Silverfort

Silverfort's Visibility and Observability

Gain unified visibility and observability into all identities, including human, non-human and AI agents, across on-prem and cloud environments

The Challenge: **Gaps in identity observability create blind spots in hybrid environments**

Most organizations can't fully protect and govern identities they cannot see. With today's complex hybrid environments, spanning on-prem, cloud, SaaS applications, and cloud infrastructure, visibility gaps extend across human, non-human and AI agent identities. Tools that fail to integrate lead to fragmented insights, while static reports fall short of showing how access is granted and used, and where exposures lie. These blind spots create coverage gaps across hybrid environments, leaving organizations unable to enforce the least privilege, maintain compliance, or detect anomalous behavior before attackers exploit it.

Without unified visibility and observability, organizations face persistent challenges:

- → Tool sprawl results in siloed solutions that increase complexity, waste spend and deliver inconsistent results
- → Lack of unified view of all identities, including their access, activity, relationships, and risk context across hybrid environments
- → Difficulty in linking granted permissions to actual usage or risk, making it hard to enforce least privilege
- → Fragmented governance that leaves critical gaps between detection, investigation, and enforcement
- → Inability to track or measure identity security posture improvements or demonstrate compliance readiness over time

Silverfort Visibility and Observability: Uncover blind spots across all identities

Discover and contextualize every identity.
Automatically identify human, non-human, and AI agent identities across AD, cloud IdPs, SaaS apps, and cloud infrastructure, and classify them with rich context on ownership, access, and behavior

Map access and activity with precision.
Uncover hidden risks, misconfigurations and excessive privileges with deep context, including role, activity patterns and authentication behavior

Correlate activity to risk.
Link every action to its true origin and build a complete timeline of identity behavior. Provide enriched data that accelerates root-cause investigations, simplifies compliance reporting, and supports proactive remediation

How it works

Silverfort connects directly to your AD, cloud IdPs, SaaS platforms, and cloud infrastructure systems to consolidate identity data across your environment. From deployment, it continuously discovers and enriches every identity, including human, non-human, and AI agents, building a unified real-time view.

Step 1: Discover access lineage and ownership

Continuously trace assigned, inherited, and nested permissions, and enrich each identity with lifecycle details such as account creator, responsible owner, creation date, and last seen activity.

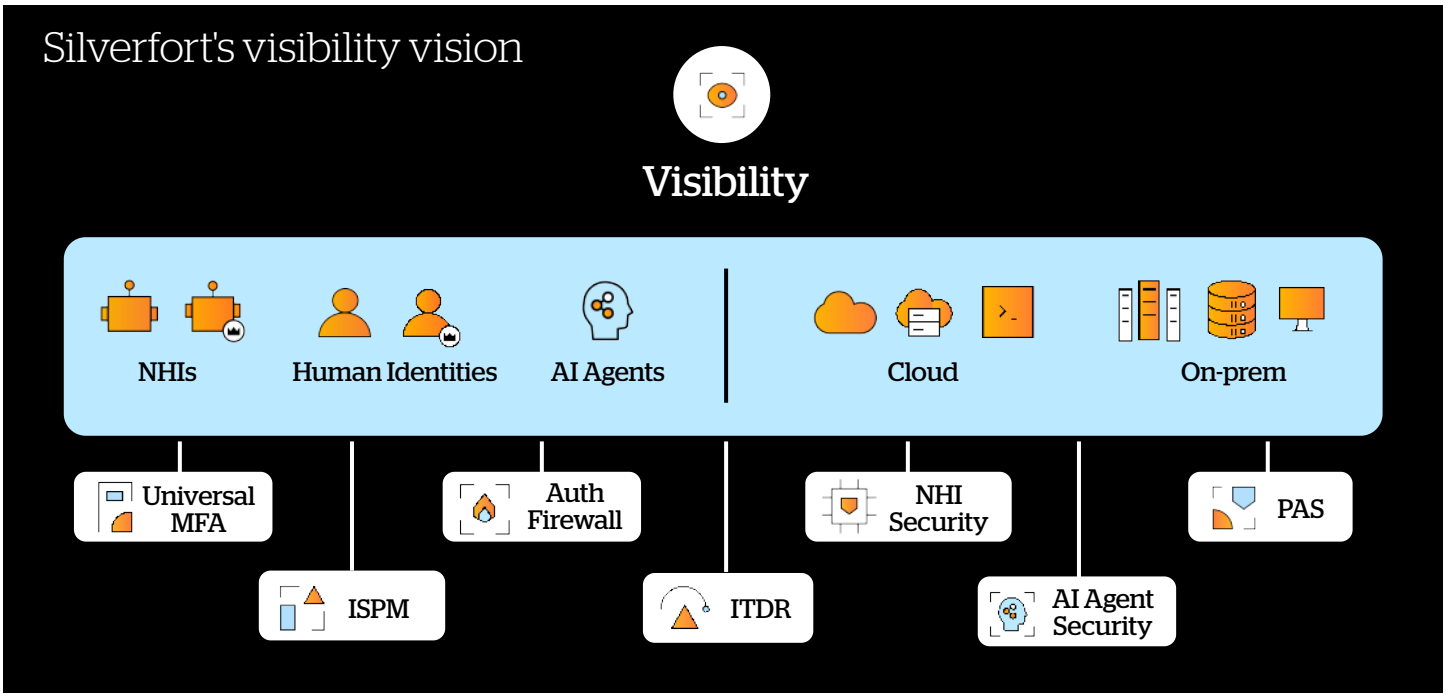
Step 2: Monitor activity and behavior patterns

Track authentication flows, anomalies, and risk signals to understand how identities behave in practice, and to detect suspicious activity.

Step 3: Map relationships across on-prem and cloud environments

Link accounts, entitlements, and access paths across on-prem and cloud environments to expose hidden misconfigurations and potential attack paths.

The result: Organizations achieve real-time visibility and observability of all identities. With enriched context and activity insights, organizations can accelerate investigations, demonstrate compliance, and proactively reduce identity-driven risk.



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.