Silverfort

Identity Security Posture Management (ISPM)

Gain a unified view of identity exposures across cloud and on-prem environments with prioritized risks, actionable context, and built-in controls to remediate at scale

The Challenge: Lack of Unified Visibility into Identity Risks

Organizations are flooded with identity data yet lack a unified understanding of their security risks across on-prem and cloud environments. Traditional tools highlight exposures like excessive privileges and misconfigurations, yet fail to explain risk, guide remediation, or show what matters most.

Posture insights remain fragmented, leaving teams unsure how to prioritize or validate controls. Without this clarity, identity risks go unaddressed and create dangerous blind spots, exposing organizations to credential compromise, lateral movement, and failed audits.

Without centralized visibility into identity posture, organizations face persistent challenges in detecting and managing exposures:

- No unified visibility into identity posture across different platform cloud and on-prem environments
- In the cloud, identities are fragmented across cloud platforms creating siloed insights that undermine control over the full identity landscape
- Inability to measure, report, or improve identity security posture over time
- Lack of clear guidance on how to reduce identity risk or enforce least privilege at scale
- Hard to prioritize what to fix or in what order, complicating efforts to address the most critical identity risks.

Silverfort ISPM: Detect, prioritize, and remediate all identity risks

Gain centralized visibility into your identity attack surface across on-prem and cloud environments to continuously uncover exposures to close posture gaps across hybrid environments.

Understand which identity exposures matter most with risk scores based on severity level, MITRE-mapped context, and explainable risk storylines, enabling for smarter, faster identity threat mitigation.

Remediate identity risks with built-in guidance and automated controls from enforcing MFA and deny policies to removing excessive privileges and streamlining workflows through SIEM and log integrations for audit readiness and compliance requirements.

How it works

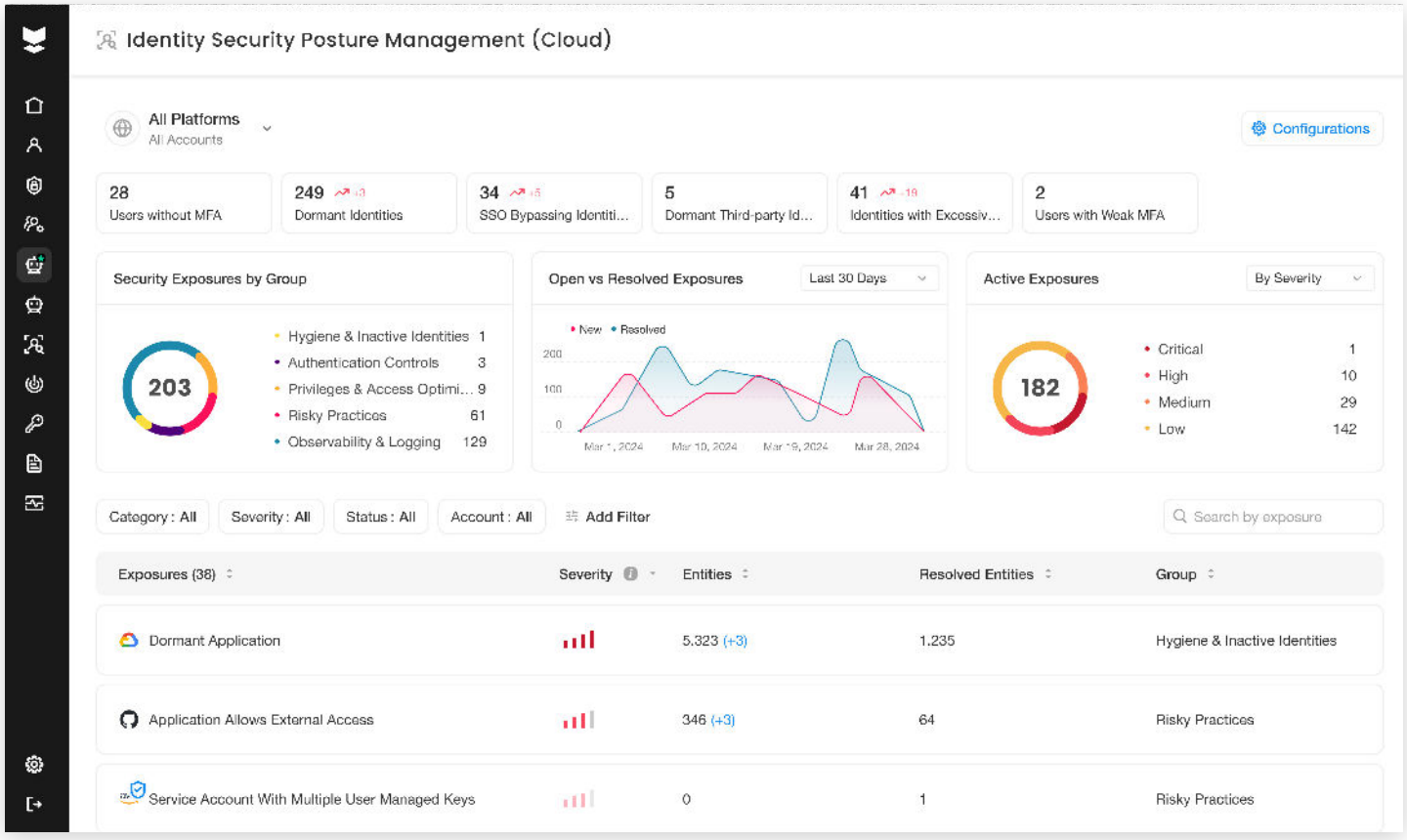
The moment Silverfort is deployed, it continuously detects and monitors all accounts across Active Directory, cloud IdPs, SaaS apps, and cloud infrastructures, providing real-time visibility into activity and associated exposures. Silverfort follows a three-step approach to detect exposures, prioritize risks, and remediate across hybrid environments:

Step 1: Discovers and monitors all accounts, human and non-human identities across on-prem and cloud environments, and detects identity exposures across users, access paths, and systems.

Step 2: Detects on potential exposures and assigns severity scores to entities, their authentications, and related exposures. Each exposure is enriched with explainable risk storylines and MITRE context to highlight which issues matter most and guide remediation.

Step 3: Delivers tailored recommendations to enforce MFA, deny risky authentications, and remove excessive entitlements while integrating with SIEM, SOAR, and logging tools for workflows and compliance tracking

The result: Teams gain centralized visibility, actionable risk prioritization, and guided remediation to reduce their identity attack surface. This enables organizations to strengthen posture and meet compliance requirements.



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.