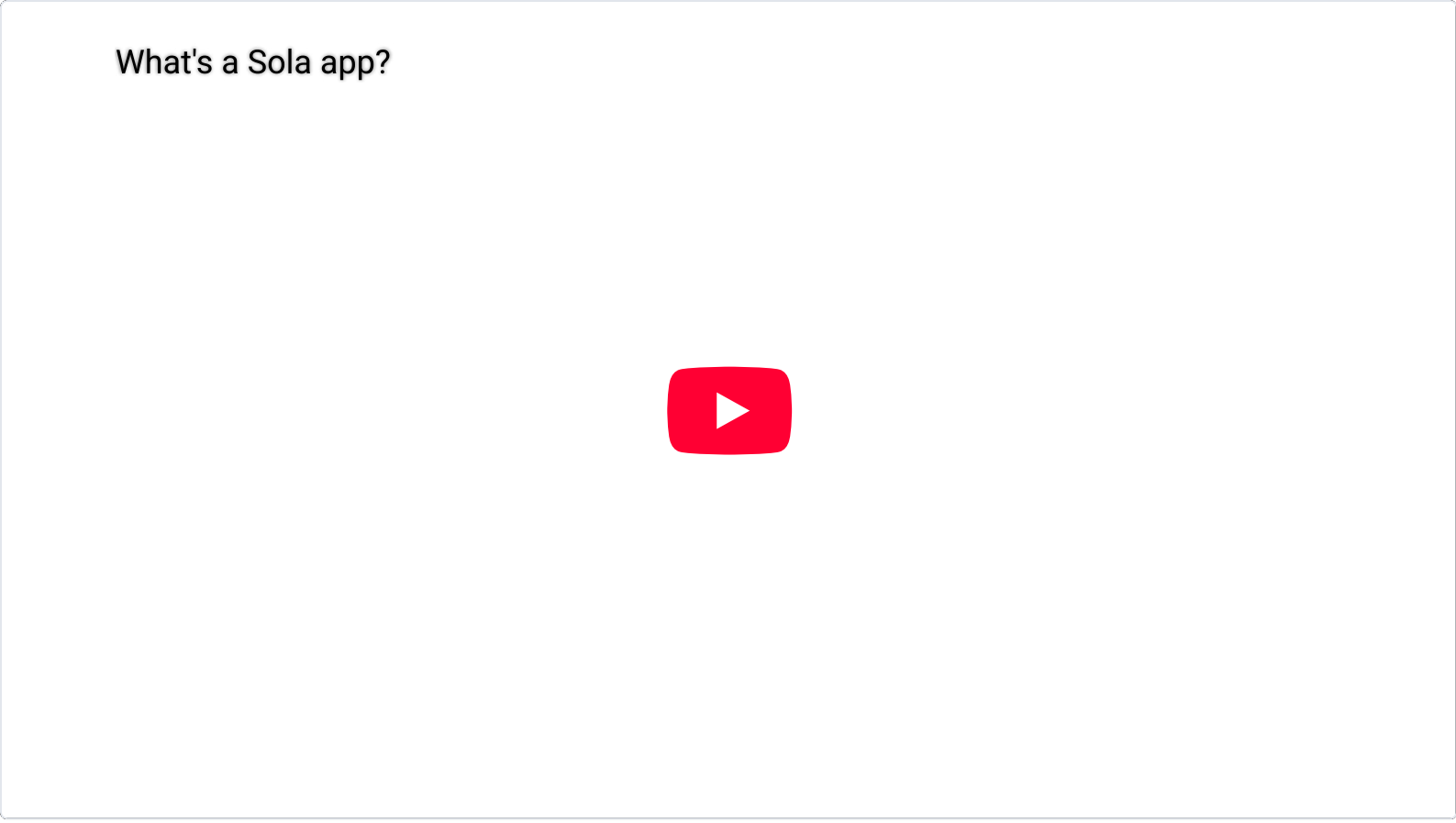
1. **Sola AI Copilot** - Ask questions and get insights about your security.
2. **Queries** - Expose the underlying data from your sources.
3. **Canvases** - Vibe-code your data into fully interactive interfaces.
4. **Alerts** - Turn key questions into rules that monitor your data.
5. **Workflows** - Structure and automate actions with AI-native flows.

Pro tip: Create security apps your way

Sola gives you the flexibility to structure your apps based on your security priorities.

For example, you can create apps by security use case (e.g., Identity and Access Management), by data source (e.g., AWS Security Posture, GitHub Security Posture), or a combination of both (e.g., AWS Identity and Access Management, Salesforce Identity and Access Management).

*How you create your apps is entirely up to you. C*hoose what makes the most sense for your security needs.

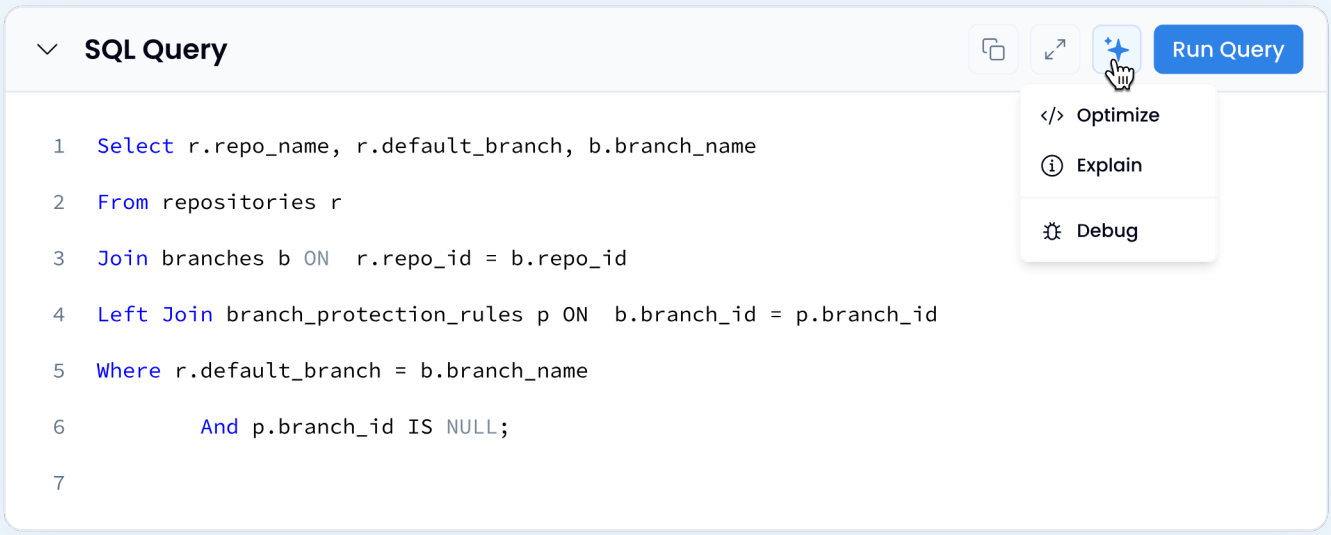


What's a Sola app?

Creating apps

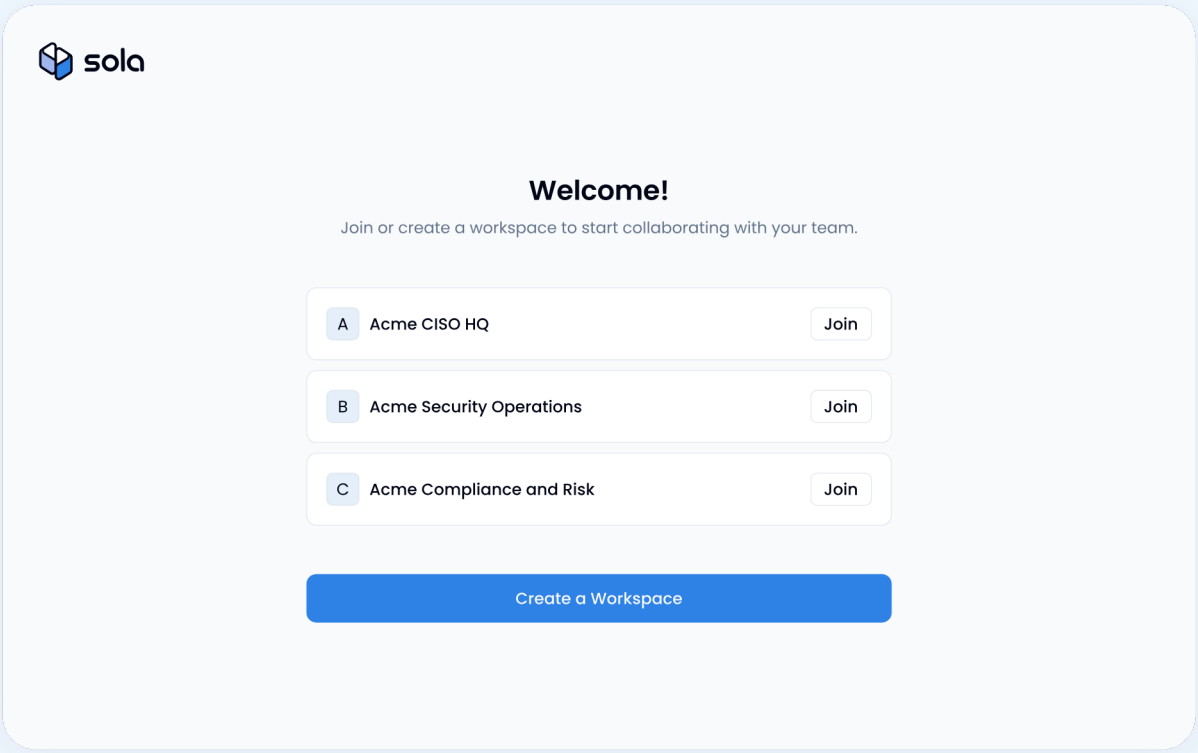
Your apps can be as simple or as complex as you need. Depending on how technical you want to get, the queries component of your app provides the flexibility to query your data using natural language with Sola AI and SQL queries.

✨ Sola AI helps you quickly generate queries and refine them, making it easier to explore your data and uncover insights.

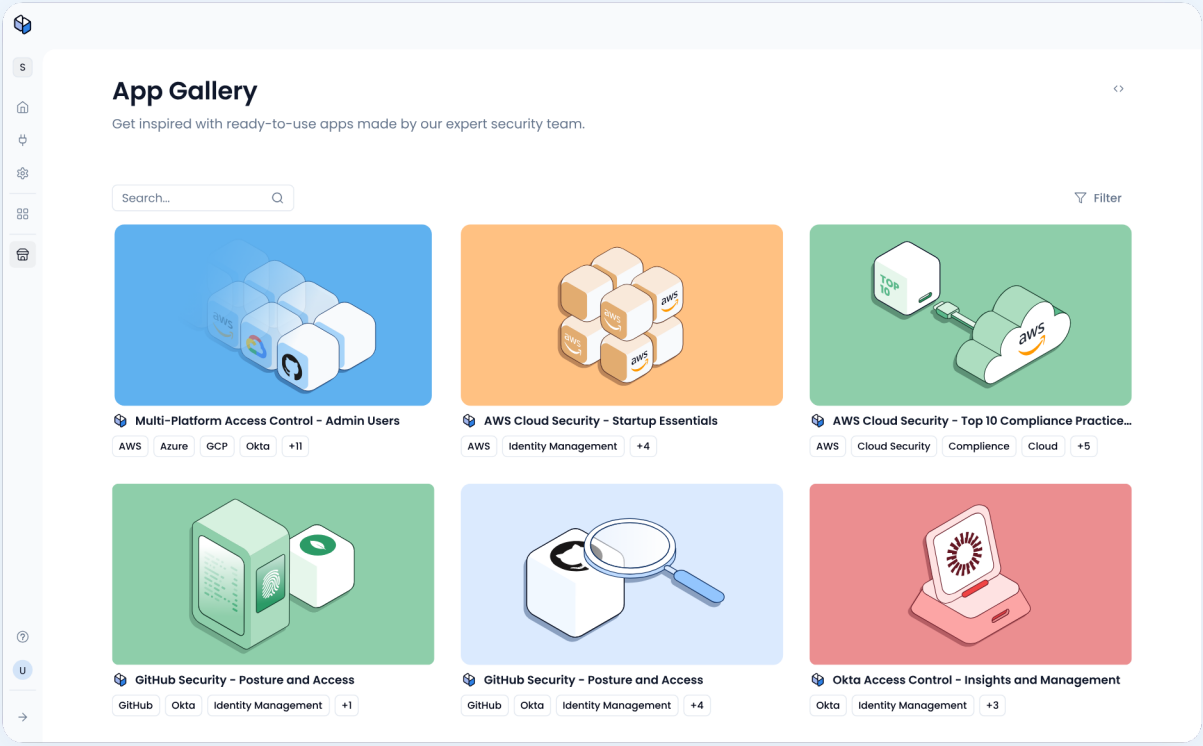


Using Sola AI to query data and fine-tuning the generated SQL query

Create a new app from scratch, join an existing one in your workspace, or use a prebuilt app from the app gallery made by our expert security team.



Joining a workspace



Creating a new app from the app gallery

Who can create and install apps?

Only **workspace owners** and **admins** can create apps, join existing apps, or install apps from the app gallery.

Connecting data sources

To create a new app, you'll need to connect it to one or more data sources.

