Silverfort

Identity Threat Detection and Response (ITDR)

Detect and stop identity-based attacks across cloud, SaaS, and on-prem environments with real-time insights, actionable context, and automated response from a single platform.

The Challenge: Blind Spots in Detecting Identity-Based Attacks

Modern attacks exploit identity across cloud and on-prem environments, using valid credentials to move undetected between systems. Security teams struggle to correlate identity activity like a session that spans Okta, AWS, and on-prem AD, leaving blind spots in coverage. Most ITDR solutions promise to help but often lack unified visibility across environments.

Without an effective threat detection solution in place, identity-based threats remain undetected, leaving organizations overwhelmed with alert fatigue, exposed to significant operational risks, and vulnerable to failed compliance audits.

Without the ability to detect identity-based risks, organizations face persistent challenges in preventing and responding to attacks:

- Limited visibility into identity activity across cloud, SaaS, and on-prem environments
- Inability to correlate signals across fragmented identity platforms (AD, Entra ID Okta, AWS, GCP) preventing complete detection of identity threats that span environments
- Alert fatigue from disconnected signals leaving SOC teams overwhelmed by noise and unable to identify what truly matters
- Incomplete threat investigations due to lack of end-to-end identity context making it hard to visualize attack paths or respond quickly

Silverfort ITDR: Detect, prioritize, and remediate all identity threats

Gain unified visibility into identity activity across cloud, SaaS, and on-prem environments, including IdPs, directories, and infrastructure, to continuously detect anomalous behaviors and known TTPs in real time.

Detect and investigate threats in real time with behavioral analytics, infrastructure-level signals, and MITRE ATT&CK-aligned context that enrich alerts with explainable details for faster, more confident investigations.

Accelerate SOC efficiency by consolidating hybrid identity telemetry into a single platform, surfacing only high-confidence threats, reducing alert fatigue, and enabling smarter, faster response.

How it works

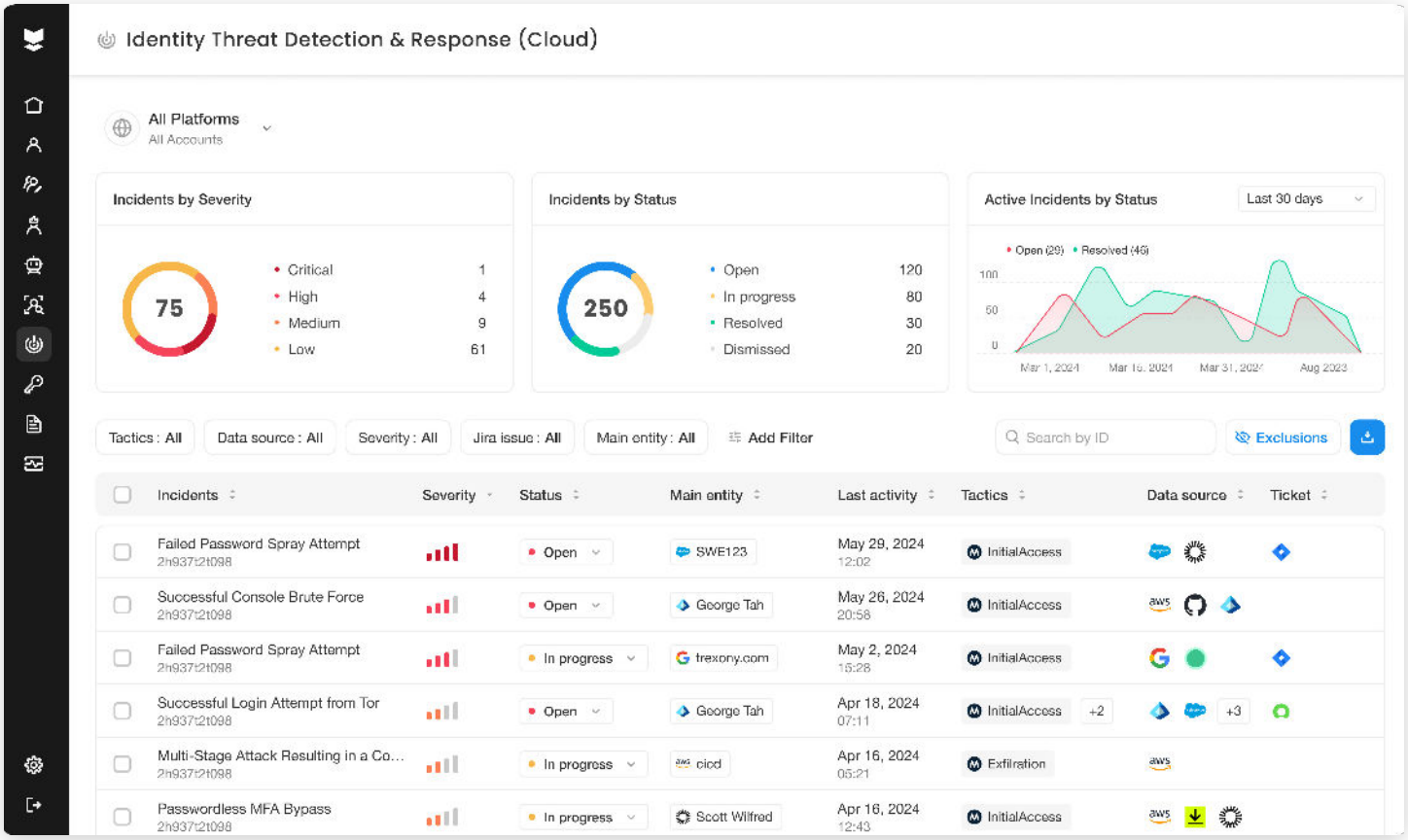
The moment Silverfort is deployed, it continuously detects, investigates, and responds to identity-based threats across cloud, SaaS, and on-prem environments. By correlating signals from identity providers, infrastructure, and applications, it provides full visibility into identity activity, surfaces high-confidence incidents, and stops attacks in real time. Silverfort follows a three-step approach to unify visibility, accelerate investigations, and enable proactive protection:

Step 1: Monitors all authentication and access activity across cloud IdPs, SaaS apps, SaaS platforms, and on-prem directories. Detects suspicious behaviors such as credential misuse, anomalous access, and lateral movement across accounts even when attackers switch usernames.

Step 2: Correlates identity activity across hybrid systems to expose the complete attack storyline. Surfaces MITRE ATT&CK-aligned, context-rich alerts that highlight threat progression, enabling SOC teams to understand impact, prioritize response, and investigate faster with confidence.

Step 3: Enforces real-time protection by triggering MFA, denying risky access, or applying automated policies at the point of authentication. Integrates seamlessly with SIEM, SOAR, and logging tools to streamline workflows.

The result: Teams gain unified visibility, high-confidence detections, and automated enforcement across the entire identity attack surface. This reduces alert fatigue, accelerates investigations, and enables organizations to prevent identity-based attacks before they spread across environments.



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.