Silverfort

Silverfort Identity Security Platform

Silverfort is the first identity security platform that extends modern identity security controls across the entire IAM infrastructure. With Silverfort you can discover every identity across every environment, analyze exposures to reduce your attack surface, and stop identity-based attacks including lateral movement and ransomware.

Silverfort capabilities

Identity Graph & Inventory

End-to-end visibility into all identities and their access

Silverfort Identity Graph & Inventory unifies identity data from Active Directory (AD), cloud IdPs, SaaS applications, and cloud infrastructure into a single view. It maps relationships, entitlements, and activity for every human identity, eliminating blind spots caused by silos. With contextual insights and advanced search, organizations can investigate privilege misuse, validate offboarding, and simplify audits, governance, and incident response.

Identity Security Posture Management (ISPM)

Continuously uncover, prioritize, and remediate identity risks across hybrid environments

Silverfort ISPM provides real-time visibility into exposures across both on-prem and cloud environments, such as misconfigurations, excessive privileges, stale accounts, and insecure protocols. It assigns severity level to each finding, links them to MITRE ATT&CK and compliance frameworks, and guides remediation with built-in steps. This unified approach reduces the identity attack surface, accelerates investigations, and strengthens audit readiness.

Universal MFA

Enforce MFA everywhere, including on-prem resources and legacy systems

Silverfort extends MFA to resources traditional solutions can't reach, including RDP, command-line tools, file shares, and legacy apps, without any infrastructure's changes. It unifies MFA across on-prem and cloud environments, eliminating gaps attackers exploit for lateral movement and ransomware, and ensuring compliance with regulations and cyber insurance requirements.

Service Accounts Protection

Discover, classify and protect your AD service accounts

Silverfort automates the discovery, access control, and protection of all on-prem service accounts in the environment. Organizations get granular visibility into every NHI and machine-to-machine authentication, as well as its sources, destinations, authentication protocols, and activity volume. By enforcing virtual fencing, Silverfort limits each service account to its intended purpose. Silverfort also monitors their behavior and, when it detects a deviation, can trigger an alert or real-time blocking.

Cloud Non-Human Identities (Cloud NHI)

Discover, monitor, and secure every cloud-based NHI

Silverfort discovers and classifies different types of NHIs across all identity providers, including cloud IdPs, cloud infrastructure platforms, and SaaS applications, providing complete visibility into their privileges. It helps identify ownership, reduce unnecessary permissions, and remediate critical exposures with actionable recommendations, minimizing the attack surface and closing compliance gaps.

Authentication Firewall

Block malicious authentications in real time

Silverfort enforces Least Privilege identity-based access policies across AD-managed resources, including legacy and OT systems. It blocks excessive permissions, denies risky protocols like NTLMv1 and LDAP, and stops lateral movement by containing attacks at the authentication stage.

Identity Threat Detection and Response (ITDR)

Real-time detection, investigation, and response to identity-based threats

Silverfort ITDR correlates identity activity across cloud, SaaS, and on-prem environments to uncover live threats. It surfaces high-confidence, MITRE ATT&CK-aligned alerts enriched with identity context, while enabling immediate enforcement actions like MFA or deny access. This reduces SOC fatigue, accelerates investigations, and stops identity-based attacks before damage occurs.

Access Intelligence

Real-time detection, investigation, and response to identity-based threats

Silverfort Access Intelligence provides dynamic visibility into how access is granted, inherited, and used. It maps full identity-to-application access paths, uncovers excessive or unused privileges, and correlates them with real usage signals. This enables smarter enforcement, faster remediation, and continuous governance—all without re-architecting your identity stack.

Privileged Access Security (PAS)

Discover, classify, and enforce least privilege for all privileged users

Silverfort PAS automatically discovers and classifies all privileged accounts, including hidden or cross-tier authentications, and enforces Just-in-Time (JIT) access policies. By removing standing privileges and restricting admin accounts to their intended purpose, it prevents lateral movement and privilege misuse.

AI Agents Security

Gain visibility and control over autonomous AI agents

Silverfort continuously discovers and classifies AI agents across IdPs, cloud platforms, SaaS, and infrastructure. It maps each agent to its human owner and initiator, tracks privileges and behavior, and surfaces over-privileged or rogue agents. With built-in risk scoring and governance controls, Silverfort ensures AI-driven automation operates securely, closing blind spots, supporting audits, and preventing misuse without disrupting innovation.

Trusted by leading organizations globally

Silverfort is trusted by leading organizations worldwide to help them strengthen their identity security posture and stop identity-based attacks.

See why customers trust us

About Silverfort

Silverfort secures every dimension of identity—human, machine and AI—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.