Connecting your data source is important because it allows you to get answers to your questions that are relevant to your data. By linking your data sources, you can easily find security insights and answers based on your organizational data.

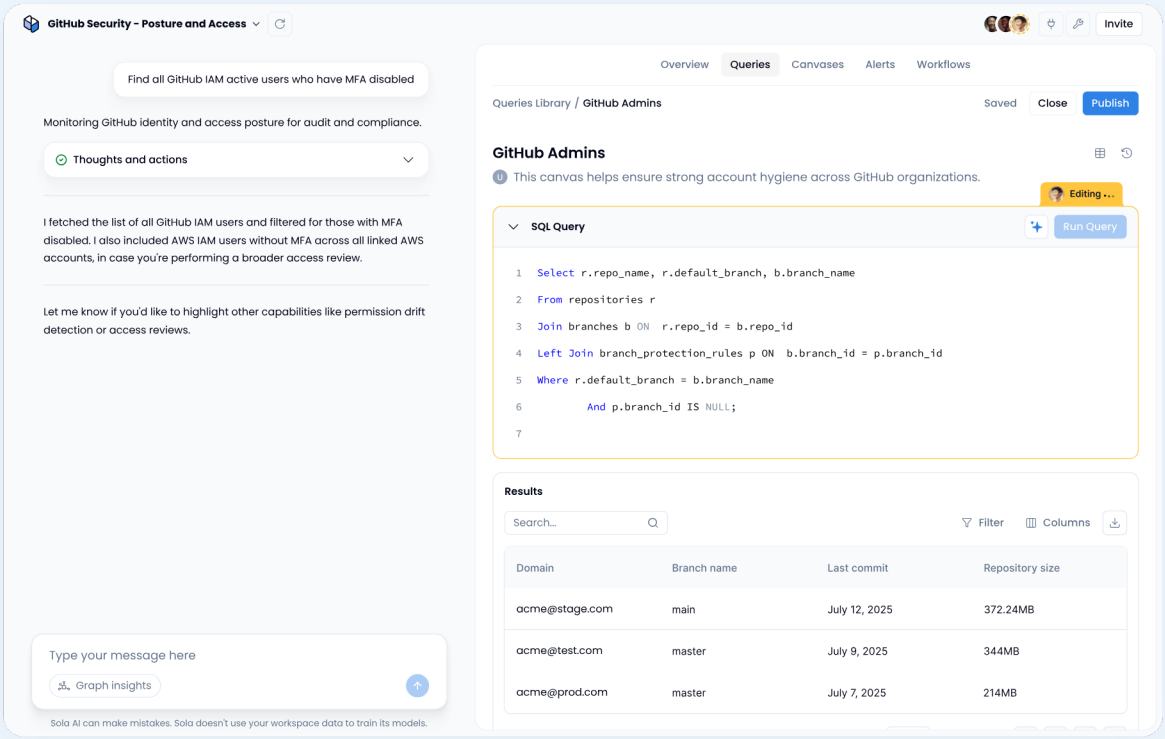
You can skip this step for now and use a placeholder data source, which includes only the table schema (without data). Connect your data source later when you're ready.

Viewing and collaborating on apps

Sola provides two ways to access apps in your workspace:

- **My Apps** - Apps that you are a member in, whether created by you or someone else
- **Workspace Apps** - Apps in your workspace that you can join.

Collaborate in real time to share insights, refine security findings, and build on each other's work. See who else is active in the same app or building block as you create.



Collaborate in real time

FAQs

Who can create or install apps in Sola?

Only workspace owners and admins can create apps, join existing apps, or install apps from the app gallery. If you don’t have the necessary permissions, reach out to your workspace admin.

How does Sola AI assistant use my data?

Sola AI assistant follows strict security practices to keep your data safe. Your data is stored securely according to our standard security policies ↗.

Sola AI assistant does not use your data to train our models. Any data processed through Sola AI is used solely to generate responses and is not retained for training purposes.

Can I enable or disable the Sola AI Assistant?

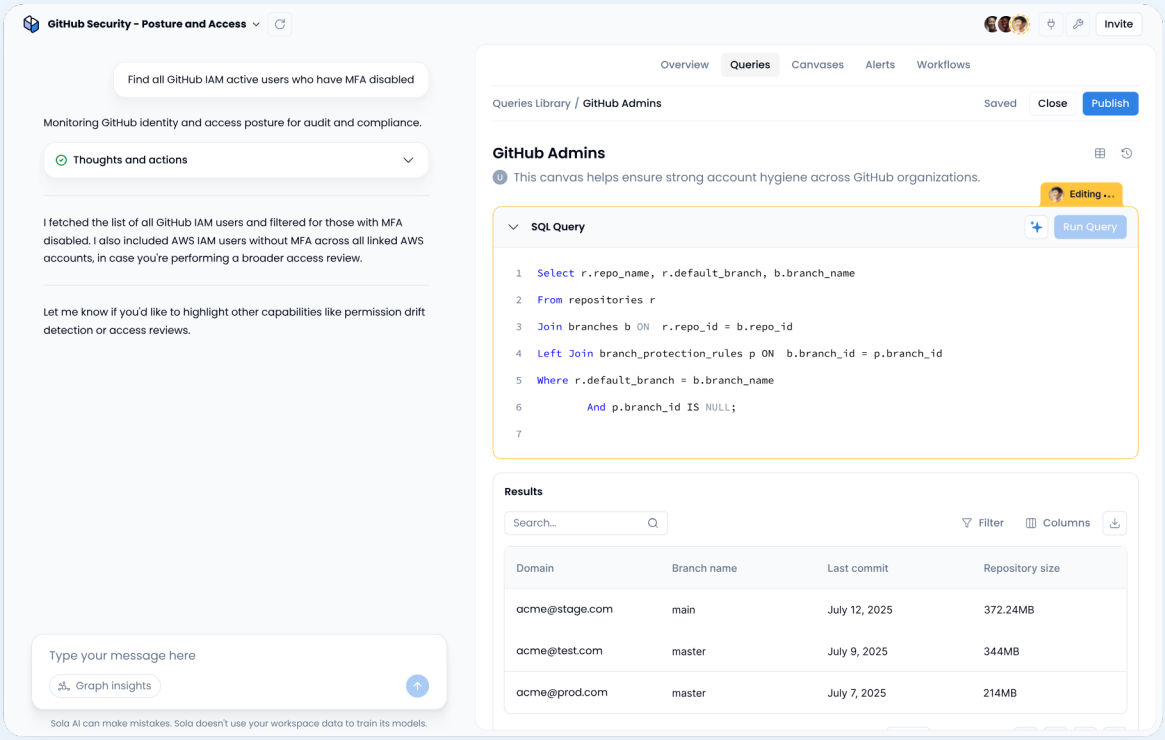
Yes. You can enable or disable the option to skip the Sola AI assistant when creating new queries.

Queries

Query your security data for insights

Queries help you analyze security risks by retrieving relevant data from your connected sources. Querying your data allows you to explore your security posture across different environments, detect potential threats, and uncover critical security insights.

Queries are one of the building blocks that make up an app, alongside canvases, alerts, and workflows.



Query real-time collaboration

Creating queries

There are two ways to create queries:

- **Use Sola AI** to ask security-related questions in natural language and generate queries automatically.
- **Write your queries** from scratch using the SQL query editor.

> **Pro tip: Enhance your SQL queries with ✨ Sola AI**
>
> Sola AI can help you identify the right tables and columns that contain the data you need or refine SQL syntax for more accurate results.

Once created, queries can be **saved**, **published**, and **modified** to refine your insights over time.

Publishing queries

A query extracts a specific dataset from your connected data sources. Publishing a query saves the retrieved dataset as a table in your app. This makes the data set available across your app for:

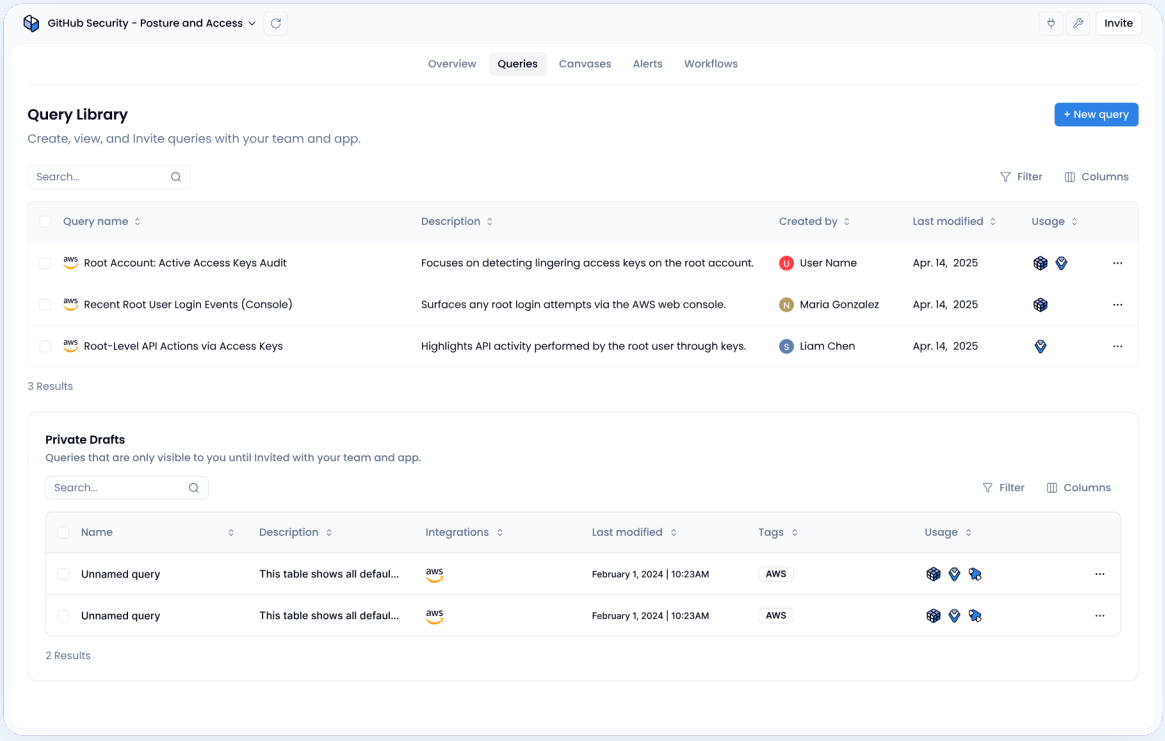
- Canvases - Turn query results into charts, graphs, and tables.
- Alerts - Set up alerts based on query results.
- Workflows (*coming soon*) - Automate security actions.

Managing queries

The **Query Library** is where you can access all queries in your app.

Queries can be:

- **Published** - Available for use across the app's building blocks—canvases, alerts, and workflows—and accessible to all app members.
- **Private drafts** - Visible only to you until shared.



Public and private queries in query library

Queries have two modes:

- **View mode** - Displays the last published version of the query.
- **Edit mode** - A real-time shared draft, where multiple users can collaborate, edit together, and see changes live before publishing.

> Edits are only applied and visible to all app members once published. When you publish, all changes you and others have made are published together.

In the query library, depending on your role permission, you can:

- **View** all available queries in your app.
- **Create** and **modify** queries.
- **Duplicate** a query to modify it without changing the original.
- **Delete** a query.
  Note: This action cannot be undone. Assets using the query, such as canvases or alert rules, will break or stop working.

> To manage your **app role permissions**, go to *Workspace Settings* > *App Permissions*.

Pro tip: Refine your SQL queries with Sola AI

✨ Access Sola AI from the query sidebar, or use the AI icon next to Run Query for quick actions:

- **Optimize** - Improve query efficiency.
- **Explain** - Understand what the query does.
- **Debug** - Identify syntax issues and get suggested fixes.

