SILVERFORT

5 Quick Wins You Can Achieve with Silverfort

Smart organizations understand that they are likely to be compromised and need to develop proactive security controls to prevent this.

Here are 5 quick wins you can implement to strengthen your identity security posture management.

1. Deployment and Time to Value

Time to Value: One week to a month

Unlike PAM or IGA projects, with Silverfort, you don't need to worry about complex and time-consuming deployments. Instead, you will able to demonstrate a step change in security posture to the business within a month.

- We place a lightweight adapter on the DC for forwarding authentications to the Silverfort VM, where computing and analysis take place
- We run due diligence on the DC health and are certified by Microsoft
- Deployment requires minimal resources, with minimal impact on BAU activities and low staff overhead (typically max 1/2 SME)
- AD performance is not affected by the implementation of MFA and Service Account protection
- Our expert Customer Success team is tailored to meet the complexities of your environment to speed up deployment

2. Detects and Monitors All Users

Time to Value: Instantly

The moment Silverfort is deployed into your environment, it will detect and monitor all user accounts and provide real-time insights into their activity and associated risks, providing instant benefit to your security operations.

- Alerts on risky users and malicious activity
- Alerts for interactive service account login
- Alerts on identity threats such as brute force, Kerberoasting, and more
- Real-time insights into threats and attacks
- Full visibility into users' activity empowers you to block or mitigate an incoming threat

3. Enforcing MFA on Command-Line Access Tools

Time to Value: One week

Quickly reduce the use of command-line interfaces and PowerShell by applying MFA protection to all command-line tools. Silverfort's architecture obviates the protocol support issue because it's able to analyze and gain insight into any authentication packet forwarded by Active Directory. This makes Silverfort the only solution that can protect remote connections between the host or server that is using command-line tools that are integrated with most ransomware attacks, effectively mitigating the risk of ransomware spreading in the environment.

- Real-time prevention of ransomware propagation by enforcing MFA on administrative tools
- Block any attack propagation such as lateral movement and ransomware attacks and more
- Stop admins from running scheduler scripts on their behalf by enforcing MFA on remote command-line tools

4. Service Account Visibility & Protection

Time to Value: One week to a month

Silverfort identifies service accounts based on the repetitive behavior that sets them apart from human users. Silverfort monitors the behavior of every service account and allows you to apply suggested tailor-made access policies that will either alert the SOC team or block access upon deviation from standard behavior.

- Automated and comprehensive discovery of all service accounts within the environment
- Full visibility into each account's risk level as well as sources and destinations, enabling effortless dependency mapping
- Real-time detection alerts of any deviation from the service account's standard behavior
- Automatic suggested policies for each service account to enable alerts or protection in a single click
- Assess the risk of every authentication attempt and detect any suspicious behaviors or anomalies

5. Identity Segmentation

Time to Value: One Week

The concept of network segmentation has been around for quite some time and is one of the core elements of the Zero Trust framework. Although network segmentation reduces the attack surface, it is extremely time-consuming and does not protect against adversary tactics and techniques at the identity layer. As a result of Silverfort's identity segmentation capabilities, a quicker time to value can be achieved rapidly by reducing identity threats, costs and operational complexity.

- Gain full context and visibility into every user and authentication activity
- Block access requests for every type of user, service account, access method, and resource in real time
- Assign each user account and service account to access group-segmented policies
- Enforce policies to either require MFA or block access to any privileged account that attempts to access a resource