Everyday Identity

Trust Nothing. Verify Everything. Protect Everyone.

NHI Security Health Check – 2025

Discovery & Classification

- [ ] Have all NHIs (service accounts, bots, API keys, etc.) been discovered and inventoried?
- [ ] Are all NHIs tagged with Owner, Use Case, Risk Tier, and Expiration Date?
- [ ] Is this metadata integrated with a CMDB or identity directory?

Federation & Secrets Management

- [ ] Are federated identities used for cloud workloads and CI/CD (e.g., OIDC, IAM roles)?
- [ ] Are secrets centrally managed in a secure vault?
- [ ] Are static secrets rotated at least every 90 days and monitored for usage?

Lifecycle Management

- [ ] Do NHIs follow a Join-Move-Leave lifecycle with automated provisioning and deprovisioning?
- [ ] Are NHIs deactivated or rotated when their related services are retired or updated?
- [ ] Are service account creation requests gated by an approval or ticketing process?

Access Governance

- [ ] Are NHIs assigned least-privilege access using RBAC or ABAC?
- [ ] Are environments (e.g., dev, stage, prod) segmented and scoped for NHI permissions?
- [ ] Are Conditional Access policies used to limit high-risk NHI activity?

Identity Reviews

- [ ] Are NHIs included in quarterly access certifications?
- [ ] Is ownership and access scope revalidated each quarter?
- [ ] Are unused or orphaned NHIs deactivated or rotated?

Access Governance

- [ ] Are NHIs assigned least-privilege access using RBAC or ABAC?
- [ ] Are environments (e.g., dev, stage, prod) segmented and scoped for NHI permissions?
- [ ] Are Conditional Access policies used to limit high-risk NHI activity?

Monitoring & Alerts

- [ ] Is NHI behavior monitored in real time using SIEM or CSPM tools?
- [ ] Are logs retained and audited for all NHI activity?
- [ ] Are alerts configured for NHI anomalies (e.g., off-hours access, privilege escalation)?

- Tag 100% of NHI inventory with ownership metadata
- >95% of NHIs reviewed quarterly
- 70%+ of NHIs federated (vs static credentials)
- Orphaned identities identified and removed regularly

Quick Tip:

Aim for 90%+ compliance across all categories to dramatically lower your identity-related security risk.