Silverfort

Cloud Non-Human Identity (NHI) Security

Discover, monitor, and secure every cloud-based non-human identity

The Challenge

Cloud NHIs: A growing blind spot in identity security

As cloud environments expand, so does the number of non-human identities—service accounts, API keys, tokens, and more. These identities are often created by different teams, over-permissioned, unmanaged, have poor security controls, and are invisible to existing tools.

Without visibility and governance, cloud NHIs become one of the largest and most unaddressed attack surfaces in modern environments. Organizations face mounting challenges:

- → Limited visibility and inability to detect the full range of NHIs operating across cloud environments.
- → Misconfigurations resulting in over-permissive access to NHIs, particularly for third parties, which increases exposure and risk.
- → Static, long-lived credentials, with rotation occurring infrequently—typically only once per year, if at all.
- → No clear ownership or governance, leaving NHIs overprivileged at creation or dormant and unmanaged when no longer in us

Silverfort's NHI Security: Full coverage of cloud NHIs

Discover and classify different types of non-human identities across identity providers such as **Okta** and **Entra**, cloud infrastructure platforms including **AWS**, **Azure**, and **GCP**, and SaaS applications like **Salesforce**, **Slack**, **GitHub**, **Atlassian**, and more.

Gain complete visibility into effective privileges across your entire NHI inventory to reduce unnecessary permissions and strengthen security.

Prioritize and remediate the most critical NHI exposures by identifying account ownership and applying actionable recommendations to minimize your attack surface and close compliance and lifecycle gaps across your environment.

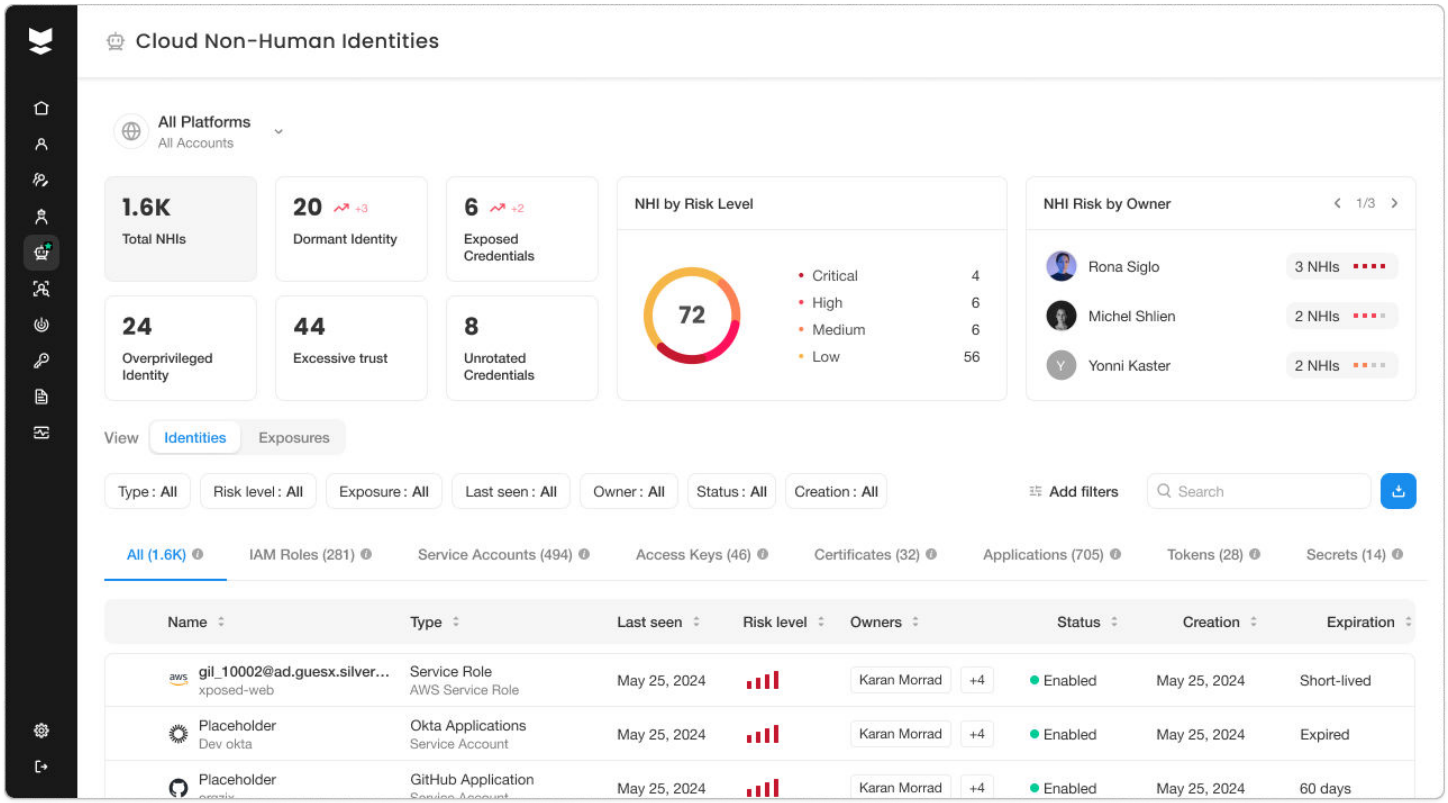
How it works

Seamlessly integrate Silverfort with your cloud IdPs, infrastructure, and SaaS applications in just minutes. Once integrated, Silverfort continuously analyzes cloud configurations and activity logs to automatically discover and classify all NHIs across your environment.

Each NHI is enriched with detailed metadata, such as important timestamps like creation or last seen dates, assigned permissions and credentials, privilege level, and ownership, and is visualized in an interactive graph to support deep-dive investigations.

By correlating configuration and usage data, Silverfort identifies and prioritizes exposures like excessive or unused permissions and dormant accounts. You receive actionable, context-aware remediation guidance tailored to each exposure. You can also initiate ticketing workflows directly from the platform, pre-filled with relevant identity data to accelerate response and reduce manual effort.

The result: End-to-end visibility, faster decision-making, and stronger security for every NHI in your cloud ecosystem.



About Silverfort

Silverfort secures every dimension of identity—humans or machines across the cloud and on-prem. We deliver end-to-end identity security that is easy to deploy and won't disrupt business operations, resulting in better security outcomes with less work. Discover every identity, analyze exposures, and enforce protection inline to stop lateral movement, ransomware, and other identity threats.