

From exposure to evidence.

CTEM with AI at the core.

Hashiro connects AI-led pentesting, external attack-surface visibility, cloud posture and vulnerability workflows in a Continuous Threat Exposure Management platform. Teams define the scope, review candidate findings and carry evidence through remediation and retesting.

AI proposes. Humans decide.

Built for in-house security teams and security service providers managing assessments across customer organizations.

<https://hashiro.ai> / hello@hashiro.ai

One connected exposure workflow

AI-led pentesting

Run scoped assessments with Automatic, Assisted or Checklist interaction. Inspect progress and evidence; review candidates before accepting findings. Available controls depend on permissions and configuration.

External attack surface

Discover domains, assets, URLs and exposed services. Collect technology and HTTP metadata, detect potential exposures and monitor changes on configured schedules.

Cloud posture

Connect AWS, Azure and GCP accounts to review resources, misconfigurations and CIS benchmark mappings. Compliance tracking is not a certification.

Findings and reporting

Keep evidence, severity, affected assets and remediation guidance together. Track review, remediation and retesting, map attack chains and generate project PDF reports.

Teams and integrations

Use organization-scoped workspaces for internal teams and providers. Connect workflows through Jira synchronization, the public API and the Galileo CLI.

Capabilities, limits, run profiles and plugins depend on license, permissions and provisioning. A completed assessment can still contain blocked work, incomplete coverage or unverified candidates; it is not a guarantee that an environment is secure.

A pentest finds a path. CTEM closes the loop.

01 Define

Set authorized scope, exclusions and project context.

02 Discover

Build visibility into exposed assets and services.

03 Validate

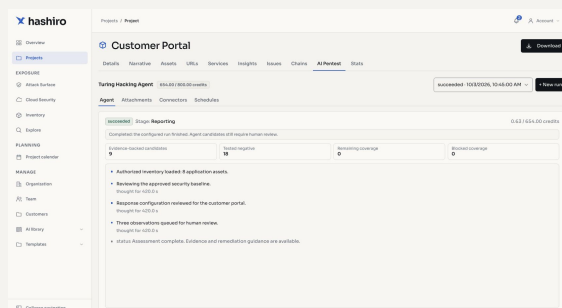
Investigate with AI-led assessments; review the evidence.

04 Remediate

Keep finding status, ownership and guidance connected.

05 Retest

Verify the fix and inform the next assessment.

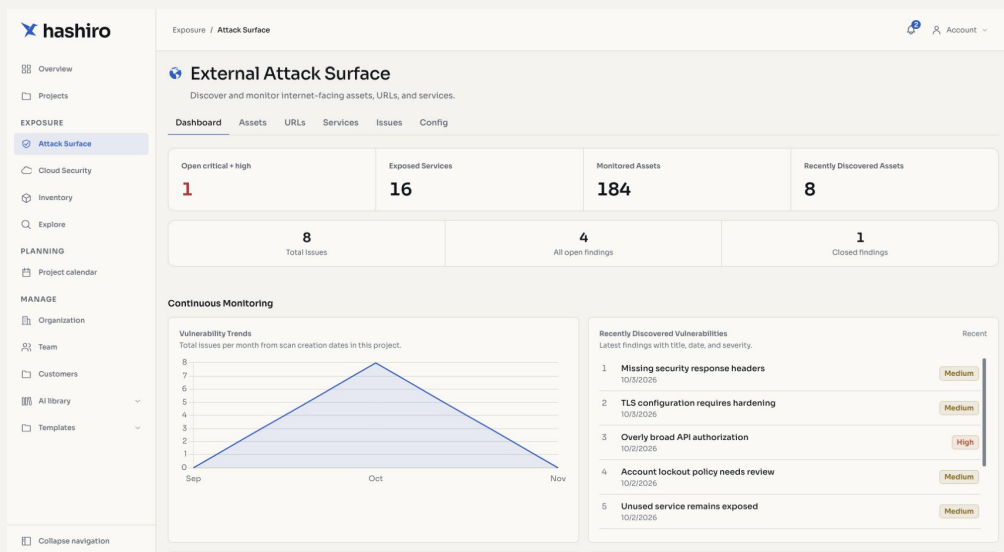


AI assessment workspace: configured runs, progress and results for review.

