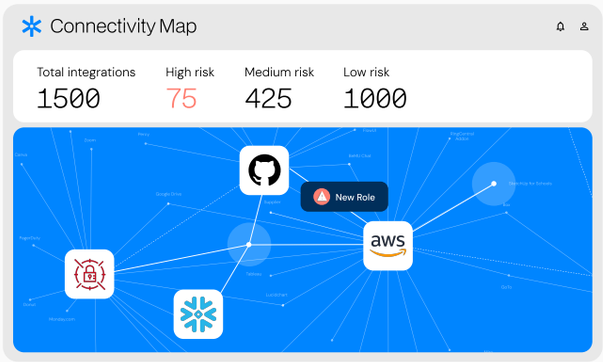
Astrix

Securing Non-Human Identities in AWS

NHIs like IAM users, roles, service accounts, external keys and secrets provide powerful access to resources in your cloud environment. Only Astrix tells you **what** permissions NHIs have, to **which** resources, **who** is behind them, and the **risk** they pose.



Key Benefits

Discover NHIs in real-time

Manage NHI access with continuous inventory of users, roles, service accounts and keys. Map their interconnectivity within your AWS and with external platforms and suppliers. See the owners of each NHI and its usage.

Prioritize NHI risks

Attend to the top 5% risks using threat algorithms based on parameters such as services and resources an NHI can access, permissions, behavioral analysis, and internal or external use.

Easily respond to third-party breaches

Expedite IR efforts when a supplier is breached. Map every associated NHI, and see everything it's connected to so you can remove or rotate in a jiff.

Detect suspicious NHI behavior

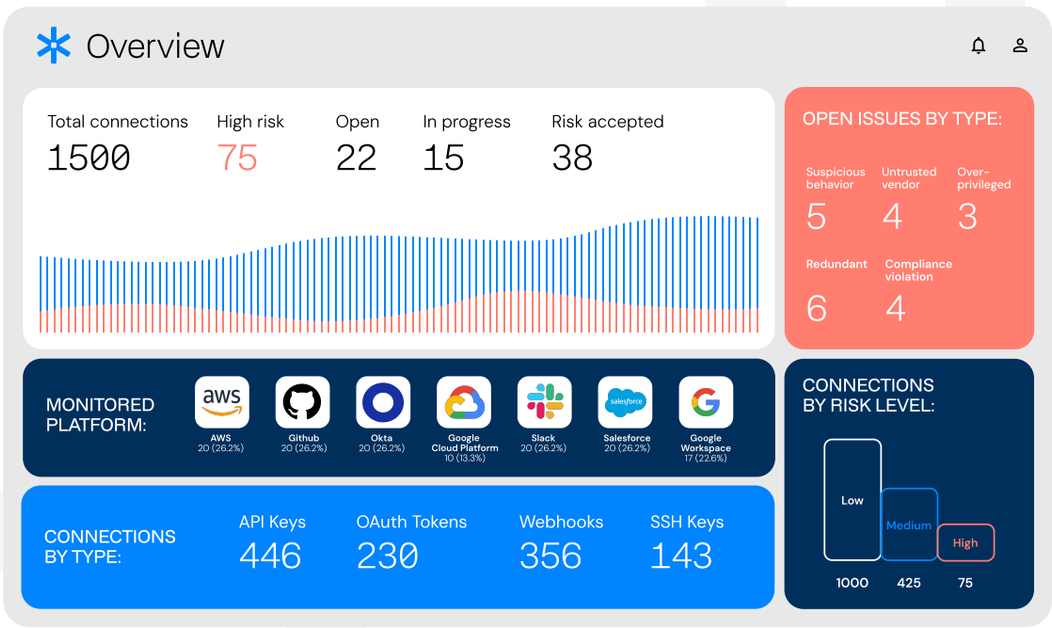
Easily respond to potential attacks with real-time alerts, workflows, and investigation guides on anomalous NHI activity such as unusual user agent, geo, and API activity.

Remediate & automate

Use out-of-the-box policies, custom workflows and context to remediate NHI risks across your environments. Reduce overhead with native SIEM, SOAR and ITSM integrations.

Protect your secrets

Map all your exposed secrets across cloud environments. Prioritize their risk and easily rotate or revoke using rich context.



Key Capabilities

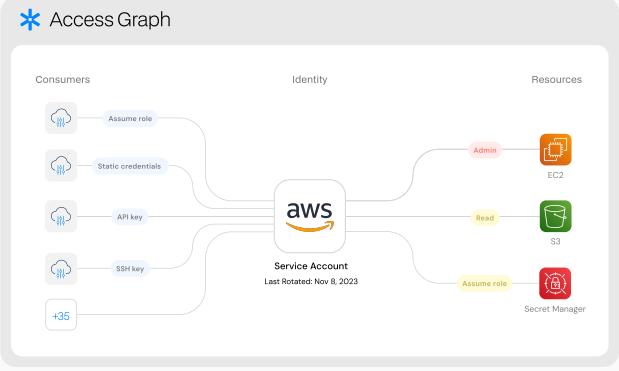
VISIBILITY & POSTURE

Real-time discovery

Get a continuous inventory of provisioned or in-use service accounts, roles, entitlements and keys. Complete the picture with the owners, usage or third-party suppliers behind them.

Actionable risk modeling

Prioritize risk with context into the services & resources an NHI can access (API Gateway, S3, secret managers), the permissions it has (full access, read, add), and internal or external use.



NHI ownership

Streamline remediation and verification by easily assigning ownership for each NHI to their human owners and, if external, the third-party supplier.

NHI usage & redundancy

Usage analysis and holistic visibility across environments helps you easily understand if an NHI is used, what it's connected to, and how to rotate or remove it without breaking anything.

Supply chain breach likelihood

Astrix's likelihood engine rates suppliers according to their reputation, configuration, maintenance and anomaly detection - highlighting the ones most likely to get breached.

Next-gen secret scanning

Map all your exposed secrets across cloud & SaaS environments. Prioritize their risk and easily rotate or revoke using context into secret permissions, in-use services, owner, cross-environment connectivity, and rotation policy.

ITDR & REMEDIATION

Behavioral threat detection

Get alerted on potential breaches in real time. AI-based threat engines detect abuse of NHIs based on parameters such as unusual IP, user agent and API activity.

Threat mitigation

Quickly respond to potential breaches using anomaly investigation guides and activity logs, outlining the anomaly and the baseline along with suggested response steps.

Automatic end-user communication

Remediate faster with end-user feedback. Automatically gather business justification from users behind NHIs so you can remove risky access without interfering with business processes.

Integrations with existing tech stack

Maintain productivity by integrating Astrix with your existing security stack. Get a Slack notification, automatically open Jira tickets, use API automations or work with your SIEM.