Silverfort

Silverfort Authentication Firewall

Stop lateral movement and unauthorized access with real-time, identity-based access control

The Challenge: **Static controls can't stop dynamic threats**

As identity threats grow more sophisticated, traditional access controls can no longer stop lateral movement and privilege escalation once credentials are compromised. Network segmentation and AD group permissions are static and lack identity context, leaving excessive permissions and insecure protocols like NTLM and LDAP, and local accounts exposed and exploitable.

Once attackers gain valid credentials, static defenses like network segmentation and AD permissions can't stop them from moving laterally or escalating privileges. At the same time, IAM and security teams struggle to enforce least privilege consistently across hybrid infrastructures all while trying to reduce breach impact and operational overhead.

Ongoing challenges make it harder to maintain consistent access control and stop identity threats:

- **Static network and AD controls** fail to adapt to changing user behavior or risks in real time
- **Credential-based attacks** exploit legacy authentication protocols and excessive permissions to move laterally undetected
- **Local accounts** fall outside central identity security controls, creating unmanaged pathways for lateral movement
- **Operational complexity** makes it difficult to enforce least-privilege access and containment consistently across hybrid environments

Authentication Firewall: Enforce access control and containment in real-time

Detect and block risky authentications in using deny and identity-aware access control policies that respond instantly to malicious logins or credential compromise. Prevent privilege escalation and stop ransomware before it spreads.

Apply identity-based access and segmentation policies directly at the authentication layer across AD, cloud, and local logon activity. Block unauthorized access dynamically to protect initial access to critical resources and to prevent lateral movement.

Contain active breaches the moment they occur by isolating compromised identities during an active breach. Stop attackers from moving laterally and reduce the blast radius to minimize impact.

How it works

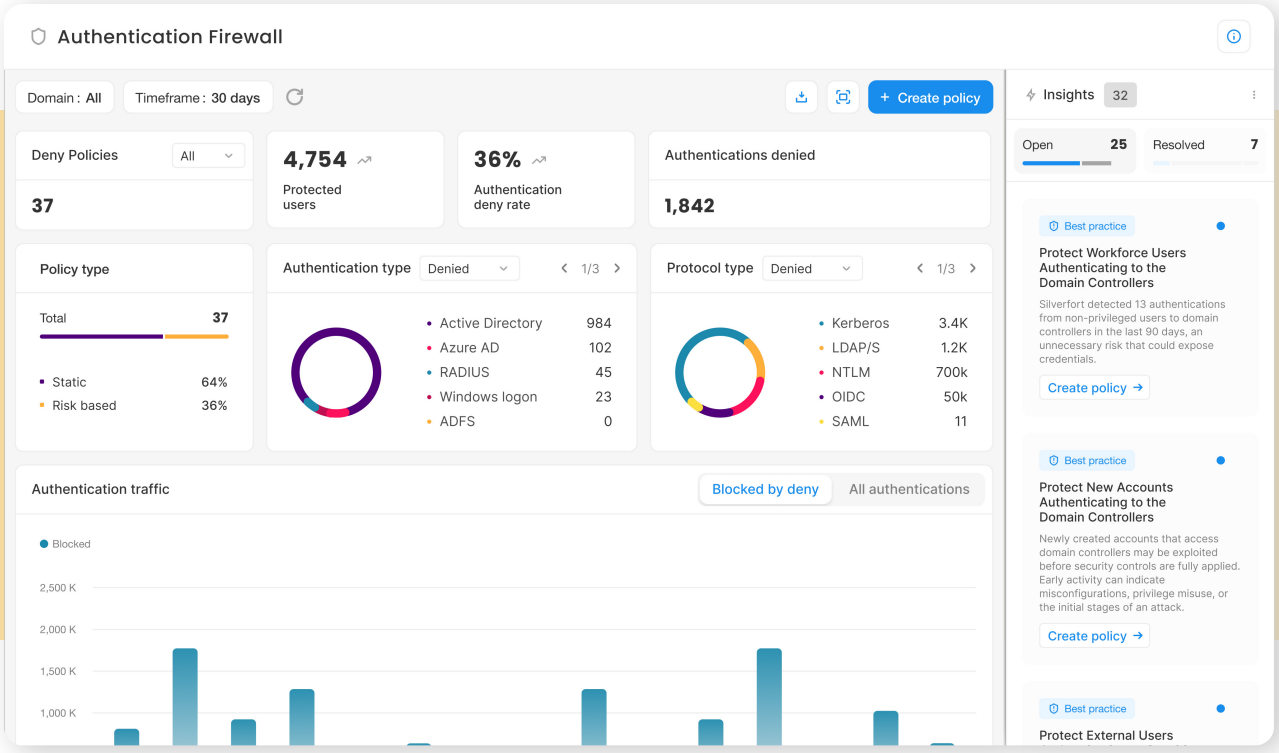
Silverfort enforces deny and segmentation policies directly at the authentication layer by integrating with Active Directory to analyze and control every access attempt in real time.

Step 1: Connect to Active Directory to gain full visibility
Silverfort integrates natively with AD to monitor all authentication traffic across cloud, on-prem, hybrid environments, and local Windows logons (via Silverfort for Windows Logon). This provides complete visibility into every access request without changing network architecture.

Step 2: Enforce deny and segmentation policies at authentication
Silverfort evaluates every authentication attempt, including Kerberos, NTLM, LDAP, and local account logins in real time against user identity, behavior, and access context, blocking unauthorized or risky access automatically to stop attackers before they move laterally.

Step 3: Contain active threats immediately
When a breach is detected, Silverfort isolates compromised identities and blocks malicious domain or local authentications to prevent further spread and minimize impact.

The result: organizations gain real-time control over access and containment all human identities, including cloud, on-prem and local accounts, stop identity-based attacks before they spread, and enforce least-privilege access across hybrid 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.