okta

Securing Non-Human Identities with Okta

Today's enterprises rely on a rapidly growing network of non-human identities (NHIs)—service accounts, bots, tokens, and AI agents—that now outnumber humans 50 to 1. These identities often operate with excessive, persistent access. They typically lack built-in security controls and are deeply embedded across all environments. Without visibility or governance, NHIs create an invisible but extensive attack surface—a silent threat that evades traditional Identity management. This enables unauthorized changes, uncontrolled access, and security gaps across critical systems and workflows.

Okta brings NHIs into the same unified identity framework as human identities, providing visibility, access control, governance, and remediation across all environments. This end-to-end approach eliminates silos and ensures every identity is managed and secured with confidence.

Reveal hidden identity risks before they become threats

NHIs are one of the biggest blind spots in enterprise security. Okta brings them into focus—revealing service accounts, tokens, and AI agents that often go unmanaged. **Identity Security Posture Management (ISPM)** delivers unified insight across all identities, surfacing risks like unrotated credentials, excessive access, and orphaned accounts. ISPM continuously discovers and classifies NHIs across environments—helping teams proactively detect threats early and reduce exposure.

Enforce precision access to limit your attack surface

Reducing risk starts with limiting access—making it time-bound and aligned to actual need. **Okta Privileged Access (OPA)** secures credentials, rotates secrets, and audits privileged actions to ensure NHIs never retain standing access. **Secure Identity Integrations (SIIs)** extend these controls into top SaaS apps like Google Workspace, Microsoft 365, and Salesforce—ensuring NHIs only access what they need, when they need it.

Scale and stay compliant without the overhead

Okta helps teams scale securely without sacrificing compliance—automating provisioning, deprovisioning, and policy enforcement through pre-build governance workflows. These workflows help reduce overhead and ensure ongoing alignment with security policies. They're easy to adopt through the **Okta Integration Network (OIN),** which provides pre-built integrations that accelerate deployment and simplify non-human identity management across the enterprise.

By unifying visibility, access control, and governance, Okta transforms a fragmented and high-risk identity landscape into a secure, manageable part of the enterprise identity strategy. This approach enables organizations to reduce complexity, maintain least privilege, and scale securely—without compromising compliance or operational efficiency.

Key benefits

End-to-End Visibility
Discover and monitor all non-human identities across environments.

Least Privilege Access
Enforce time-bound, need-based access to reduce exposure.

Automated Lifecycle Management
Provision, deprovision, and govern NHIs at scale.

Unified Identity Framework
Manage all identities—human and non-human —through one secure system.

Unmanaged service accounts and overprivileged API keys are top attack vectors.

- 2025 OWASP Top 10 Non-Human Identity Risks

Learn how ISPM and OPA bring NHIs under control