Canvases

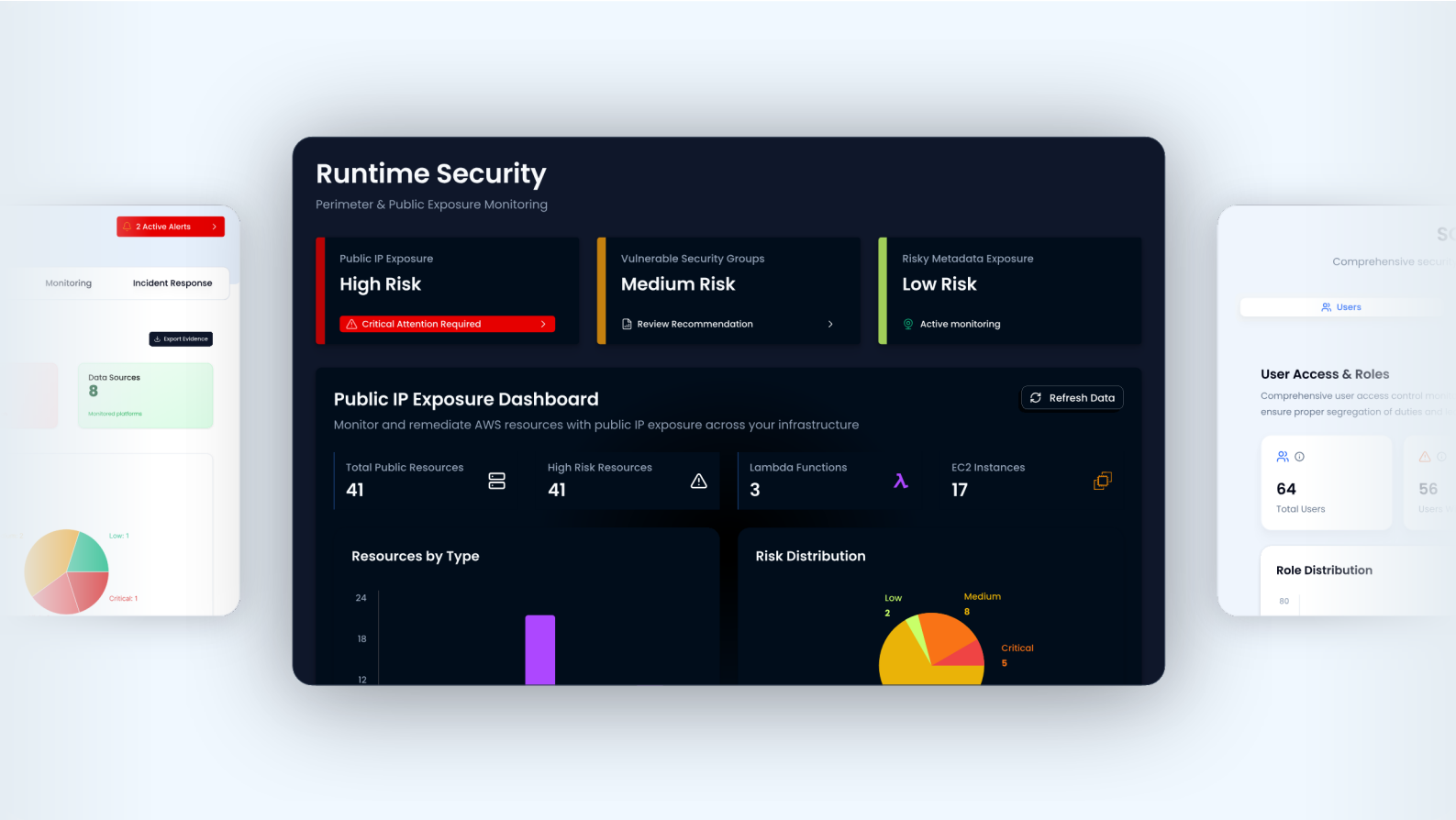
Vibe-code your data into fully interactive interfaces

Canvases are an **AI-powered** way to transform your security data into **fully customizable interactive interfaces**. Think of it as a vibe-coding app builder, driven by Sola's unique capabilities to ingest, understand, and query your security data.

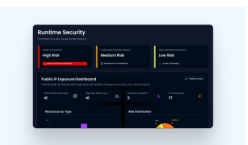
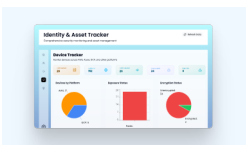
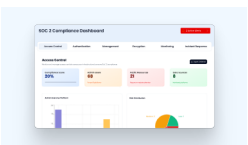
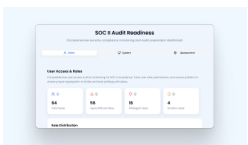
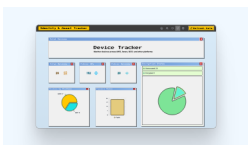
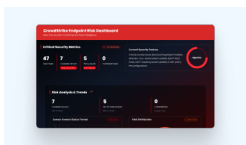
Use natural language prompts to create any interactive dashboard or report with dynamic charts, tables, filters, and other interactive visuals, from your query results and connected data.

Get the exact results you want with unlimited flexibility in layout, customization, colors, fonts, and styles.

Canvases are one of the building blocks that make up an app, alongside queries, alerts, and workflows.



Vibe-code your security data into fully interactive dashboards

Creating canvases

To create a canvas, click *New canvas* from the *Canvases* tab and describe the dashboard or insights you want in a prompt. Sola AI will generate your canvas.

Once the canvas is created, it is automatically published and available to all app members.

> See the Prompt Guide for tips and examples to refine your prompts and get the best results.

Managing canvases

The **Canvas Library** is where you can access all canvases in your app.

Canvases are live, interactive interfaces that update as you change them. Edits by collaborators are applied in real time and visible to all app members.

Canvases are tied to your connected data, they continuously update to reflect the latest query results and configurations, ensuring insights stay current without manual refresh.

Examples and use cases

Canvases are flexible and support a wide range of security use cases, such as monitoring, tracking, and guiding.

Monitor

Track security posture, exposures, and compliance checks in one place.

For example,

- Cloud Security Posture (CSPM) dashboard.
- Attack Surface Management (ASM) exposure tracking.
- Vulnerability management reports by severity/repo.

Explore

Drill into assets, vulnerabilities, and risks to follow changes over time.

For example,

- Asset inventory boards (with filters and drill-down).
- Threat intel trackers with prioritized IOCs.
- Patch tracking dashboards.
- Access review boards (Okta/Azure AD risky accounts).

Report

Provide high-level summaries and compliance views for leadership and audits.

For example:

- Executive reports highlighting key risks, posture trends, and KPIs.
- Compliance summaries for SOC2/ISO readiness and audit preparation.
- Risk heatmaps and scoring across business units or domains.
- Posture overview dashboards tailored for board or CISO reporting.

Guide

Provide structured security knowledge and step-by-step instructions for teams.

For example,

- Developer onboarding security guides.
- SOC runbooks with step-by-step instructions.
- Secure coding quizzes/games.
- Attack simulation walkthroughs.

Each canvas is generated with Sola AI prompts.

See the Prompt Guide for tips and examples of how to phrase your requests for different use cases.

FAQs

What kinds of visualizations can I add to a canvas?

Canvases support a wide range of visuals to fit different use cases. You can add dynamic charts (bar, line, pie, stacked), interactive tables, scorecards, and counters for KPIs. Beyond data, canvases also allow you to embed text blocks, images, and layouts—making it possible to build narrative-driven dashboards, security guides, or even fully branded executive reports.

Can I create canvases that combine data from multiple sources?

Yes. Canvases can unify insights from multiple sources in a single view. For example, you can correlate AWS cloud configurations, GitHub repository settings, and Okta identity data side by side to reveal risks, toxic combinations, or compliance gaps across your environment.

Can I share canvases?

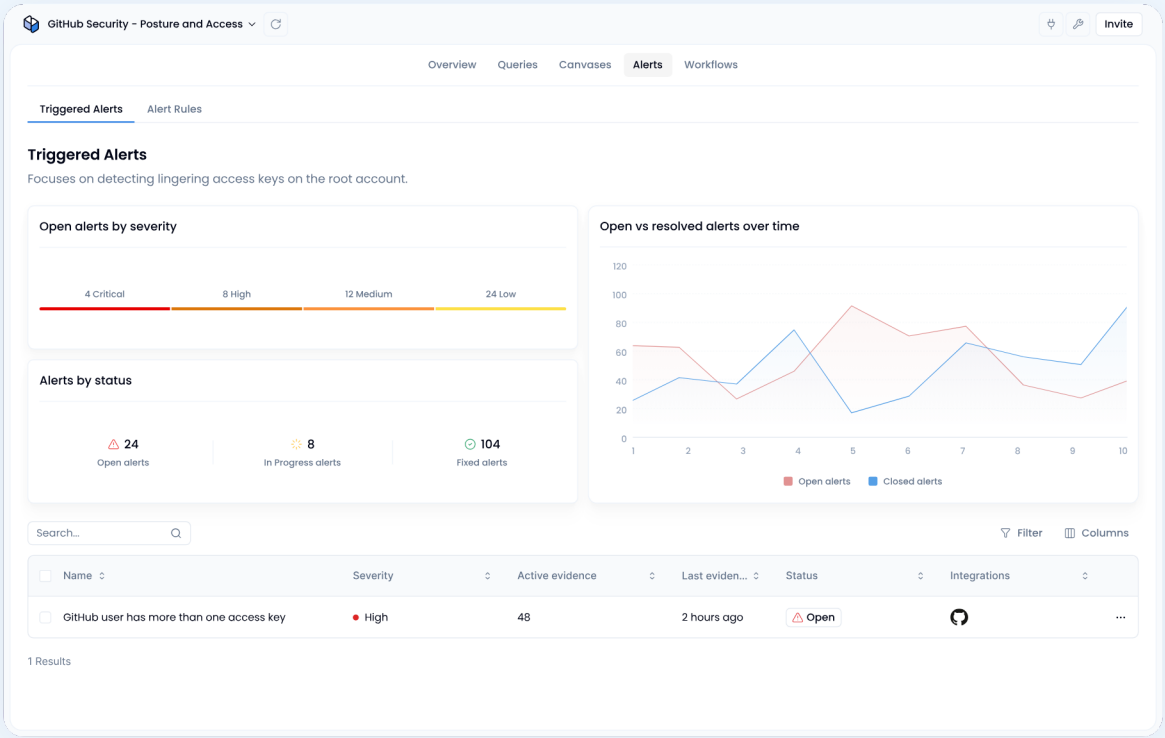
Currently, canvases are only visible within your app. No external sharing yet.

Alerts

Stay informed about security risks and policy violations

Alerts help you track security risks, misconfigurations, and policy violations by notifying you when query records meet specific conditions. They allow you to proactively monitor security events and respond quickly when risks arise.

Alerts are one of the building blocks that make up an app, alongside queries, canvases, and workflows.



Reviewing triggered alerts

Creating alert rules

Alerts allow you to track security risks by monitoring query records and triggering notifications when conditions are met.

To create an alert rule, from the *Alerts* tab of your app, go to *Alert Rules* > click *New rule*.

Define the following in the Sola wizard:

- **Rule query** - Select the query you want to monitor. Use an existing published query.
- **Query record fingerprint** - Specify which columns uniquely identify your records for deduplication. By default, all columns are included.
- **Grouping** - Configure how query records are grouped into alerts with findings.
- **Alert scope** - Choose whether to apply the rule to all existing query records or only new ones, after the rule is enabled.
  Note: Simulation will run on existing records.
- **Alert name** - Use the rule name or a custom alert name. Insert dynamic placeholders for dynamic alert names.
  Note: Use $ to add a dynamic placeholder (e.g., ${id}, ${created_at})
- **Alert description** - Add a description that will appear with the triggered alert. Insert dynamic placeholders for dynamic alert descriptions.
  Note: Use $ to add a dynamic placeholder (e.g., ${id}, ${created_at})
- **Steps to remediate** - Add guidance on how to fix or address this issue.
- **Alert severity** - Select the alert severity level.
- **Activate rule** - Enable to start enforcing this rule on the selected query.
- **Alert email notifications** - Add members or valid email addresses to get email notifications when this alert is triggered.

Email notifications are sent for:

- New alerts (excluding those triggered during the initial alert rule setup)
- Newly discovered evidence in existing alerts

Available dynamic placeholders depend on the Grouping setting

- If no grouping is applied, all query columns can be used as dynamic placeholders.
- If grouping is based on specific columns, only those columns will be available as dynamic placeholders.

This applies to both Alert Name and Alert Description.

Once configured, alerts will automatically track matching query records and display them in the triggered alerts view.

Managing alert rules

Alerts are managed in two views:

Triggered alerts

The *Triggered Alerts* view is where you can:

- **View** all triggered alerts and their severity.
- **Investigate** findings and update the alert status as you resolve them.
- **Assign** alerts to team members for resolution.

Alert rules

The *Alert Rules* view is where you can:

- **Create and edit** alert rules to track security findings.
- **Enable or disable** rules as needed.
- **Delete** rules that are no longer relevant.

> **Your permissions depend on your app role**
>
> App permissions, such as create and edit, are based on your app role.
> To see available permission levels and check your role, go to Settings > Workspace Settings.

> **Editing an alert rule**: Once an alert rule is created, you can only edit the name, description, severity, and remediation steps. The core logic (e.g., query, fingerprint, or grouping) cannot be modified.
> To change the logic, create a new rule.

Alert lifecycle evidence

When an alert is triggered, it includes supporting evidence that helps you understand why the alert was triggered. Evidence is categorized into three states, which impact the alert lifecycle:

1. **Active evidence** - Evidence found in the last alert calculation.
2. **Excluded evidence** - Evidence found that was manually excluded from the active evidence list. Excluded evidence can be re-activated if needed.
3. **Old evidence** - Evidence that existed in a previous calculation but is no longer detected.

To review evidence for a triggered alert, click on an alert from the triggered alerts view.

Managing evidence enables you to control when an alert remains active, is resolved or suppressed.

Reviewing alerts

After an alert is triggered, you can review its details, investigate findings, and take action.

Opening an alert shows the matching query records and why it was triggered.

You can assign alerts to team members and update their status as you work through them.

