Silverfort

Access Intelligence

Gain dynamic contextual intelligence to control identity access and enforce governance without rearchitecting your identity stack.

The Challenge: Excessive Access Without Real-Time Insight

Organizations can't defend what they can't see and right now they can't see effective access across hybrid environments. Access risk is hiding in nested inherited permissions that span on-prem and cloud systems. IGA tools are slow to deploy and often fail to deliver real-time, actionable insights. Reviews are time-stamped due to lack of visibility into what access does.

Teams want context, not more infrastructure to understand and reduce privilege sprawl. Today's identity tools show group membership, not what users can do. This leaves organizations with excessive access, inconsistent enforcement, and major blind spots making Zero Trust and compliance initiatives harder to execute.

Without the ability to understand and control identity access with real-time insights, organizations face ongoing governance gaps and enforcement challenges:

- No visibility into effective access across hybrid environments makes it challenging to see how permissions are granted and used.
- Outdated group-based models and static reports fail to capture how privileges drift over time, often resulting in excessive access and hidden inheritance across real-world access paths.
- Overwhelming entitlement sprawl leads to confusion and inability to prioritize risk or enforce meaningful controls.
- Blind access reviews are time-stamped, leaving teams without context on user access usage to make informed decisions.

Silverfort's Access Intelligence: Full Coverage of Identity Access

Map end-to-end access paths across cloud and on-prem environments for both human and non-human identities. Visualize not just provisioned entitlements, but inherited, effective, and used access.

Surface risks with real usage signals by correlating activity and context to pinpoint where excess access truly exists. Replace assumptions with actionable intelligence for enforcement and governance.

Drive strategic governance through proactive reviews and cleanup workflows from a unified intelligence layer. Deliver board-level risk reporting, audit readiness, and maturity tracking in one interface.

How it works

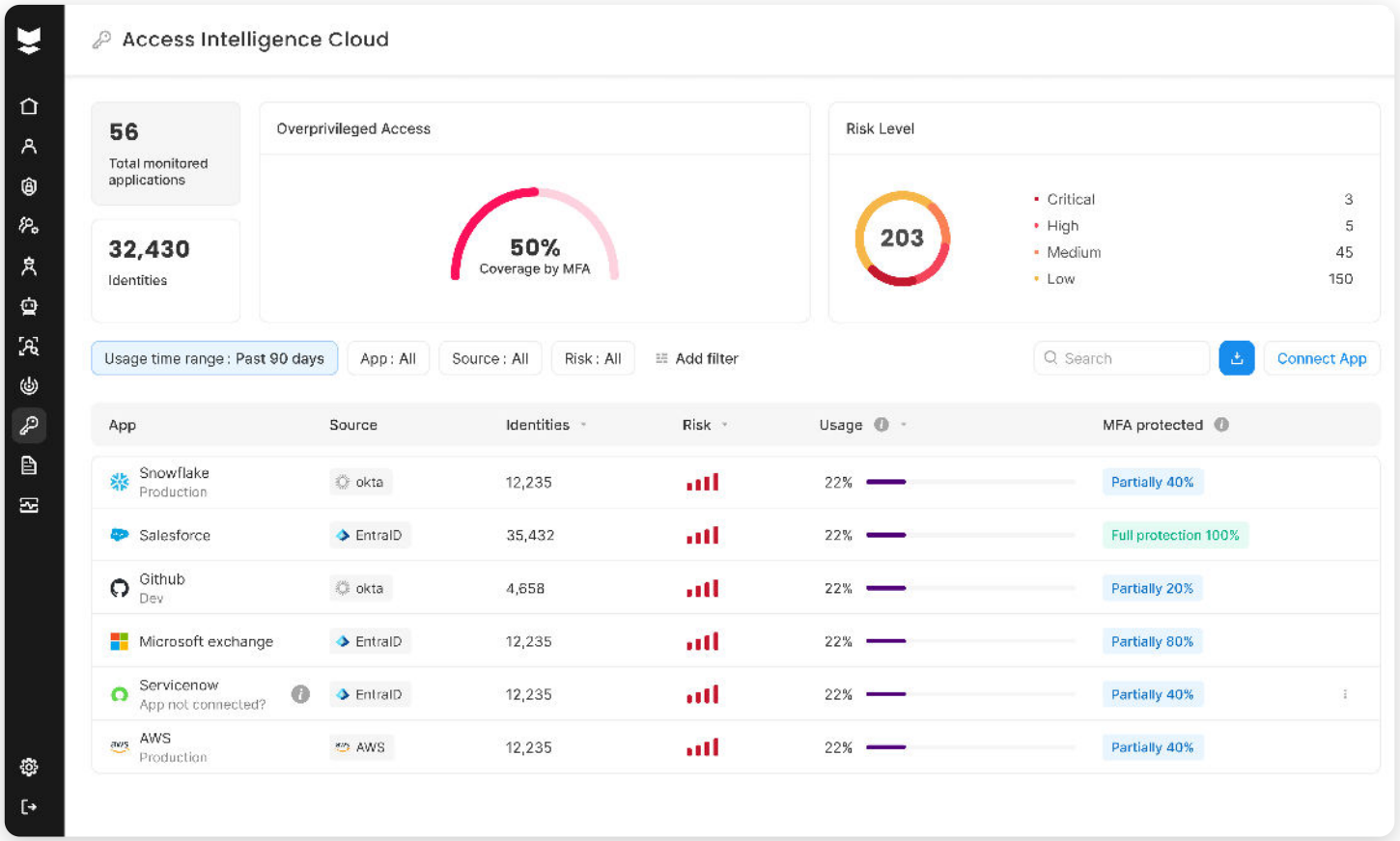
Silverfort connects natively to IdPs, cloud platforms, and SaaS environments with a SaaS-only deployment with no agents or code changes.

Step 1: Visualize how access is granted, inherited, and used across cloud and on-prem environments. Visibility full identity-to-application paths and see assigned vs. effective privileges.

Step 2: Correlate real usage with risk signals to discover unused, excessive, or risky access while detecting hidden exposures from indirect or inherited entitlements.

Step 3: Enable reviews, cleanup workflows, and automated governance from one interface. Support audits, board-level risk reporting, and maturity tracking with continuous intelligence.

The result: Organizations gain the clarity to understand who has access, how they got it, and why being used. With this intelligence, teams can enforce Zero Trust with confidence, remediate faster, and govern smarter.



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.