Silverfort

NHI security

Discover, monitor, and protect all non-human identities in your hybrid environment at scale, without requiring password rotation.

Why is NHI protection a critical challenge?

Non-human identities are a highly exposed and targeted attack surface, especially in Active Directory environments:

- Low visibility level, with many active NHIs operating under the IAM and security teams' radar.
- High access privileges to multiple resources to manage the services they are accountable for.
- Impossible to protect with MFA because they're not human.
- Difficult to protect with PAM password rotation due to operational disruption concerns.

Silverfort is the first solution to automate NHI security, finally putting this critical need within every organization's reach.

The whole journey: from visibility to comprehensive security.

Automated discovery

Gain visibility into your entire NHI inventory, including name, privilege level, security posture, sources and destinations of every account, so you can effectively prioritize.

Real-time protection

Activate an auto-generated policy that allows the account to access its standard sources and destinations, and triggers access block or alert when it deviates from its normal behavior.

Effortless to scale

Group all the accounts you want to protect under a single policy, continue adding accounts until all are protected, and integrate with your app management tool for ease of use.

We protect all non-human identities, no matter the scale or complexity.

Silverfort leverages its native integration with the on-prem and cloud IAM infrastructure to identify and classify NHI accounts based on their repetitive and pattern-like behavior.

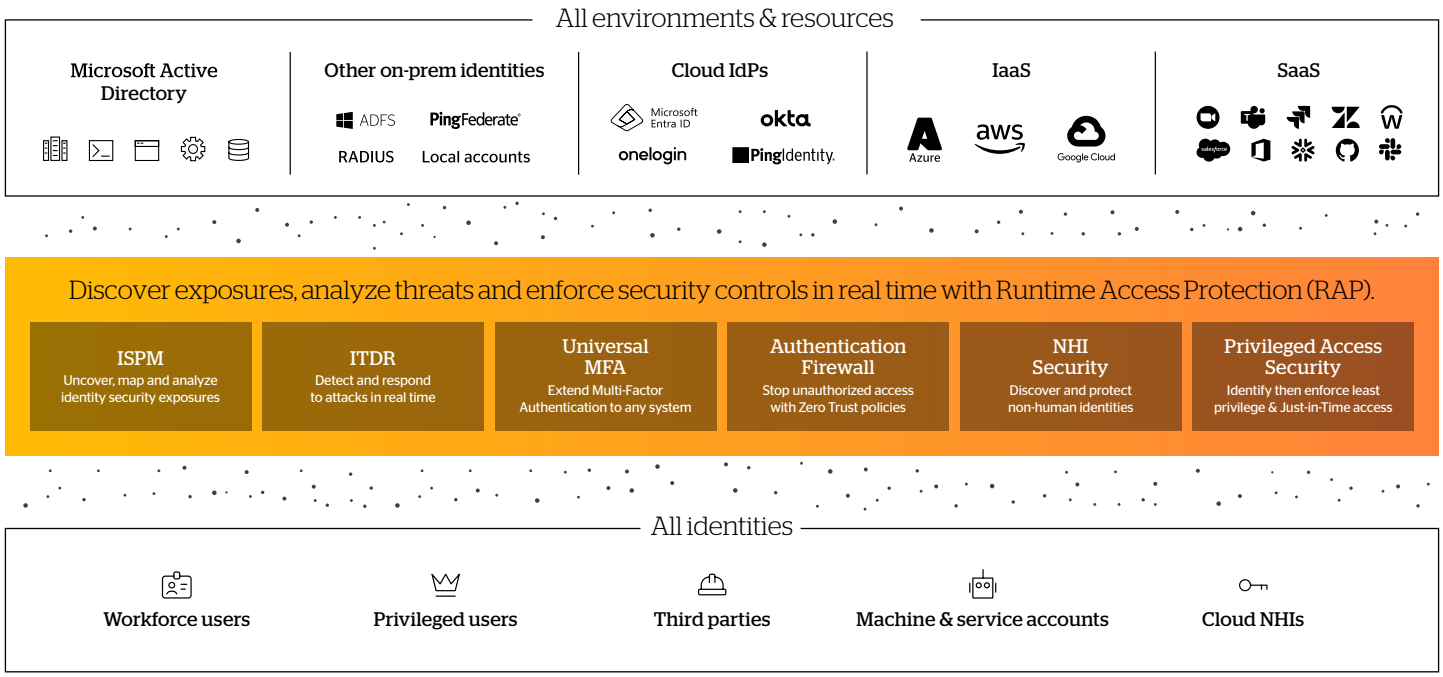
Once Silverfort validates an account as an NHI, the platform maps its baseline activity and automatically creates a virtual fencing policy that limits its access to its baseline destinations.

When activated, this policy would disable adversaries' ability to use the compromised account for lateral movement since every anomalous access will be blocked.

84%

of the lateral movement attacks investigated by Silverfort researchers have involved the compromise and use of an NHI, usually an Active Directory service account.

The Silverfort Identity Security Platform



Identity security: Mitigate the risk of compromised credentials

NHI security 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 in the enterprise 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.