SILVERFORT

Authentication Firewall

Actively govern and control access to resources based on user identity in a single click with no infrastructure changes

An authentication firewall is an identity security approach designed to control and monitor user access activity to resources by enforcing strict authentication controls. This allows identity security teams to create and enforce policies to restrict access and remove excessive access permissions.

With Silverfort's authentication firewall, organizations can, for the first time, block access to resources based on user identity and real-time authentication analysis. The authentication firewall's policies do not require any changes to the underlying networking infrastructure and can be implemented seamlessly and rapidly. By deploying the authentication firewall adaptive risk engine, identity security teams can enhance their environment's resilience to identity threats as well as optimize their response processes in the event of an active breach.

Authentication Firewall Key Capabilities

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

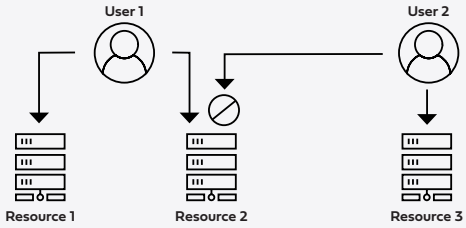
Increase your environment's resilience to identity threats by eliminating the use of insecure protocols such as NTLMv1 and cleartext LDAP, as well as other risky authentications.

Identity Incident Response

Contain a known attack with a single click by blocking any attempted malicious access and halting the attack's progression.

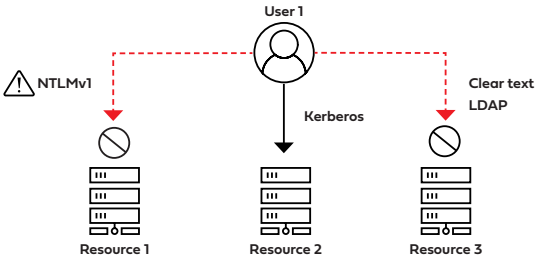
How does Silverfort's Authentication Firewall Work

Identity Segmentation



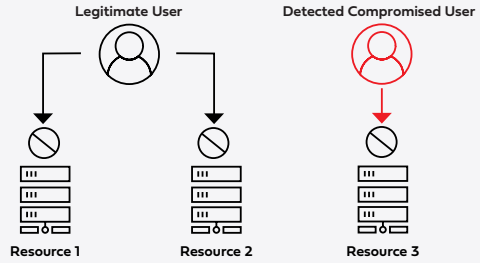
- Ensure users only access the resources they need and nothing beyond that.
- Segment internal networks based on each user's Organizational Unit (OU) and role.
- Align with any existing network segmentation and create another layer of security that limits access between different zones in the network.

Attack Surface Reduction



- Detect and block the use of insecure protocols that could expose user passwords. Prominent examples are NTLMv1 which uses a weak encryption algorithm, or LDAP which sends the actual cleartext password over the wire.
- Deploy Silverfort's risk analysis in your environment to gain a wide range of risk indicators that relate either to the user, the source and target machines, or the authentication itself.
- Utilize risk indicators to trigger a deny access policy, based on the organization's specific security needs and practices.

Identity Incident Response



- If a breach occurs, the authentication firewall's deny access policy can be applied for immediate containment of the attack. In this manner, attackers would be prevented from accessing additional resources.
- After all malicious presence has been eradicated during the response process, gradually remove all blocking of access to users and resources.
- Apply this level of protection to any type of lateral movement, regardless of protocol and access method, including command line tools often used by adversaries like PsExec, PowerShell, and WMI-based utilities.