Silverfort

Authentication Firewall: The power of deny

Enforce granular access control policies based on identities and activate protection in a single click—with no infrastructure changes.

Dynamic and flexible interface to govern all user access.

Silverfort leverages its patented Runtime Access Protection (RAP) technology to control all user access in the hybrid environment and provide access policies that are far more granular and flexible than those configured in the underlying IAM solution.

You can implement the authentication firewall's policies quickly and seamlessly, activating or disabling them in a single click. These policies can serve a wide range of purposes, such as eliminating the use of legacy protocols, enforcing least privileged access policies, or containing active attacks by revoking all user access.

Built for the needs of both IAM and security teams.

Identity segmentation

Enforce least privileged access policies on your workforce, ensuring users only access the resources they truly need and removing any excessive access permissions.

Attack surface reduction

Increase your environment's resilience to identity threats by eliminating the use of insecure protocols, such as NTLMv1 and cleartext LDAP, and other risky authentications.

Rapid incident response

Contain attacks with a single click by blocking any malicious attempted access, halting the attack's progression before it can do further damage.

The authentication firewall's advantage

Authentication firewall is the best way to manage users' access in your AD environment. Too often, AD access policies are either too basic or too complicated to effectively control your users' secure access.

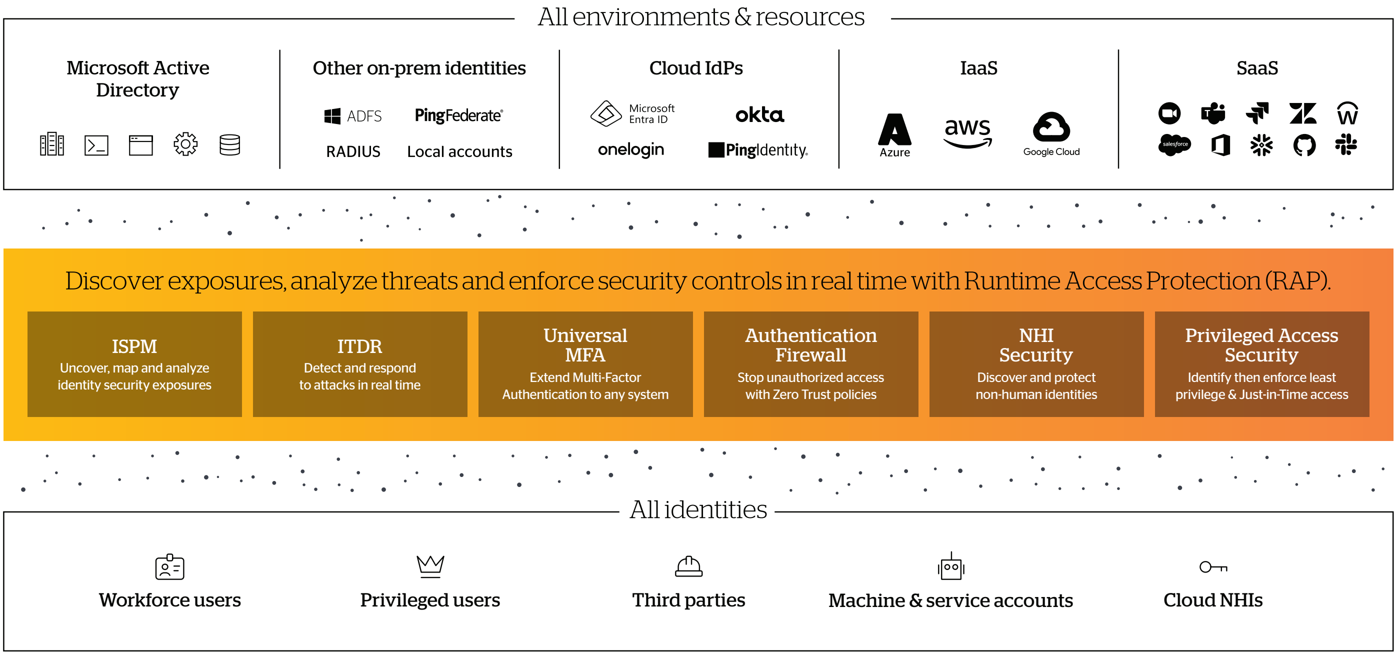
The high flexibility of the authentication firewall interface ensures IAM teams can easily and accurately implement their secure access strategy of choice:

- **User accounts** can be configured based on their individual identity, their AD group, or a combination of both.
- **Source and destination resources** can also be configured based on their individual identity, their AD group, or a combination of both.

86%

of data breaches involve the use of compromised credentials for lateral movement. This makes the ability to block the spread of detected attacks a critical need for every organization.

The Silverfort Identity Security Platform



All environments & resources

Discover exposures, analyze threats and enforce security controls in real time with Runtime Access Protection (RAP).

ISPM Uncover, map and analyze identity security exposures

ITDR Detect and respond to attacks in real time

Universal MFA Extend Multi-Factor Authentication to any system

Authentication Firewall Stop unauthorized access with Zero Trust policies

NHI Security Discover and protect non-human identities

Privileged Access Security Identify then enforce least privilege & Just-in-Time access

All identities

Identity security: Mitigate the risk of compromised credentials.

Authentication firewall plays 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 your 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 covers all users, all resources, and all on-prem and cloud environments, so you can secure your 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.