Alert statuses

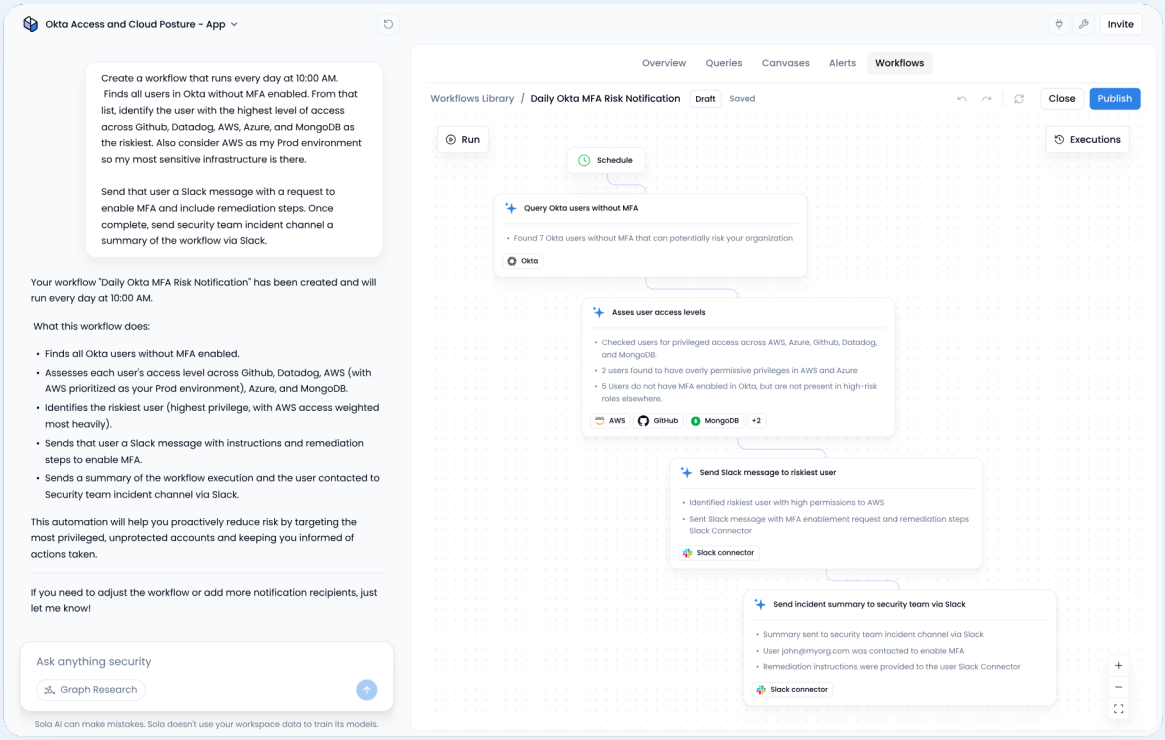
Status	Description
Open	A new alert has been triggered and requires investigation.
In Progress	The alert is being reviewed or worked on.
Suppressed	The alert is acknowledged but does not require action.
Resolved	The issue has been addressed and no longer needs attention.
Auto-Resolved	The issue has been automatically resolved by the system, since there is no active evidence.
Deprecated	The alert has been deprecated, since the query used in the alert rule, representing the rule logic, has changed.

Workflows

Structure and automate your security operations with AI-native flows

Agentic Workflows bring intelligent Directed Acyclic Graph (DAG) structure and automation to your security apps. Use workflows to structure multi-step actions, orchestrate investigations, and automate across data sources and connectors.

Workflows are one of the building blocks that make up an app, alongside queries, canvases, and alerts.



AI-powered workflows

Workflows combine **AI-native reasoning** with **structured execution** to overcome single prompts and old school automation limitations, bringing flexibility, transparency, and real-world resilience **to your security operations**.

Learn more in the Sola blog ↗

Workflow components

Workflows are made up of key components that define how they start, run, and deliver results.

Single-step AI block

In Sola Workflows, each **AI block (step)** is like an AI agent. It takes input from the previous block, uses the necessary data sources and tools, and performs the task defined in the prompt.

Trigger	Defines when a workflow starts, such as on a schedule (e.g., daily at 10 AM), in response to an event (e.g., a new alert), or manually.
Step / Block	A single action in the workflow, such as running security queries, filtering results, performing cross-platform checks, or sending notifications.
Prompt	The AI instruction that guides a workflow step.
Automation	The ability to automatically gather, analyze, and take action on data (e.g., find users without MFA, determine who has the most permissions, send a Slack message, or create a ticket).
Integrations	Data sources and connectors (e.g., AWS, GitHub, Slack, Jira) for coordinated actions.
Notifications and reporting	Configurable outputs at the end of a workflow to share results, alerts, or summaries with relevant stakeholders.
Execution	A single run of a workflow from trigger to completion, with all steps performed and results tracked for review.
Directed Acyclic Graph (DAG)	The structured visual representation of workflow steps, showing the order, logic, and connections without loops.

Creating workflows

Workflows enable multi-step orchestration and automations that use queries, connectors, and AI to respond to security issues, coordinate actions, and reduce manual effort. They can be used for remediation, enrichment, reporting, and other structured flows directly inside your app.

Each workflow is structured as a Directed Acyclic Graph (DAG), giving you precise control over the order, conditions, and logic of each step. Ensuring consistent, repeatable responses to security events.

To create a workflow, use Sola AI to describe the outcome you want.

Sola AI will build your workflow, adding AI blocks (steps) with **prompts**, **connectors**, and **logic** based on your request. You can then review and adjust each prompt, connected data sources, and actions.

Workflows can only be created with Sola AI, not by manually building steps. Describe the workflow you need, and Sola AI will generate the blocks and logic for you, which you can adjust manually or with Sola AI.

Running and managing workflows

Workflows can be run manually, on a schedule, or triggered by events within Sola. When a workflow runs, each AI block executes in sequence according to the defined sequential logic.

To run a workflow:

- **Manual run** - Trigger the workflow directly from the app.
- **Scheduled run** - Set workflows to run automatically at defined times.
- **Event-triggered run** - Start a workflow based on specific or multiple alerts.

After a run completes, you can review the output for every step to see what actions were taken, what data was used, and the results produced. This provides visibility to validate the workflow's effectiveness and debug issues.

To manage a workflow:

- **Edit step prompts** - Adjust the instructions for each step manually or with Sola AI.
- **Update connectors** - Change or add integrations used by the workflow.
- **Adjust logic** - Modify conditions, branching, or sequence to adapt to evolving needs.

What makes Sola workflows different

AI-native, not just AI-supported
Sola Workflows don't just use AI, they are AI native. AI drives the logic, flow, and outcomes. This means they can reason and adapt dynamically, making them far more flexible and effective than traditional automations.

Resilient and adaptive execution
Traditional automations fail when they hit friction such as missing data, edge cases, or unexpected inputs. Sola's AI-led workflows adapt in real time. They're designed to creatively solve blockers, improvise when needed, and maintain progress toward meaningful outcomes.

Deterministic where it matters
Sola combines the flexibility of AI with the control of determinism. Enforcing strict and reliable logic for actions where precision is critical. Ensuring predictability and auditability.

Security intelligence built-in
Every workflow is grounded in Sola's domain expertise and understanding of security context. Instead of just executing tasks, workflows reason over identity, access, risk severity, and posture impact, turning automations into intelligent responses.

FAQs

Are workflows only for automating scheduled processes?

No. A single prompt can be used in most cases. However, when running complex and multiple step investigations, workflows can help create a relatively more deterministic outcome, be simpler to debug and provide more transparency into the outcome of each step in a long process.

What data sources and connectors can workflows use?

Workflows can potentially utilize any data source or connector associated with the app it is built in. To do this, data sources and connectors must be associated with the app beforehand. In addition, like the chat, workflows have the native ability to use the web for fetching specific information (with the same compliance and guardrails of the Sola chat).

Integrations

Data Sources

Connect Sola to your data sources and create your solutions

A data source is a secure connection from your Sola workspace to your organizational data.

Data can be imported from various sources, including cloud providers, cloud services, operational applications, security tools, and any other source desired.

Learn more about data privacy ↗.

Data sources and records quota are subject to pricing and packages ↗.

Available data source integrations

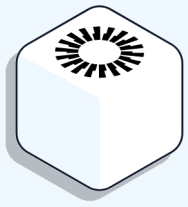
Amazon Web Services (AWS)

Google Cloud Platform (GCP)

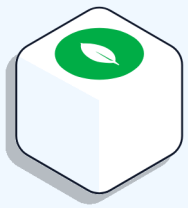
Microsoft Azure

Google Workspace

GitHub Cloud



Okta



MongoDB Atlas

Wiz

WordPress

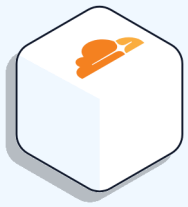
Sola Web Checker

Lovable App Scanner

CSV File

Zoom

Jira Cloud

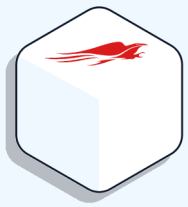


Cloudflare

SentinelOne

CircleCI

Datadog



Crowdstrike

Salesforce

Microsoft Entra ID

OpenAI Platform

OX Security

Upwind

Jamf Pro

Data source tables

Each **data source** contains multiple **tables** that store structured data retrieved from your connected source. This data is organized for easy analysis and is available for queries, visualizations, and alerts.

Sync status

Sola syncs **your data daily** to ensure your insights stay up to date. Sync cycle times vary based on the data size.

Checking sync status

To check the status of your data:

- **Data Sources page** - Click on a data source to see the sync status of its tables.
- **Query Library** - Click on a specific query to check which data tables are being used and their sync status.

Last sync information

Sync details are available at two levels:

- **Data source level** - Displays the overall sync status and total number of records synced during the last update.
- **Table level** - Shows individual table sync status and the number of records synced per table.

Table sync dependencies

Some table data depends on other tables to sync successfully. If a parent table fails to sync, its dependent (child) tables will also fail.

For example, an AWS user roles table depends on successfully retrieving AWS users. If the AWS users table fails to sync, the AWS user roles table will also fail.

Sync status types

Data source sync status	Table sync status
Synced - All tables successfully synced in the last sync cycle.	**Synced** - The table or tables under the same group successfully synced in the last sync cycle.
Partially Synced - Some tables did not sync in the last sync cycle.	**Syncing** - The table or tables under the same group are currently syncing.
Out of Sync - The last sync failed.	**Tables failed** - The table or tables under the same group failed to sync in the last sync cycle.
	Disabled - This table has been disabled and is not synced.
	Enabled - This table has been enabled and will sync in the next scheduled sync.

Disabling and Enabling Tables

Disable a table if you no longer need its data to be included in sync cycles, reducing unnecessary data updates, and records quota.

- Disabled tables will no longer sync or be available for queries, canvases, or alerts.
- Disabling a parent table will also disable any child tables that depend on it.
- Re-enable a table at any time to resume syncing and restore access to its data.

Snapshots and incremental data updates

Data source tables support historical data collection, allowing you to explore changes over time.

Table's data is updated in one of two methods:

- **Snapshots** - capture a single point-in-time state of the data.
- **Incremental** - continuously collect changes, building a stream of historical records over time.

To view and use historical snapshots saved by Sola and not only the latest snapshot, include the word "snapshots" in your query or Sola AI prompt.

By querying snapshots or incremental tables, you can explore the history of your data,

investigate posture changes in posture, track configuration drift, and review past states.

For example, ask Sola AI to:

- Show AWS EC2 inventory across multiple data snapshots.
- Investigate snapshots of Github users granted admin access in the last few days.
- Find Okta role or policy that has changed in the last 3 days across snapshots and how.

Historical snapshots are available up to 90 days back, limited by when your data source was connected.

FAQs

Why should I connect my data sources?

Connecting your data sources allows you to find answers to your security questions using your own organizational data.

The collected data is used to create apps.

Why should I trust Sola with my data?

At Sola, we prioritize the security and privacy ↗ of your data through strong encryption, strict access controls, and compliance with industry standards. Our systems are regularly audited, monitored for threats, and undergo continuous security improvements to ensure your sensitive data remains protected.

What happens with my data?

Sola has **read-only** access to your data. Once connected, your data is securely stored in **structured tables** that uniquely map the data content and its sources. This is what makes it easy to query and find answers to your specific use cases. **Sola AI** brings an additional layer of security knowledge available for you to use.

What happens if I don't connect my data?

If you don't connect a data source, you'll only be able to explore **sample data** within Sola. While this allows you to see how apps and queries work, you won't get **real insights** based on your organization's security data.

Why does Sola need wide permission-level read access to my data?

The answers to your questions could be hidden anywhere in your data. Limiting access to your data will limit the insights and answers you can gather.

Learn more about data privacy ↗

Amazon Web Services (AWS)

Connect Sola and AWS to get security insights

Overview

The Amazon Web Services (AWS) integration connects data from your AWS account to your Sola workspace, making it easy to search and find answers to your specific use cases.

The AWS integration gives you a complete view of your AWS environment, allowing you to monitor and analyze AWS security posture and potential threats.

With the AWS integration, you can:

- Ensure cloud security best practices
- Gain full visibility into your cloud resources
- Identify security risks across your cloud environment

Your data can only be retrieved, never modified.

Once connected, your data is securely stored, and access is restricted to retrieving configurations and metadata only. Authentication methods ensure secure delegation of permissions while maintaining data integrity.

No hidden indirect cloud provider charges
The Sola integration won't use resources that increase your cloud costs.

Set up AWS data source integration with Sola

Go to ***Integrations*** > ***Data Sources*** > click ***New data source*** > select ***AWS***.

The Sola wizard will take you through the steps.

Connect AWS to Sola

To connect AWS, you'll need an AWS account, with the necessary permissions to create an IAM role.

Cross-Account Role

Recommended for secure, production environments. These methods use an IAM role delegation within your account to securely grant Sola read-only access to your AWS services and resources.

- CloudFormation (Recommended)
- Terraform

Access Token

AWS IAM access key and secret.

