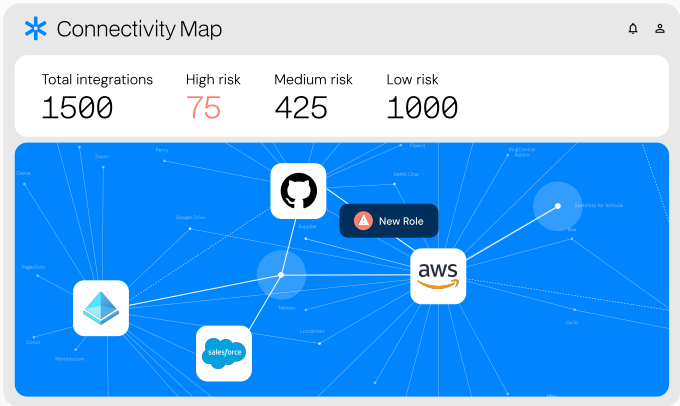




Securing Non-Human Identities

Secure, manage, and govern non-human identities across IaaS, SaaS, PaaS, and on-prem environments.



Key Benefits

Discover NHIs in real-time

Get a continuous inventory of service accounts, OAuth apps, IAM roles, and API keys. Map their interconnectivity within your environments, external apps, and suppliers.

Prioritize NHI risks

Focus on the top 5% of risks using threat algorithms that analyze services and resources accessed, permissions, behavioral patterns, and internal/external use.

Manage NHI lifecycle

Enable policy-based attestation, alerts, and offboarding from creation through permission changes, rotation events, revocations, and expirations.

Quickly respond to vendor breaches

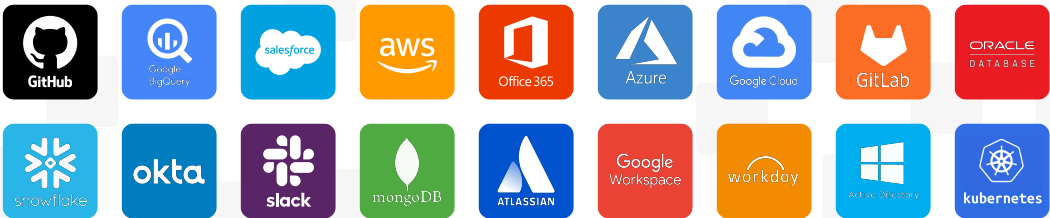
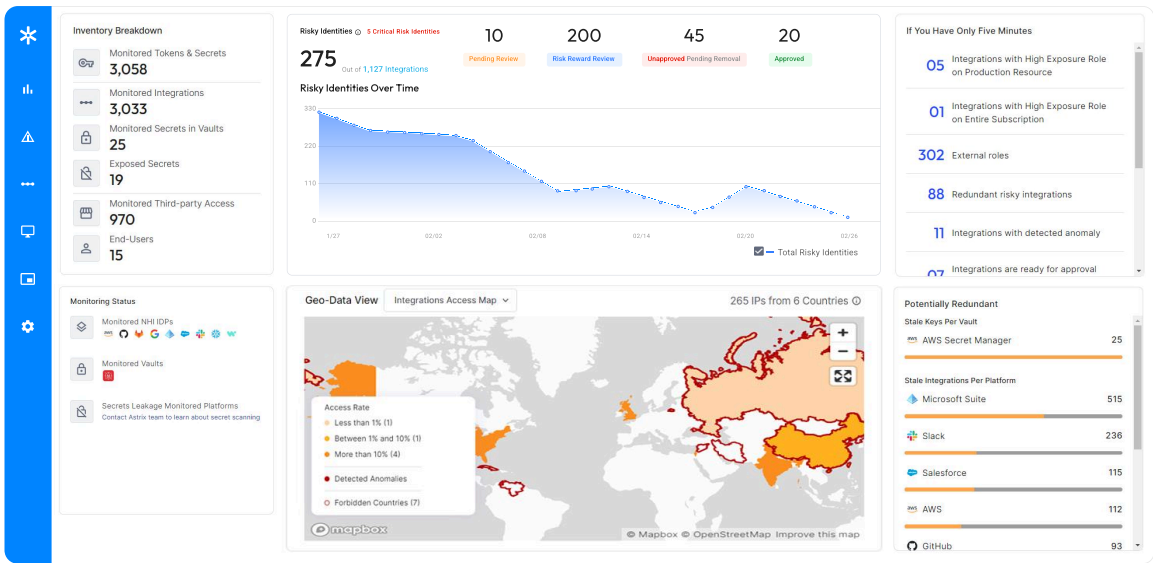
Expedite IR efforts when a vendor is breached. Map every associated NHI, and see everything it's connected to so you can remove or rotate in a jiff.