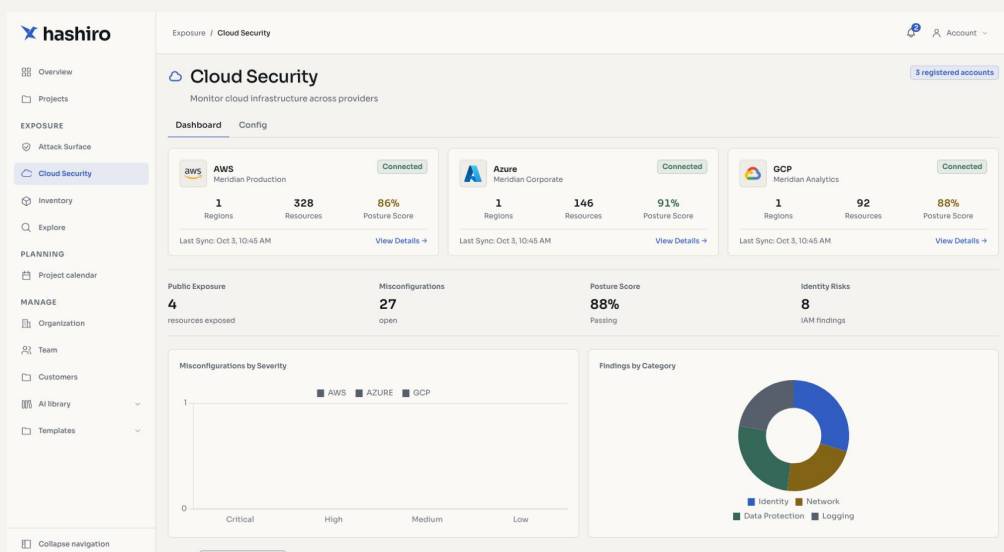
Actual product UI with fictional demonstration data. These images are illustrative, not customer evidence or measured performance. The included captures are in English.

Inside the product

Actual product UI with fictional demonstration data. These images are illustrative, not customer evidence or measured performance. The included captures are in English.



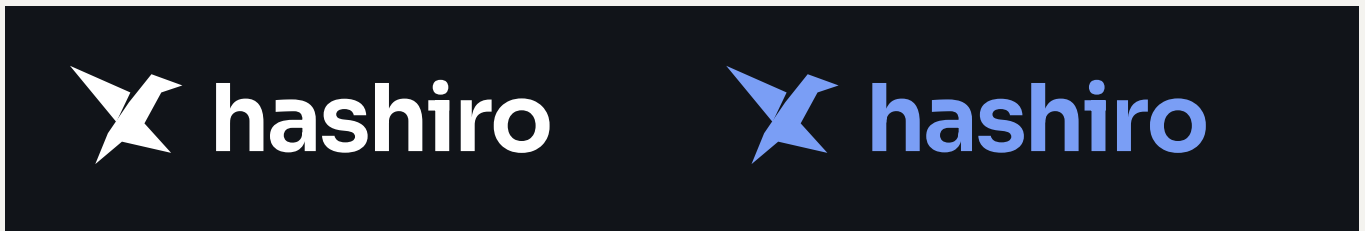
External attack surface: discovered assets, exposed services and monitored findings.



Cloud posture: connected accounts, resources and misconfigurations.

Flight identity

Use the supplied Flight emblem and outlined lowercase wordmark. The product name is Hashiro; lowercase styling belongs to the logo artwork.



Use ink artwork on light backgrounds and white artwork on dark backgrounds. Use blue artwork only where contrast is clear.

Keep the supplied proportions and geometry. Do not redraw the wordmark, stretch, rotate or add effects to the logo.

Packaging guidance: leave at least one quarter of the emblem's height as clear space. Use the full lockup when introducing the brand; use the mark alone where Hashiro is already named.

SVG is preferred for print and scalable layouts. Transparent PNG files are provided for tools that do not accept SVG. White PNG artwork is intentionally invisible on white backgrounds.

Sora is the primary type family; JetBrains Mono is used for technical labels. Included static fonts retain their SIL Open Font License notices.

Keep screenshot captions and the demonstration-data notice with images. Crop only when it does not alter the represented workflow or hide relevant context.

 Flight blue #7A9EF5

 Ink #111419

 Paper #F4F3EF

 White #FFFFFF

 Text blue on light #2C54C2

Copy and contact

Short description

Hashiro is a CTEM platform connecting AI-led pentesting, attack-surface visibility, cloud posture and finding workflows, with human review at the center.

About Hashiro

Hashiro is a Continuous Threat Exposure Management (CTEM) platform with AI-led pentesting at its core. It brings external attack-surface discovery, cloud posture, scoped assessments and vulnerability workflows into a connected workspace. Security teams and providers define authorized boundaries, inspect assessment evidence and review candidate findings before deciding what to act on. Accepted findings retain asset context, severity and remediation guidance through retesting and reporting. Organization-scoped workspaces support internal programs and providers working across customer organizations.

General contact and demo enquiries

hello@hashiro.ai

<https://hashiro.ai>

Describe capabilities, not guaranteed outcomes. Do not add customer logos, testimonials, certification badges, performance statistics, funding history or founder biographies without separately verified approval. No such proof is included in this kit.

Use these materials to describe Hashiro accurately. Brand ownership is unchanged; this kit does not grant a general trademark license or imply endorsement. Contact the team for permissions or uses beyond editorial coverage.