Sync behavior and limitations

Some tables have specific sync constraints due to data size, retention policies, or performance considerations. Below are special cases to be aware of:

Table	Sync details
aws_securityhub_finding	Includes only findings with an Active status.

Explore the app gallery for AWS apps

Get started with AWS-focused security apps ↗, built by our expert security team.

Google Cloud Platform (GCP)

Connect Sola and GCP to get security insights

Overview

The Google Cloud Platform (GCP) integration connects data from your GCP account to your Sola workspace, making it easy to search and find answers to your specific use cases.

The GCP integration gives you a complete view of your GCP environment, allowing you to monitor and analyze GCP security posture and potential threats.

With the GCP integration, you can:

- Ensure cloud security best practices
- Gain full visibility into your cloud resources
- Identify security risks across your cloud environment

Your data can only be retrieved, never modified.

Once connected, your data is securely stored, and access is restricted to retrieving configurations and metadata only. Authentication methods ensure secure delegation of permissions while maintaining data integrity.

No hidden indirect cloud provider charges
The Sola integration won't use resources that increase your cloud costs.

Set up GCP data source integration with Sola

Go to ***Integrations*** > ***Data Sources*** > click ***New data source*** > select ***GCP***.

The Sola wizard will take you through the steps.

Connect GCP to Sola

To connect GCP, you'll need a GCP account with the necessary permissions to create a service account.

Service Account

Recommended for secure, production environments. These methods utilize a GCP Service Account within your project to securely grant Sola read-only access to your GCP services and resources.

- Service Account Key (Recommended)
- Terraform

Explore the app gallery for GCP apps

Get started with GCP-focused security apps ↗, built by our expert team.

Microsoft Azure

Connect Sola and Azure to get security insights

Overview

The Azure integration connects data from your Azure account to your Sola workspace, making it easy to search and find answers to your specific use cases.

The Azure integration gives you a complete view of your Azure environment, allowing you to monitor and analyze Azure security posture and potential threats.

With the Azure integration, you can:

- Ensure cloud security best practices
- Gain full visibility into your cloud resources
- Identify security risks across your cloud environment

Your data can only be retrieved, never modified.

Once connected, your data is securely stored, and access is restricted to retrieving configurations and metadata only. Authentication methods ensure secure delegation of permissions while maintaining data integrity.

No hidden indirect cloud provider charges
The Sola integration won't use resources that increase your cloud costs.

Set up Azure data source integration with Sola

Go to ***Integrations*** > ***Data Sources*** > click ***New data source*** > select ***Azure***.

The Sola wizard will take you through the steps.

Connect Azure to Sola

To connect Azure, you'll need an Azure account with the necessary permissions to create and configure an App Registration.

App Registration

These methods use an Azure App Registration within your subscription to securely grant Sola read-only access to your Azure services and resources.

- App Registration (Recommended)
- Terraform

Explore the app gallery for Azure apps

Get started with Azure-focused security apps ↗, built by our expert team.

Google Workspace

Connect Sola and Google Workspace to get security insights

Overview

The Google Workspace integration connects data from your Google Workspace to your Sola workspace, making it easy to search and find answers to your specific use cases.

This integration gives you visibility into drive and file-sharing activity across Google Workspace, enabling you to identify exposure risks and maintain compliance across your organization.

With the Google Workspace integration, you can:

- Detect publicly or externally shared files.
- Monitor file sharing permissions to prevent unauthorized access.
- Investigate access levels granted to third parties.
- Maintain compliance with internal and external data-sharing policies.

> **Your data can only be retrieved, never modified.**
>
> Once connected, your data is securely stored, and access is restricted to retrieving configurations and meta-data only. Authentication methods ensure secure delegation of permissions while maintaining data integrity.

Set up Google Workspace data source integration with Sola

Go to ***Integrations*** > ***Data Sources*** ↗ > click ***New data source*** > select ***Google Workspace***.

The Sola wizard will take you through the steps.

Connect Google Workspace to Sola

This integration links a Google Cloud Platform (GCP) **service accoun**t with a Google Workspace user.

It allows Sola to **impersonate workspace users** and securely sync their data without needing individual credentials.

Google Cloud Platform (GCP) Prerequisites

- **GCP project with owner permissions** - Use an existing project or create a new one for this integration.

Google Workspace Prerequisites

- **Super admin user** - Required for the initial integration setup, and will not be used by Sola.
- **Admin user** - Use an existing user or create a new one for this integration, with at least a Group Admin role permissions. The user must log in to Google Workspace at least once.

Explore the app gallery for Google Workspace apps

Get started with Google Workspace-focused security apps, built by our expert team.

GitHub Cloud

Connect Sola and GitHub Cloud to get security insights

Overview

The GitHub Cloud integration connects data from your GitHub account to your Sola workspace, making it easy to search and find answers to your specific use cases.

The GitHub integration gives you a complete view of your GitHub organization, allowing you to monitor and analyze GitHub security posture and potential threats.

With the GitHub integration, you can:

- Gain full visibility into repository access and permissions.
- Monitor security policies, including branch protection and organization settings.
- Track and manage Dependabot vulnerability alerts.
- Ensure security best practices for your GitHub organization.

> **Your data can only be retrieved, never modified.**
>
> Once connected, your data is securely stored, and access is restricted to retrieving configurations and metadata only. Authentication methods ensure secure delegation of permissions while maintaining data integrity.

Set up GitHub data source integration with Sola

Go to ***Integrations*** > ***Data Sources*** ↗ > click ***New data source*** > select ***GitHub Cloud***.

The Sola wizard will take you through the steps.

Connect GitHub to Sola

To connect GitHub Cloud, you'll need a GitHub account with organization owner permissions or admin access to all repositories in your GitHub organization.

GitHub App

Recommended for secure, production use.
This method leverages a GitHub App to grant Sola temporary, permissioned access to your GitHub resources, at either the repository or organization level, based on your choice. It minimizes risks associated with personal tokens and long-term credentials by enforcing strict, scoped access.

- GitHub App (Recommended)
  Install Sola's GitHub App to securely and easily grant access to your organization's GitHub data.
- Custom GitHub App
  Create and install your own GitHub App for full control over permissions and configuration (see how-to guide below)

Not sure which method to choose? We recommend starting with the GitHub App for the fastest and most reliable setup.

Access Token

Personal access token with read permissions.

Required scopes:

- repo
- read:org
- read:user
- user:email
- gist
- read:project

How do I set up a GitHub data source using custom GitHub App?

Complete the following steps to set up and configure your GitHub App to integrate Sola with GitHub Cloud.

> Learn more about creating GitHub Apps ↗.

1. Create and configure your GitHub App

- Log in to your GitHub account and go to ***GitHub Settings*** > ***Developer settings*** > ***GitHub Apps***.
- Click ***New GitHub App***, and set:
  - `App Name:` Sola Integration (recommended)
  - `Homepage URL:` https://app.sola.security ↗
  - `Webhook:` Uncheck Active (No webhook required)
  - `Permissions:` We recommend providing ***Read-Only*** permissions for all repository and organization related permissions.
    - To access GitHub workflows, you will need at least ***Read & Write*** permissions.
    - For valuable insights, provide access to at least the following scopes:
      - `repository:administration`
      - `repository:metadata`
      - `repository:webhooks`
      - `organization:administration`
      - `organization:webhooks`
- Click ***Create GitHub App*** and save the ***App ID***.

2. Generate a Private Key

- In your newly created app settings, navigate to ***General*** > ***Private Keys***.
- Click ***Generate a private key***.
- Securely store the downloaded **.pem file**. This is your GitHub App private key.

3. Install the GitHub App

- In the app settings, go to the ***Install App*** tab.
- Select the organization or account where you want to install the app.
- Click **Install** and confirm the installation.

4. Get your installation ID

After installing the app, you will be redirected to the installation page:
https://github.com/settings/installations/<app_installation_id>

- Copy and save the **<app_installation_id>**.

5. Provide your credentials to Sola

Complete the integration by providing the following parameters in the Sola wizard:

- [x] GitHub App ID
- [x] GitHub App Installation ID
- [x] GitHub App private key (.pem file)

Sync behavior and limitations

Some tables have specific sync constraints due to data size, retention policies, or performance considerations. Below are special cases to be aware of:

Table	Sync details
github_commit	Includes data from the last 1 month.
github_actions_artifact	Includes data from the last 3 months.
github_issue	Includes data from the last 3 months.
github_issue_comment	Inherits the 3-month limit from github_issue, as comments are linked to issues.
github_pull_request	Includes data from the last 3 months.
github_release	Includes data from the last 3 months.
github_tag	Includes data from the last 3 months.

Explore the app gallery for GitHub Cloud apps

Get started with GitHub-focused security apps ↗, built by our expert team.

Okta

Connect Sola and Okta to get security insights

Overview

The Okta integration connects data from your Okta account to your Sola workspace, making it easy to search and find answers to your specific use cases.

The Okta integration provides a complete view of your identity and access across your organization, allowing you to monitor and analyze Okta security posture and potential threats.

With the Okta integration, you can:

- Gain visibility into user identities, groups, and roles.
- Monitor Okta activity and get insights into configuration settings.
- Ensure users and applications only have the access they actually need.
- Maintain security best practices for your Okta environment.

Your data can only be retrieved, never modified.

Once connected, your data is securely stored, and access is restricted to retrieving configurations and metadata only. Authentication methods ensure secure delegation of permissions while maintaining data integrity.

Set up Okta data source integration with Sola

Go to ***Integrations*** > ***Data Sources*** ↗ > click ***New data source*** > select ***Okta***.

The Sola wizard will take you through the steps.

Connect Okta to Sola

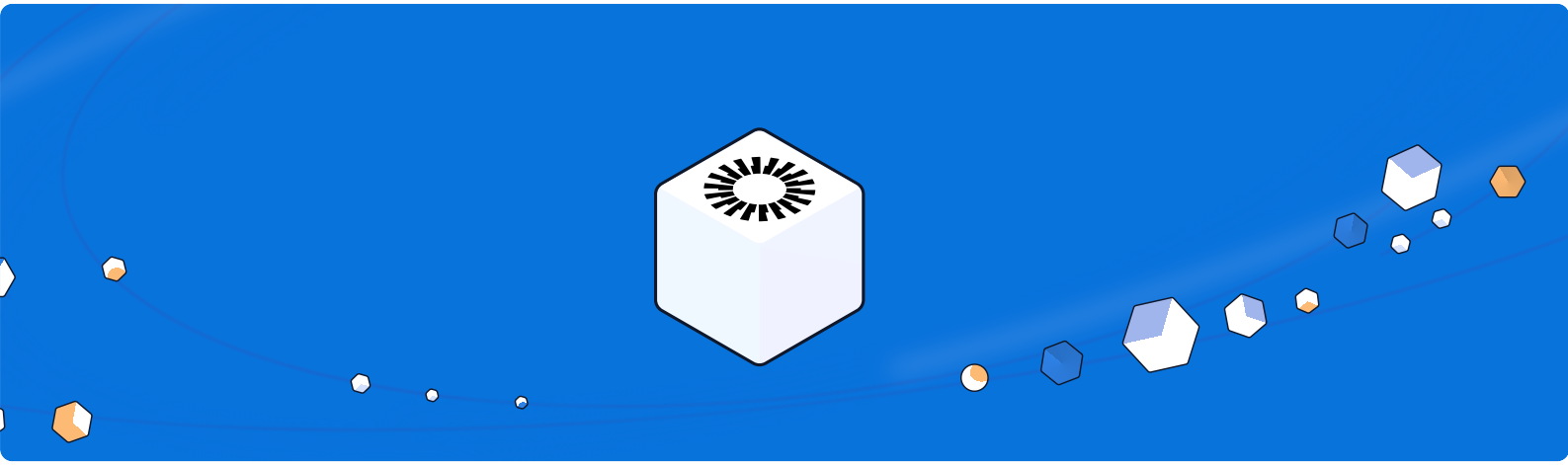
To connect Okta, you'll need an Okta admin account.

API Token

This method uses an API token ↗ to securely grant Sola read-only access to your Okta services and resources.

Explore the app gallery for Okta apps

Get started with Okta-focused security apps ↗, built by our expert team.



MongoDB Atlas

Connect Sola and MongoDB Atlas to get security insights

Overview

The MongoDB Atlas integration connects data from your MongoDB Atlas account to your Sola workspace, making it easy to search and find answers to your specific use cases.

The MongoDB Atlas integration gives you a complete view of your MongoDB environment, allowing you to monitor and analyze MongoDB security posture and potential risks.

With the MongoDB Atlas integration, you can:

- Gain insights into MongoDB user roles, access permissions, and authentication methods.
- Monitor network exposure and cluster security configurations.
- Track user activity trends.
- Ensure security best practices for your MongoDB environment.

Your data can only be retrieved, never modified.

Once connected, your data is securely stored, and access is restricted to retrieving configurations and metadata only. Authentication methods ensure secure delegation of permissions while maintaining data integrity.

Set up MongoDB Atlas data source integration with Sola

Go to ***Integrations*** > ***Data Sources*** ↗ > click ***New data source*** > select ***MongoDB Atlas***.

The Sola wizard will take you through the steps.

