



Protect Cloud NHIs at scale with Geofencing

Geofencing is an access control that restricts where an identity can be used, allowing organizations to define the locations (such as an IP address, IP range, or geographic region) from which a credential is expected to authenticate, and block access from everywhere else.

This capability is particularly effective for non-human identities, which behave more predictably than human users. That predictability turns location into a meaningful security control: if attackers compromise a credential, geofencing can prevent them from using it outside its approved environment. The credential itself may still be valid, but it is nearly useless to an attacker operating from a different location.



Silverfort's Geofencing for NHIs

Supported platforms: *Entra ID, AWS*

Silverfort's geofencing capability restricts cloud non-human identities from being used outside their legitimate locations. Silverfort is the automation layer that identifies which identities are fenceable, builds the policy for each one, and deploys it at scale to run natively in the IdP.

The capability builds a behavioral of each NHI over a minimum of 30 days of observed activity, identifies the IP addresses it originates from, and auto-suggests a geofencing policy based on that location-behavior. Once approved, Silverfort pushes the policy into the identity provider for enforcement, where any authentication attempt from outside the baseline addresses is denied.

**Enforcement in Entra ID requires Microsoft's Workload ID Premium license.*

How it works



Observe: Silverfort builds a baseline of each NHI over a minimum of 30 days of observed activity.



Suggest: Silverfort identifies the IP addresses each identity originates from and auto-suggests a fencing policy based on its location based behavior.



Enforce: Approved policies are pushed into the IdP, denying any authentication from outside the legitimate addresses.



Inside the Platform

The screenshot displays the Silverfort platform interface. On the left is a sidebar with a list of cloud NHI instances, including 'rg-agent-nc-...AgentIdentity Glitch', 'Lab Agent Instance 1 Glitch', 'Okta Microsoft Graph Client XPosed AzureAD', 'RezonRoRole Sandbox', 'RezonRoRole Log Archive', 'RezonRoRole Audit', 'Quality Evalu...opilot Studio) XPosed AzureAD', and 'Customer Ser...pilot Studio) XPosed AzureAD'. The main panel shows a detailed view for a selected instance, with tabs for 'Summary', 'Remediation', and 'Changelog'. The 'Remediation' tab is active, showing 'Quick actions' such as 'Apply geofencing policy' (which instantly restricts the workload identity to its historical source IP addresses) and 'Remediation guidelines' for applying an 'Entra workload identity geofencing policy'. The guidelines include instructions on how to use the option to validate the geofence before enforcing it.

While the actual enforcement resides with the cloud provider, the intelligence that makes it usable comes from Silverfort's observed access patterns.

This setup is what makes it highly scalable across all platforms at once. Instead of hunting through logs one identity at a time, Identity Security teams get hundreds of ready-made, per-identity policies at once.

Key benefits



Immediate risk reduction

Cloud NHIs can only authenticate from their known locations. Any deviation is blocked by the IdP, at the moment of authentication, before damage is done. Whether the attacker is human or AI, a leaked or stolen credential remains unusable outside the identity's approved locations.



Protection at scale

Manually building fencing policies identity-by-identity doesn't scale across hundreds of NHIs and multiple platforms, and it's not an efficient use of time. Silverfort's auto-suggested policies get you full coverage in a fraction of the time, without the manual effort.



Predictable and effective control

Nearly 75% of cloud NHIs resolve to 25 addresses or fewer, and 20% to a single address. This predictable behavior allows a high level of certainty about where legitimate access originates.



Workflows keep moving

Since each suggested policy is derived from a behavioral baseline before it's applied, it allows your team a high level of certainty for each NHI's actual behavior, while taking your existing IdP policies into account to avoid misalignment.

About Silverfort

Silverfort secures every dimension of identity—human, machine, and AI—across on-prem, cloud, and hybrid environments. We are the first to deliver an end-to-end Identity Security platform that is easy to deploy and won't disrupt business operations, resulting in better security outcomes with less work. Discover every identity across every environment, analyze exposures to reduce your attack surface, and enforce security controls inline and at runtime to stop lateral movement, ransomware, and other identity threats.