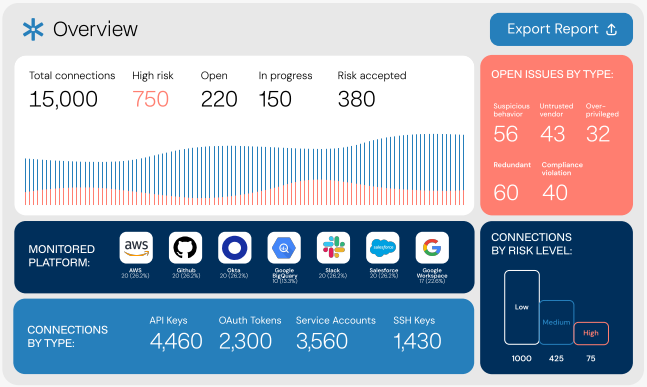
Astrix

NHI Security & Governance for Financial Services

Ensure Continuous Compliance with PCI DSS

Non-human identities (NHIs), including service accounts, API keys, and OAuth applications, now outnumber human users 45:1, creating a rapidly growing security blind spot in financial services. Just as compliance requirements become more demanding, NHIs become prime targets for exploitation without the proper visibility and control.

Astrix Security gives financial companies full control over NHIs, automating threat detection and response, mitigating third-party risks, and ensuring continuous compliance with regulation frameworks like PCI DSS.



Key Benefits

Discover unknown unknowns

You can't govern what you can't see (or understand). Get your team the NHI visibility and context they need across all your environments.

Control & reduce risk

Nothing feels better than removing redundant attack surfaces and controlling risk. Astrix automates both and allows you to manage risk using your existing security frameworks.

Ensure continuous compliance

Security frameworks and regulations constantly evolve. Astrix continuously maps and updates your compliance posture to frameworks like PCI DSS, NIST, and OWASP NHI Top 10.

How Fintech Companies use Astrix to secure NHIs

"Astrix strengthens our identity security program by providing us with continuous visibility and governance over thousands of NHIs."

PAGAYA

Yaniv Toledano
CISO
Pagaya | Fintech

"Astrix democratizes security by allowing end users to explain why a tool can access our environment, which is crucial for security teams."

MERCURY

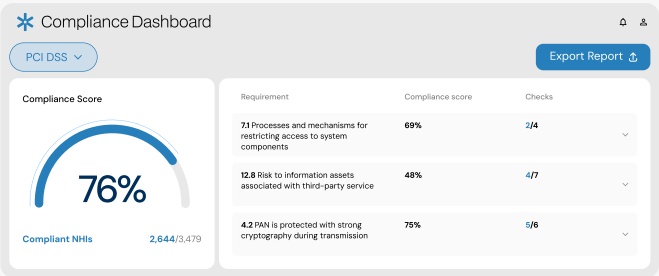
Branden Wagner
CISO
Mercury | Digital Bank

Key Product Capabilities

VISIBILITY & RISK MANAGEMENT

Reduce your attack surface

Gain continuous visibility and control of service accounts, API keys, OAuth apps, and IAM roles. Prioritize risk based on usage context, owners, permissions, and third-party consumers.



Control third-party risk

Map all vendor access, enforce the least privilege principle, and zero trust for third-party NHIs. Get alerted on compliance and policy deviations.

Proactively respond to threats

Respond to anomalous NHI behavior, third-party breaches, and policy deviations with near real-time alerts, workflows, and playbooks.

Align with industry frameworks and compliance regulations

Map NHI risk to industry frameworks like PCI-DSS, NIST, and OWASP NHI Top 10. Continuously assess and update compliance posture across environments.

OWNERSHIP, POLICY & SECRET MANAGEMENT

Streamline ownership and policy-based attestation

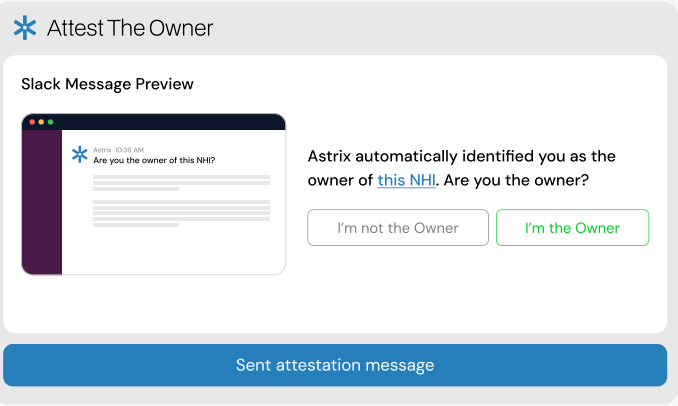
Assign clear ownership of NHIs to individuals and enforce policy-based attestation to enhance accountability, streamline remediation, and ensure compliance with security policies.

Centrally manage secrets

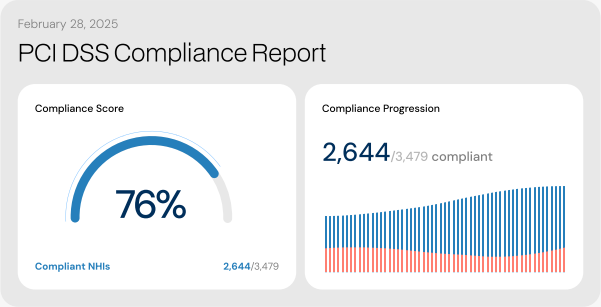
Automate secret rotation, retrieval, and access monitoring to meet compliance requirements and reduce risk across secret managers and vaults.

Safely decommission NHIs

Automate the offboarding of NHIs when employees depart or a vendor is no longer used.



REPORTING & REMEDIATION



Compliance-ready reporting

Generate audit-ready reports tailored to frameworks such as PCI DSS, SOX, ISO and OWASP NHI Top 10. Provide stakeholders with key insights into NHI access, permissions, and activity.

Enterprise integrations

Seamlessly integrate with ITSM, GRC and ticketing platforms to enrich compliance workflows and automate ticket creation and notifications for compliance violations.x