Connect MongoDB Atlas to Sola

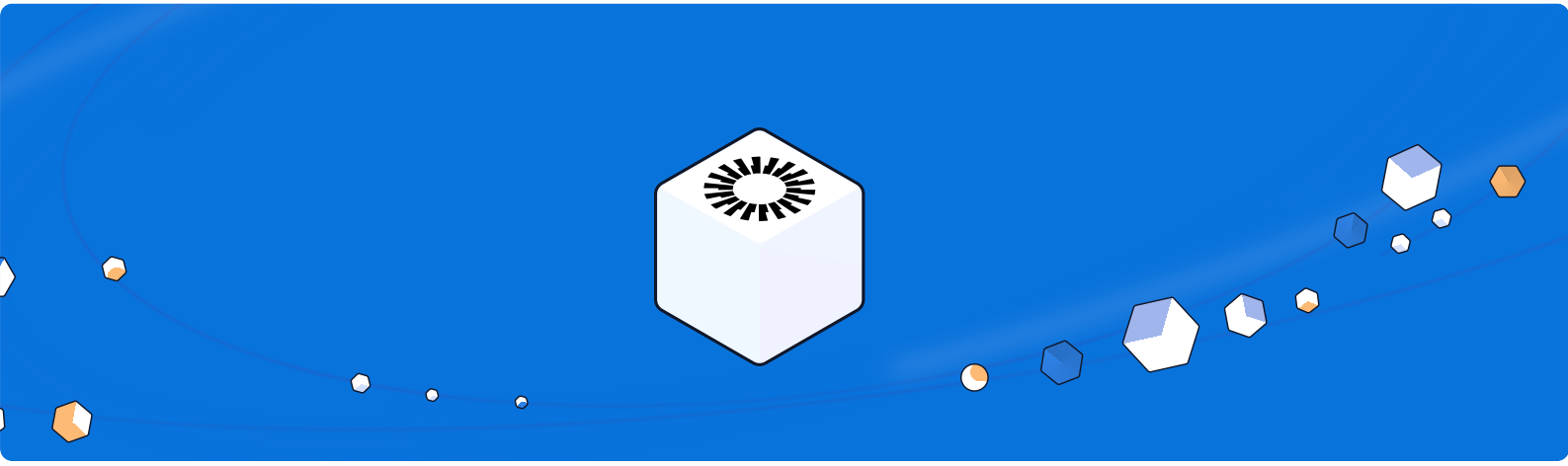
To connect MongoDB Atlas, you'll need a MongoDB Atlas account with organization owner access to Atlas.

API Key

This method uses an API key ↗ to securely grant Sola read-only access to your MongoDB Atlas services and resources.

Explore the app gallery for MongoDB Atlas apps

Get started with MongoDB-focused security apps ↗, built by our expert team.



Wiz

Connect Sola and Wiz to get security insights

Overview

The Wiz integration connects data from your Wiz account to your Sola workspace, making it easy to search and find answers to your specific use cases.

The Wiz integration provides a complete view of your Wiz environment, allowing you to monitor and analyze security posture and potential risks.

With the Wiz integration, you can:

- Gain visibility into security issues across your Wiz projects.
- Identify misconfigurations, vulnerabilities, compliance risks, and other findings.
- Get a centralized view of the most critical issues detected by Wiz.
- Monitor access controls and manage service accounts.
- Consolidate Wiz insights with other security tools for cross-platform analysis.

> **Your data can only be retrieved, never modified.**
>
> Once connected, your data is securely stored, and access is restricted to retrieving configurations and metadata only. Authentication methods ensure secure delegation of permissions while maintaining data integrity.

Set up Wiz data source integration with Sola

Go to ***Integrations*** > ***Data Sources*** ↗ > click ***New data source*** > select ***Wiz***.

The Sola wizard will take you through the steps.

Connect Wiz to Sola

To connect Wiz, you'll need a Wiz admin account with the `read:all` scope permissions to create and configure a service account.

Service Account

This method uses a Wiz service account to securely grant Sola read-only access to your Wiz findings, issues, and configurations.

Explore the app gallery for Wiz apps

Get started with Wiz-focused security apps ↗, built by our expert security team.

WordPress

Connect Sola and WordPress to get security insights

Overview

The WordPress integration allows you to enrich Sola Apps with issues found for your WordPress websites, scanning for common vulnerabilities and misconfigurations.

Add your WordPress website URLs to uncover hidden risks and continuously monitor the security posture of your public WordPress websites.

With the WordPress integration, you can:

- Get visibility into security risks across all public WordPress sites
- Uncover hidden exposures that traditional tools can miss
- Monitor the security posture of your assets over time
- Surface exposed admin panels and login endpoints
- Track headers and security best practice compliance

Your data can only be retrieved, never modified.

Once connected, your data is securely stored, and access is restricted to retrieving configurations and metadata only. Authentication methods ensure secure delegation of permissions while maintaining data integrity.

Set up WordPress data source integration with Sola

Go to ***Integrations*** > ***Data Sources*** ↗ > click ***New data source*** > select ***WordPress***.

The Sola wizard will take you through the steps.

Connect WordPress to Sola

Analyze your WordPress websites using one of two verification methods to confirm ownership and begin scanning for security issues.

Email domain matching

Automatic verification

This method matches the domain of the WordPress site to the email domain associated with your Sola account.

- Quick and easy setup

> Only websites matching your **verified email domain** can be scanned using this method.
>
> For example, if you signed up with *name@mysecurityorg.com*, Sola will only be able to scan ***.mysecurityorg.com** (your domain and any subdomains), such as *blog.mysecurityorg.com* or *wp.mysecurityorg.com*.

HTTP verification using a TXT file

This method allows HTTP verification by uploading a TXT file to your website.

- Flexible and secure for multi-site environments

How to set up HTTP verification:

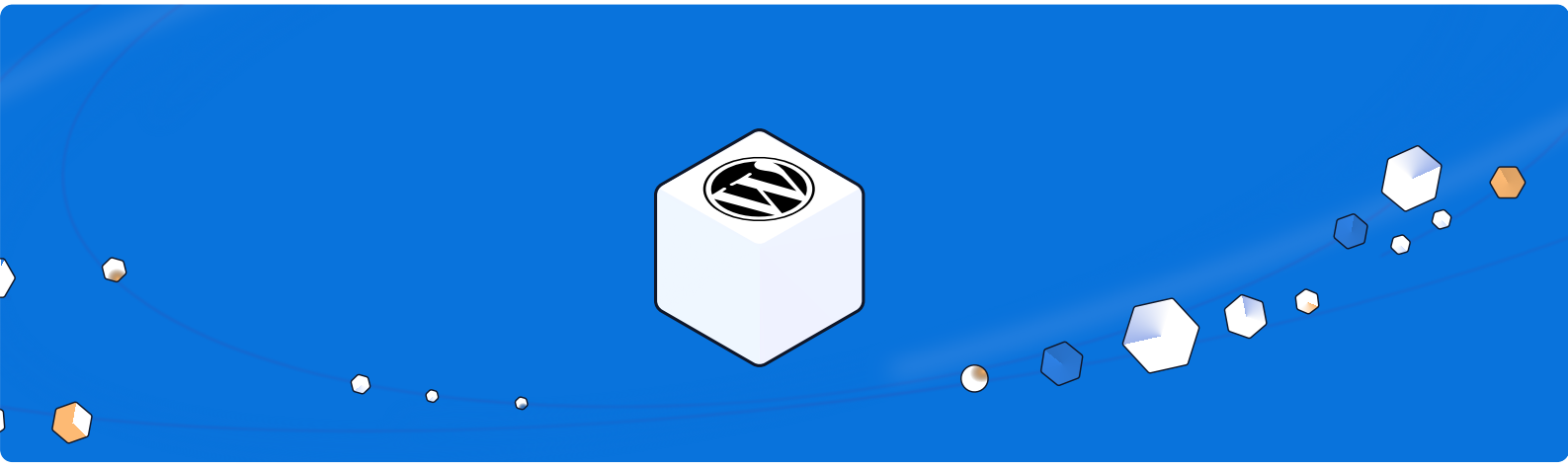
Upload the provided UUID in the Sola wizard as a ***sola-verification.txt*** file to your WordPress site under the following path:

```
/.well-known/sola-verification.txt
```

For example: `https://my-wordpress-site.com/.well-known/sola-verification.txt`

Explore the app gallery for WordPress apps

Get started with WordPress-focused security apps ↗, built by our expert security team.



Sola Web Checker

Analyze external domains, websites, and internet-facing infrastructure to get security insights

Overview

The Sola Web Checker integration allows you to enrich Sola Apps with data from your external domains, URLs, and host endpoints, scanning for common vulnerabilities and misconfigurations.

Add your domains, URLs, or IP addresses to uncover hidden risks, validate critical security protections, and continuously monitor the security posture of your public assets.

With the Sola Web Checker integration, you can:

- Monitor TLS protocol versions, cipher suites, and encryption strength
- Detect missing or misconfigured HTTP security headers
- Track certificate validity, expiration, and best practice compliance
- Identify weak configurations and DNS record issues
- Continuously assess domain posture over time

Your data can only be retrieved, never modified.

Once connected, your data is securely stored, and access is restricted to retrieving configurations and metadata only. Authentication methods ensure secure delegation of permissions while maintaining data integrity.

Set up Web Checker data source integration with Sola

Go to ***Integrations*** > ***Data Sources*** > click ***New data source*** > select ***Sola Web Checker***.

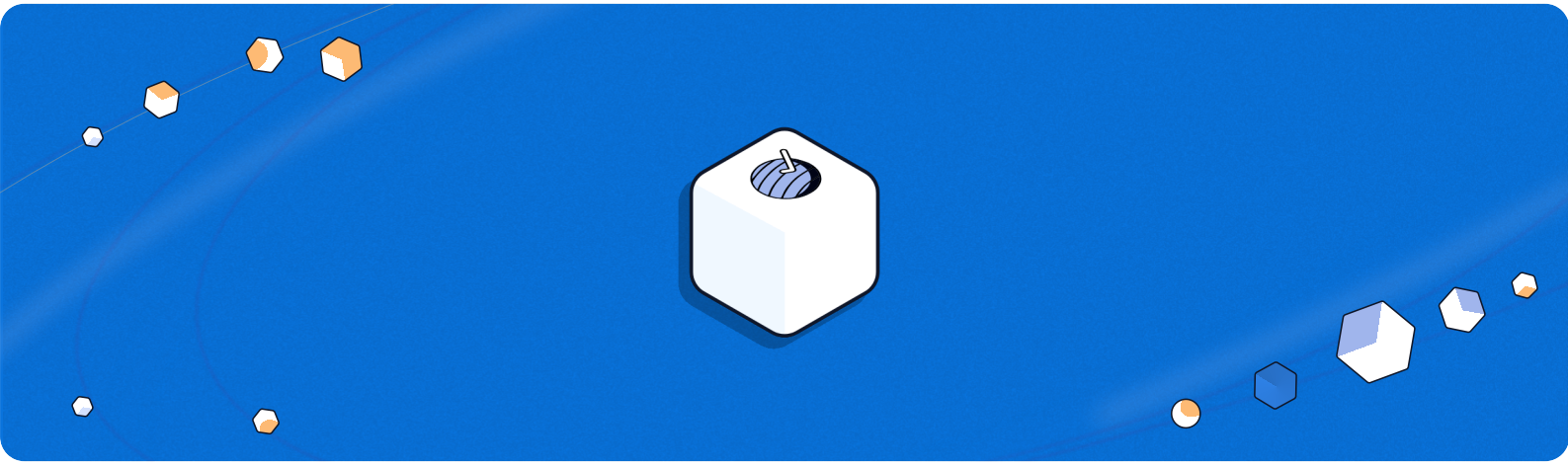
The Sola wizard will take you through the steps.

Add domains, URLs and host endpoints

Analyze DNS records, security and response headers, certificates, TLS, and public accessibility by adding your organization's publicly facing web assets.

Explore the app gallery for Sola Web Checker apps

Get started with Sola Web Checker - Domain Insights security apps ↗, built by our expert security team.



Lovable App Scanner

Analyze Lovable apps to detect endpoint, authentication, and exposure risks

Overview

The Lovable App Scanner integration brings security insights from applications built on the no-code platform Lovable.dev into Sola for analysis and monitoring.

This integration enables external scanning of your live Lovable apps.

With the Lovable App Scanner integration, you can:

- Get visibility into security risks across public Lovable apps
- Uncover vulnerabilities, misconfigurations, and hidden exposures
- Get actionable insights to improve your security posture

Your data can only be retrieved, never modified.

Once connected, your data is securely stored, and access is restricted to retrieving configurations and metadata only. Authentication methods ensure secure delegation of permissions while maintaining data integrity.

Set up Lovable App Scanner data source integration with Sola

Go to ***Integrations*** > ***Data Sources*** > click ***New data source*** > select ***Lovable App Scanner***.

