Silverfort

Identity Security Posture Management (ISPM)

Gain comprehensive visibility into the security gaps, misconfigurations, malpractices, and legacy infrastructure that expose your environment to identity threats.

An ounce of prevention is worth a pound of cure.

Silverfort leverages its patented Runtime Access Protection (RAP) technology to provide you with full visibility to any identity weakness adversaries might target to perform credential access, privilege escalation and lateral movement.

By proactively detecting and resolving threat exposures such as shadow admins, NTLMv1 usage, stale users, and many others, you're placing critical barriers in attacker's TTPs. This investment in building up your identity security posture delivers immediate ROI as attackers will move away from your environment in search for more vulnerable targets.

Balancing identity threat resilience with operational efficiency.

Threat exposure management

Discover identity threat exposures that allow adversaries to perform credential access, privilege escalation, and lateral movement.

IAM hardening

Resolve any detected issue in your AD, cloud IdP, or federation infrastructure by continuously monitoring their resilience to the widest range of identity threats.

User and authentication hygiene

Pinpoint operational issues such as failed authentication, stale accounts, on-prem accounts that were accidentally synced to the cloud, and many more.

Be one step ahead of your adversaries.

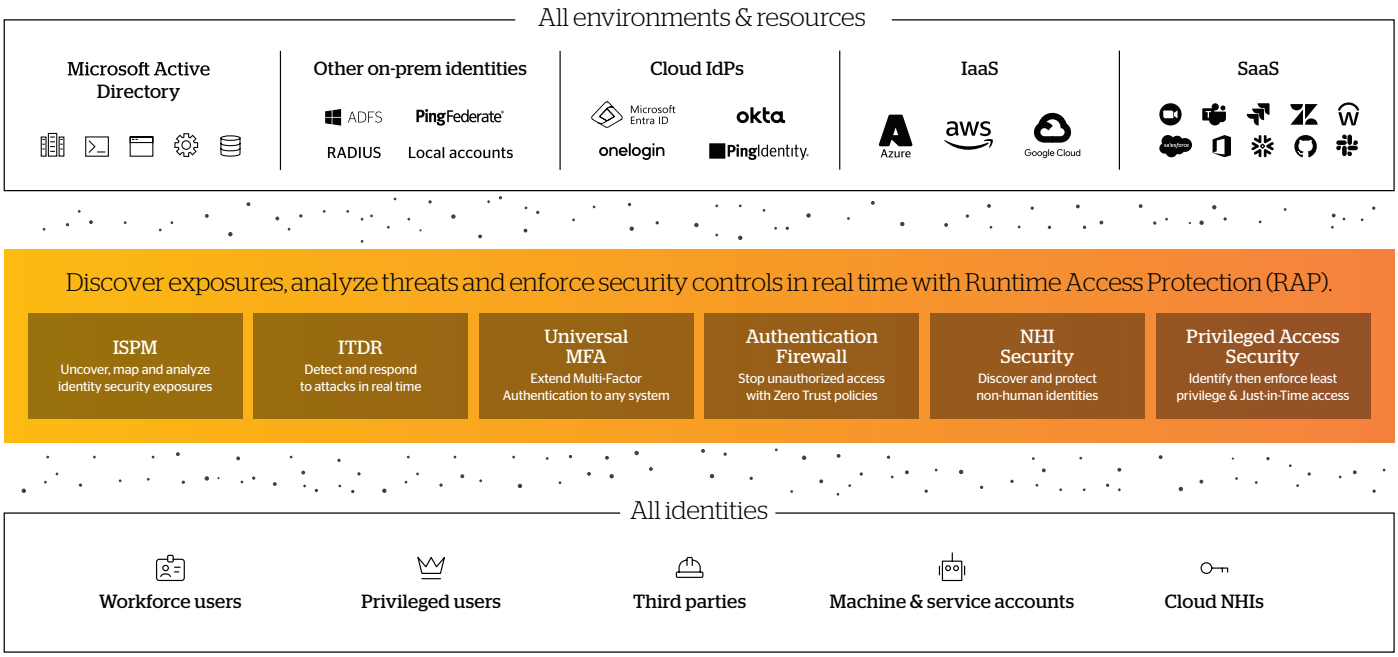
More than any other attack surface, identity is the most prone to the human errors that increase your exposure. Silverfort throws a spotlight on the weaknesses seen in all environments, so you can immunize your environments against attackers' identity threat playbook.

While investigating an active breach requires dedicated skills, time and resources, adjusting configurations, removing excessive permissions and reverting from malpractices is easily within reach. Silverfort ISPM is your ultimate companion in this journey, eliminating your knowledge blind spot and guiding you directly to the user accounts that need your attention.

86%

of data breaches involve the use of compromised credentials. This would entail credential access which would often be followed by privilege escalation. The combined impact of these tactics is the X factor that turns a local security event into an enterprise-level breach. Stay ahead of the curve and make sure your environment is resilient.

The Silverfort Identity Security Platform



Identity security: mitigate the risk of compromised credentials

ISPM is a key part in Silverfort's mission to deliver comprehensive identity security and mitigate the risk of malicious access with compromised credentials.

The Silverfort Identity Security Platform achieves this with its three core capabilities:

Continuous discovery of every user account and its activities within the hybrid environment.

Risk analysis of every account's security posture and every authentication and access attempt.

Real-time enforcement that blocks unauthorized and malicious access.

Silverfort implements these capabilities across all users, all resources, and all on-prem and cloud environments, so organizations can secure their entire identity attack surface with a single, easy-to-deploy solution.

About Silverfort

Finally, the identity security platform you deserve. Silverfort connects to your entire infrastructure to protect it from within. By breaking down silos and eliminating blind spots, Silverfort is the first to give businesses visibility into their whole network of identities and secure every identity, every resource, and every environment—all the time.