Detect suspicious NHI behavior

Respond to potential attacks with real-time alerts, workflows, and investigation guides on anomalous activities like unusual user agents, 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.



Key Capabilities


VISIBILITY & POSTURE

Real-time discovery











Get a continuous inventory of provisioned or in-use service accounts, secrets, OAuth apps, IAM roles, API keys and other NHIs. Complete the picture with the owners, third-party vendors behind them and usage.

NHI ownership & offboarding

Assign ownership of each NHI to its respective human owners and users for streamlined remediation and verification. During employee offboarding, quickly identify all related NHIs, their connections and uses, and confidently rotate or remove them.



Non-human Identity Risks

ConnectionName	Environment	NHIType	Risk	PermissionSensitivity	Last Used	Owner
<input type="checkbox"/> Appbot	 Slack	Webhook	High	Medium Show Permissions	04/07/2024	 Lena David
<input type="checkbox"/> Databricks	 AWS	Role	Critical	High Show Permissions	21/06/2024	 Kate Bergman
<input type="checkbox"/> Acrobat Reader	 Azure AD	Service Principal	High	Medium Show Permissions	19/05/2024	 Jeffery Lutton
<input type="checkbox"/> Test token	 GitLab	Access Token	Critical	High Show Permissions	10/05/2024	 Bob Adams
<input type="checkbox"/> CircleCI Backend	 GitHub	Deploy Key	Medium	Low Show Permissions	27/04/2024	 Linda Davis

NHI usage & redundancy

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

Actionable risk scoring

Prioritize remediation efforts through rich context about services and resources an NHI can access (Google Drive, S3, Git repos, Slack channels), its permissions (full access, read, add), usage, and its consumers (internal users and third-party vendors).

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 be breached.

Next-gen secret scanning

Map all your exposed secrets across secret managers and cloud environments. Prioritize their risk and easily rotate or revoke with context into which service the secret is used for, its permissions, owner, and rotation policy.

ITDR & REMEDIATION

Behavioral threat detection

AI-based threat engines detect abuse of NHIs based on anomaly indicators such as unusual IP, user agent, and API activity. Detailed investigation guides and activity logs help you respond swiftly.

Out-of-the-box remediation

Remediate with a click of a button using out-of-the-box policies for posture and incidents. Easily build custom workflows to fit your security needs.

End-user communication & remediation

Remediate faster with end-user feedback and self-remediation. Automatically gather business justification from users behind NHIs and allow them to remove risky access themselves, without interfering with business processes.

Enterprise integrations

Integrate Astrix with your existing security stack to reduce overhead. Use Slack notifications, automatically open Jira tickets, use API automations, or work with your ITSM, SIEM and SOAR systems.

Policy deviations

Prevent NHI abuse by enforcing organizational policies on NHIs. Use your existing tools to mitigate policy deviations such as access from forbidden geos, number of API calls and more.

Vendor supply chain attacks

Drastically expedite incident response when one of your vendors is compromised. Map every associated NHI, see everything it's connected to and what it's used for to quickly rotate or remove without breaking business processes.