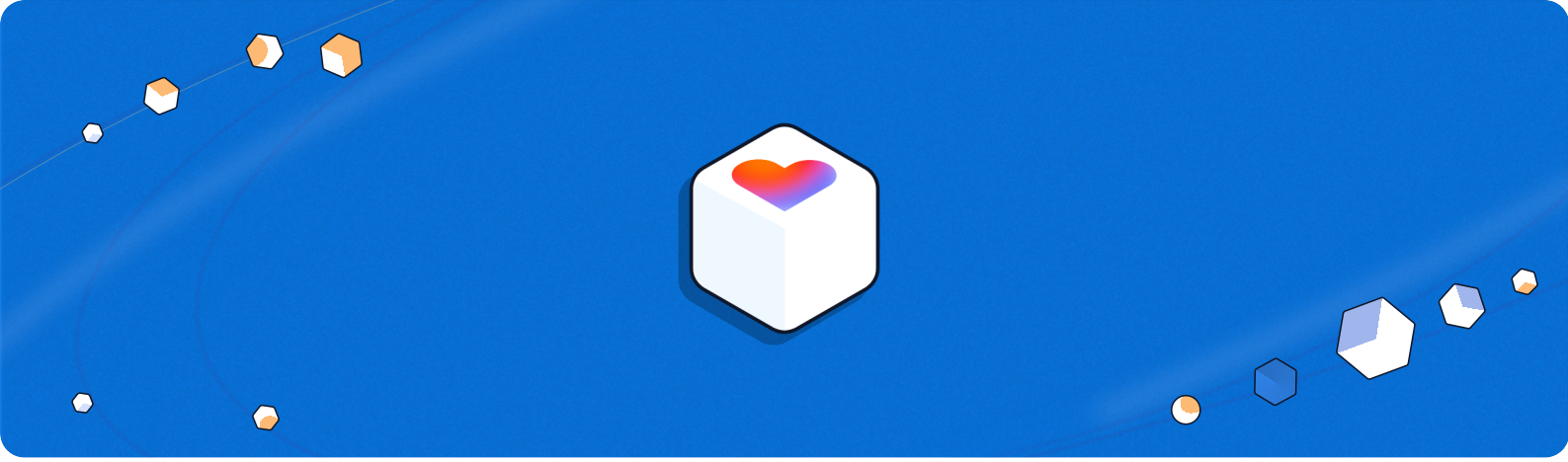
The Sola wizard will take you through the steps.

Add Lovable app public URLs

Uncover potential security risks and continuously monitor their external security posture, without modifying your live app.

Explore the app gallery for Lovable App Scanner

Get started with Lovable App Scanner - Security Posture, built by our expert security team.



CSV File

Upload CSV files with custom datasets for analysis and insights

Overview

The CSV File integration allows you to bring unique datasets into Sola by uploading structured CSV files.

Leverage your own data across Sola's capabilities to uncover insights, and analyze patterns within your custom datasets.

With the CSV file integration you can bring in custom datasets to explore insights beyond standard integrations.

> **Your data can only be retrieved, never modified.**
>
> Once connected, your data is securely stored, and access is restricted to retrieving configurations and metadata only. Authentication methods ensure secure delegation of permissions while maintaining data integrity.

Set up CSV File data source integration with Sola

Go to ***Integrations*** > ***Data Sources*** ↗ > click ***New data source*** > click the ***Upload CSV*** button (top right of screen).

The Sola wizard will take you through the steps.

Add CSV files

Start exploring your own data instantly, no connectors or integrations required.

Zoom

Connect Sola and Zoom to get security insights

Overview

The Zoom integration connects data from your Zoom account to your Sola workspace, making it easy to search and find answers to your specific use cases.

The Zoom integration provides a comprehensive view of your Zoom environment including users, roles, meetings, and settings to monitor security posture and compliance.

With Zoom integration you can:

- Gain visibility into configuration changes
- Enforce secure collaboration policies and security best practices
- Ensure compliance with internal policies and industry standards

> **Your data can only be retrieved, never modified.**
>
> Once connected, your data is securely stored, and access is restricted to retrieving configurations and metadata only. Authentication methods ensure secure delegation of permissions while maintaining data integrity.

Set up Zoom data source integration with Sola

Go to ***Integrations*** > ***Data Sources*** > click ***New data source*** > select ***Zoom***.

The Sola wizard will take you through the steps.

Connect Zoom to Sola

To connect Zoom to Sola, you need a Zoom account with Owner or Admin permissions that allow creating Server-to-Server OAuth apps in the Zoom Marketplace.

How do I set up a Zoom data source using Server-to-Server OAuth app?

Complete the following steps to set up and configure your Zoom app to integrate Sola with Zoom.

1. Sign in to your Zoom account.
2. Go to Build App in Zoom Marketplace, select ***Server-to-Server OAuth***, and click ***Create***.
3. Name the app and click ***Create***.
4. Copy and save the generated
   - ***Account ID***
   - ***Client ID***
   - ***Client Secret***
5. Complete the ***Information*** and ***Feature*** steps.
6. Add the following scopes:
   - `account:read:lock_settings:admin`
   - `account:read:trusted_domains:admin`
   - `account:read:managed_domains:admin`
   - `account:read:settings:admin`
   - `group:read:list_members:admin`
   - `group:read:list_groups:admin`
   - `meeting:read:list_meetings:admin`
   - `cloud_recording:read:list_user_recordings:admin`
   - `role:read:role:admin`
   - `role:read:role:master`
   - `role:read:list_roles:admin`
   - `role:read:list_members:admin`
   - `user:read:user:admin`
   - `user:read:list_users:admin`
7. Activate the app.
8. Complete the integration by providing the following parameters in the Sola wizard:
   - ***Account ID***
   - ***Client ID***
   - ***Client Secret***
9. Click ***Test Connection*** to validate the details, then click ***Next*** to continue.

Learn more about creating a Server-to-Server OAuth app.

Jira Cloud

Connect Sola and Jira Cloud to get security insights

Overview

The Jira Cloud integration allows you to enrich Sola apps with project and issue tracking data for enhanced visibility and operational insights.

The Jira Cloud integration imports data on projects, issues, tasks, boards, sprints, users, groups, permissions, audit records, and more. This provides security teams with visibility into access configurations and administrative changes, alongside development activity that may affect security posture.

With the Jira Cloud integration, you can:

- Gain visibility into Jira projects, issues, and sprints to understand development activity that may impact security.
- Monitor Jira permission schemes, roles, and security levels to ensure proper access controls.
- Review Jira audit records to track administrative changes and support compliance monitoring.
- Analyze Jira boards and sprints to identify bottlenecks that could delay security-related work.

> **Your data can only be retrieved, never modified.**
>
> Once connected, your data is securely stored, and access is restricted to retrieving configurations and metadata only. Authentication methods ensure secure delegation of permissions while maintaining data integrity.

Set up Jira data source integration with Sola

Go to ***Integrations*** > ***Data Sources*** > click ***New data source*** > select ***Jira Cloud***.

The Sola wizard will take you through the steps.

Connect Jira to Sola

To connect Jira Cloud, you need a Jira account with permissions according to the data you want to access, including security, projects, users and groups, and boards, ensuring secure and controlled data access.

Jira App

This method leverages a Jira App to securely grant Sola read-only, permissioned access to your Jira resources. It minimizes risks associated with personal tokens and long-term credentials by enforcing strict, scoped access.

When prompted, sign in with your Jira administrator account and approve the requested access.

Cloudflare

Connect Sola and Cloudflare to get security insights

Overview

The Cloudflare integration connects your Cloudflare environment to Sola, making it easy to search and find answers to your specific use cases.

The Cloudflare integration provides visibility into accounts, services, and configurations for monitoring security posture, allowing you to monitor and analyze access controls, account settings, traffic management, policy enforcement, and audit logs.

With Cloudflare integration you can:

- Gain visibility into access policies and account configurations.
- Monitor and analyze DNS, load balancing, and traffic management.
- Review page rules, workers, and zones for compliance with best practices.
- Track user activity and audit logs across your Cloudflare environment.

> **Your data can only be retrieved, never modified.**
>
> Once connected, your data is securely stored, and access is restricted to retrieving configurations and metadata only. Authentication methods ensure secure delegation of permissions while maintaining data integrity.

Set up Cloudflare data source integration with Sola

Go to ***Integrations*** > ***Data Sources*** ↗ > click ***New data source*** > select ***Cloudflare***.

The Sola wizard will take you through the steps.

Connect Cloudflare to Sola

To connect Cloudflare, you'll need a Cloudflare user with an administrator role.

API Token

This method uses an API token ↗ to securely grant Sola read-only access to your Cloudflare services and resources.

SentinelOne

Connect Sola and SentinelOne to get security insights

Overview

The SentinelOne integration connects endpoint security data to your Sola workspace, making it easy to search and find answers to your specific use cases.

The SentinelOne integration provides a comprehensive view of your endpoint security environment, enabling you to monitor endpoint agents, analyze threat detections, and track overall security posture across your organization.

With the SentinelOne integration, you can:

- Gain visibility into endpoint agents and threat detection events.
- Monitor vulnerabilities, applications, and detection rule activity.
- Review security management policies.
- Track and analyze endpoint activity across your environment.

> **Your data can only be retrieved, never modified.**
>
> Once connected, your data is securely stored, and access is restricted to retrieving configurations and metadata only. Authentication methods ensure secure delegation of permissions while maintaining data integrity.

Set up SentinelOne data source integration with Sola

Go to ***Integrations*** > ***Data Sources*** ↗ > click ***New data source*** > select ***SentinelOne***.

The Sola wizard will take you through the steps.

To connect SentinelOne, you'll need a SentinelOne tenant with an administrator user.

API Token

This method uses an API token ↗ to securely grant Sola read-only access to your SentinelOne services and resources.

Connectors

Connect Sola to external services and gain real time actionability

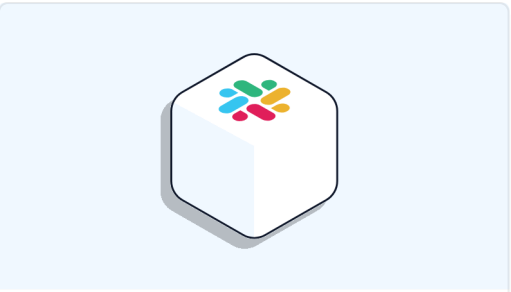
A connector is an integration that allows Sola to interact with external services in real time to perform actions, directly through in-chat Sola AI conversations.

Connectors are used to:

- Share findings during analysis and investigation
- Support remediation and incident response by escalating issues directly to the right stakeholders (Sola users or not)
- Offload insights to relevant channels in your organization

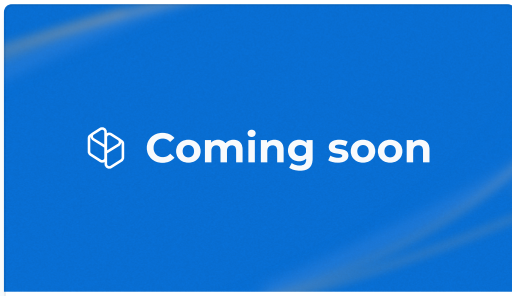
Learn more about data privacy ↗.

Available connector integrations



Slack

Jira



New connectors on the way

Triggering connectors

After adding a connector to your workspace, you can add it to apps.

Connectors are automatically triggered within the Sola AI chat to:

- Share findings, insights, and results with teammates via Slack.
- Create tickets and epics in Jira (coming soon).

Sola AI prompt tip ✨

Connectors enable these actions instantly during conversations.

For example, ask Sola AI to:

"Send the top 3 most critical issues to my SecOps Slack channel, together with remediation steps".

Permissions and actions

Connectors require permission to access, read, or write data in external systems.

There are three levels of guardrails, **workspace**, **app**, and **chat**.

1. **Workspace level**
   Configure connector permissions and scopes when adding the connector to your workspace.
   - Sola App comes pre-configured with required permissions.
   - Custom app includes a set of recommended permissions
     Note: Not applying the recommended permissions may limit functionality or prevent certain actions from working as expected.
2. **App level**
   Control which apps can use a given connector. Apps must be explicitly connected.
3. **Chat level**
   When an in-chat conversation triggers an action that needs external access, Sola will prompt for one of the following permissions:
   - Deny
   - Allow once
   - Allow for this chat

FAQs

What's the difference between connectors and data sources?

Data sources bring in and save large datasets into Sola for querying and analysis.

Connectors are used to enrich, validate, or act on data in real time.

Can I use connectors without a data source?

Yes. Connectors are used to send information from Sola to external services, this does not depend on a data source being connected.

Do connectors affect my data quota?

Connectors do not sync or store structured records and do not count toward your data source records quota. However, they can indirectly affect other limits such as your Sola AI requests per week. For more information, see Sola pricing ↗.

Slack

Connect Sola and Slack to get security insights

The Slack integration brings Sola AI directly into Slack, enabling it to provide insights, escalate issues, and participate in security conversations.

The Slack integration allows you to join public channels, read messages, and send messages to help teams stay informed and take action in context.

With the Slack integration, you can:

- Enable real-time collaboration and assistance directly from Sola inside Slack.
- Receive security alerts and insights without switching tools.
- Keep teams aligned on security actions, investigations, and decisions.

Sola can only perform the actions you approve.

Connectors require explicit permission to access or act on external systems. Permissions are securely managed at the workspace, app, and chat level to ensure control at every step.

Set up Slack connector integration with Sola

Go to ***Integrations*** > ***Connectors*** > click ***New connector*** > select ***Slack***.

The Sola wizard will take you through the steps.

Connect Slack to Sola

To connect Slack, you'll need a Slack account with a full member Slack role or higher.

Slack App

Recommended for secure, production use.
This method uses a Slack App to grant Sola scoped, permission-based access to your Slack workspace. It reduces the risks associated with user tokens and long-lived credentials by enforcing granular permission scopes and using Slack's OAuth-based authentication.

- Slack App (Recommended)
  Install Sola's Slack App to securely and easily grant access to your organization's Slack workspace.
- Custom Slack App
  Create and install your own Slack App for full control over permissions and configuration (see how-to guide below)

Not sure which method to choose? We recommend starting with the Slack App for the fastest and most reliable setup.

How do I set up a Slack connector using custom Slack App?

Complete the following steps to set up and configure your Slack App to integrate Sola with Slack.

> Learn more about creating Slack Apps ↗.

1. Create your Slack App

- In your Slack apps page ↗, click ***Create New App***, and select ***From scratch***.
- Set an ***App Name*** (Sola Integration), select a workspace, and click ***Create App***.

2. Configure permissions

- Go to ***OAuth & Permissions*** > ***Scopes*** > ***Bot Token Scopes***, select ***Add an OAuth Scope***.
- Add the following required scopes:
  - `assistant:write` - Allow Sola to act as an app agent.
  - `channels:history` - View messages and other content in public channels that Sola has been added to.
  - `channels:join` - Join public channels in a workspace.
  - `channels:read` - View basic information about public channels in a workspace.
  - `chat:write` - Send messages as @Sola App.
  - `emoji:read` - View custom emoji in a workspace.
  - `groups:read` - View basic information about private channels that Sola has been added to.
  - `im:read` - View basic information about direct messages that Sola Security has been added to.
  - `reactions:read` - View emoji reactions and their associated content in channels and conversations that Sola Security has been added to.
  - `reactions:write` - Add and edit emoji reactions.
  - `users.profile:read` - View profile details about people in a workspace.
  - `users:read` - View people in a workspace.
  - `users:write` - Set presence for Sola.

3. Install the Slack App

- Go to ***Install App***, click ***Install to Workspace***, and copy your ***Bot User OAuth Token***.

4. Paste the *Bot User OAuth Token* in the Sola wizard.

5. Click *Test Connection* to validate the details and continue.

Jira

Connect Sola to Jira to expedite remediation

The Jira integration brings Sola AI into your Jira projects allowing you to create, update, and track Jira issues directly from in-chat conversations.

The Jira integration helps streamline remediation management by turning your security findings into actionable work, keeping teams aligned and responsive.

With the Jira integration, you can:

- Turn security findings into Jira epics, tasks, or stories directly from Sola AI conversations.
- Route issues to the right stakeholders with relevant context for resolution.
- Monitor issue status, transitions, and comments, from detection to closure.

Sola can only perform the actions you approve.

Connectors require explicit permission to access or act on external systems. Permissions are securely managed at the workspace, app, and chat level to ensure control at every step.

Set up Jira connector integration with Sola

Go to ***Integrations*** > ***Connectors*** > click ***New connector*** > select ***Jira***.

The Sola wizard will take you through the steps.

Connect Jira to Sola

To connect Jira, it is recommended to use a **dedicated organization user account**, for the Sola connector, and not a personal account. For example, *sola.jira.user@company.com*.

Jira App

Recommended for secure, production use.
This method uses a Jira App to grant Sola scoped, permission-based access to your Jira account.

- Jira App (Recommended)
  Install Sola's Jira App to securely and easily grant access to your organization's Jira account.

API Token

This method uses a Jira API token to securely grant Sola access to your Jira account.

The token includes the following classic scopes:

- `read:jira-user`
- `read:jira-work`
- `write:jira-work`

Available actions with the Jira connector

- **Create issue** - Create a new Jira issue (Task, Bug, Story, Epic, etc.) with summary, description, assignee, components, and custom fields.
- **Update issue** - Update an existing Jira issue summary, description, priority, assignee, or labels.
- **Get issue** - Retrieve detailed information about a specific Jira issue by its key.
- **Get projects** - List all accessible Jira projects.
- **Get issue types** - List available issue types (Task, Bug, Story, Epic, etc.) for a specific project.
- **Add comment** - Add a comment to an existing Jira issue.
- **Get comments** - Retrieve comments for a specific Jira issue.
- **Transition issue** - Change the status of a Jira issue (e.g., move to In Progress, Done, Closed) using a transition ID.
- **Get transitions** - List all possible status transitions for a Jira issue.
- **Search fields** - Search for available fields in the Jira instance (e.g., custom fields).
- **Create issue link** - Link two Jira issues together (e.g., “relates to”, “blocks”, etc.).
- **Link to epic** - Link an issue to an Epic.
- **Batch create issues** - Create multiple Jira issues in a single batch operation.
- **Get link types** - List all available Jira issue link types.
- **Get project issues** - List issues for a specific Jira project.
- **Search issues** - Search for Jira issues using JQL (Jira Query Language).
- **Get user profile** - Retrieve a Jira user’s profile by identifier (accountId, username, or email).

System Management

Settings

View and manage the settings to your Sola account, workspaces and apps

There are two types of settings categories in Sola: account settings and workspace settings.

To access your Sola settings, click *Settings* from the sidebar.

1. Account settings

This is where you can manage your personal Sola account name, email, password, and AI assistant activation.

✨ Sola AI assistant

Enable or disable the option to skip the Sola AI assistant when you are creating new queries.

2. Workspace settings

This is where you can manage your general workspace name, members, and more.

Members

Workspace owners and admins can invite new members to a workspace using a link or by email, and define their roles.

Leaving a workspace

A workspace requires at least one owner. When leaving a workspace, you must assign a new owner.

Deleting a workspace

Workspace owners can delete a workspace when it is no longer needed. Deleting a workspace permanently removes all workspace information and associated data.

Once a workspace is deleted, all members will lose access, and **this action cannot be undone**.

Roles and permissions

There are two types of roles and permissions levels: workspace permissions and app permissions.

Workspace permissions

Role type	Permission description
Owner	Full access to manage all workspace settings, members, integrations, and apps.
Admin	Manage workspace settings, members, integrations, and apps you are an admin of. Excludes plan, billing, and password reset.
Member	View workspace settings, members, integrations, and apps.

App permissions

Role type	Permission description
Admin	Full access to manage members, add/edit/delete apps, queries, canvases, and alerts.
Contributor	View app info, add/edit/delete queries, canvases, and alerts.
Viewer	Read-only access to view queries, canvases, and alerts.

3. Privacy and security settings

This is where you can manage your account settings, including password, authentication methods, session activity, and Single Sign-On (SSO).

To manage your privacy and security settings, go to *Settings* > *Privacy and Security*.

- **My Account** - Multi-factor authentication, password, Login sessions
- **Workspace** (applicable for admin and owner users) - Account security, security check up

Single Sign-On (SSO)

Workspace owners can configure SSO to allow members to sign in to Sola using their organization's identity provider (IdP).

Go to *Settings* > *Privacy and Security* > *SSO*, click "*Setup SSO connection*" to open the wizard and add a new connection.

Available connection options:

- **SAML**: Okta, Azure AD, Google, OneLogin, Ping Identity, JumpCloud, Rippling, Custom SAML
- **OpenID**: Okta, Custom OpenID

Once configured, SSO centralizes authentication and improves access security across your workspace.

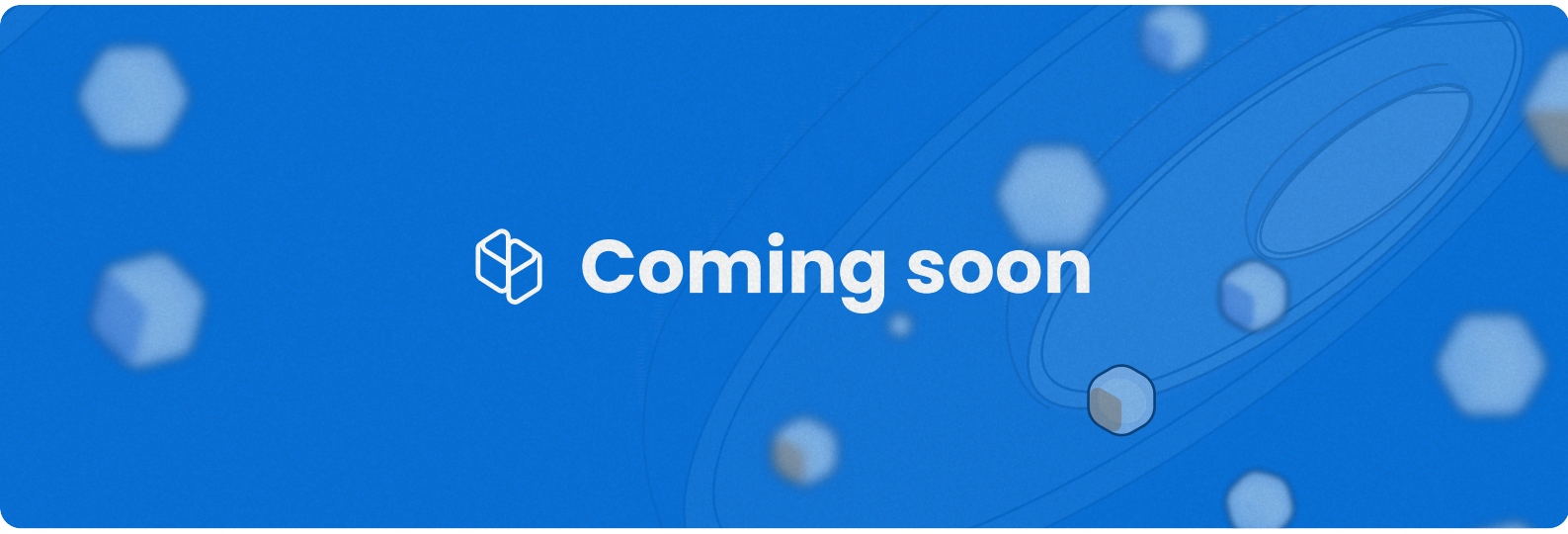
FAQs

Can I recover a deleted workspace?

No. Deleting a workspace is permanent and cannot be undone.

Resources

Glossary



FAQs

Find answers to your top questions

Browse the FAQs below or type your question in the search box at the top right, and our AI assistant will guide you.

About Sola

What's unique about Sola?

Sola isn't just another security tool. It's a new way to build security solutions, designed for flexibility, speed, and collaboration.

- Build security solutions, your way. No need for an engineering team.
- Create security apps tailored to your needs using Sola AI or SQL.
- From questions to answers, fast. Ask, analyze risks, and trigger alerts.
- Designed for teams. Share insights, track findings, and collaborate.

Sola helps you move from security gaps to solutions, faster than ever.

How much does Sola cost?

Sola is free for all users during this initial beta phase. Some limitations apply to keep things fair and sustainable, but our goal is to empower you to explore and build with Sola.

Sola will always remain affordable and accessible as we grow.

For more details, visit our pricing page ↗.

Sola Concepts

What are apps, and how should I build them?

A Sola app is a custom security solution you build based on your needs. Each app functions independently and is built to answer your security questions across different domains.

There's no single way to structure your apps. Sola gives you the flexibility to organize them however you prefer:

- By security domain. For example, Identity and Access Management, Cloud Security.
- By vendor. For example, AWS Security, GitHub Security.
- By team. For example, SOC Team Monitoring, CISO Dashboard.

Whether you're building a single-use app or a more complex multi-source security solution, it's up to you and your use case.

Apps connect to relevant data sources and can be shared with your team for collaboration.

Who is considered a workspace member?

An organization can have multiple workspaces, and users can be members of one or more. As a workspace member, your role and permissions determine what you can do. Whether it's managing settings, inviting members, building or viewing apps.

Do you need to know how to code or SQL to build a security tool in Sola?

Sola offers a no-code experience, making it easy to create security apps using natural language with Sola AI. You can ask security questions, uncover insights, and set up alerts—no coding required. Start quickly with ready-to-use apps from the App Gallery, built by our expert security team.

What should I do if I don't have access to connect a data source?

In the meantime, you can explore Sola using a sandbox environment or placeholder data source to test features and get familiar with the platform before connecting your own data.

Privacy and Security

Is my data secure?

Sola is built by security people, for security people. Security is at the core of everything we do. We uphold the highest industry standards to protect your data, systems, and operations.

Your data is encrypted at rest and in transit, with access strictly controlled through a secure authentication and authorization process.

Learn more about our security practices in Sola's Trust Center ↗.

Where is my data stored?

Sola only provides a managed service. Your data is saved within Sola databases, according to compliance and audit standards.

What access do you have to my data?

Sola has read-only access to your data and cannot modify or delete any information. Once connected, your data is securely stored, and access is restricted to retrieving configurations and metadata only. Authentication methods ensure secure delegation of permissions while maintaining data integrity. Also, you control which data is synced by enabling or disabling specific tables within your data source.

Is Sola Security SOC 2 certified?

Yes, Sola Security is SOC 2 certified.

Sola has successfully completed the SOC 2 Type II audit, which demonstrates our commitment to maintaining the highest standards for security, availability, and confidentiality. This independent third-party assessment validates that our systems and processes are designed and operated to safeguard customer data.

Learn more about our other key industry certifications, such as ISO 27001, and our latest security and compliance documentation, in the Trust Center ↗.

Does Sola support Single Sign-On (SSO)?

Yes. Sola supports SSO via SAML and OpenID, with integrations for identity providers such as Okta, Azure AD, Google, OneLogin, Ping Identity, and JumpCloud. Configure SSO in Settings.

Sola AI

How does Sola AI assistant use my data?

Sola AI assistant follows strict security practices to keep your data safe. Your data is stored securely according to our standard security policies ↗.

Sola AI assistant does not use your data to train our models. Any data processed through Sola AI is used solely to generate responses and is not retained for training purposes.

Can I enable or disable Sola AI?

Yes. You can enable or disable the option to skip the Sola AI assistant when creating new queries.