SILVERFORT

Meet Today's Cyber Insurance Requirements with Silverfort

Silverfort enables companies to qualify for cyber insurance by enabling MFA across all admin access as well as facilitating the discovery and protection of privileged service accounts.

With ransomware attacks on the rise, companies of all sizes have found their operations to be vulnerable. A resulting spike in insurance claims has led underwriters to substantially revise requirements to qualify for a policy, mandating that companies be able to enforce multifactor authentication (MFA) across all admin access (both internal and external) as well monitor and protect privileged accounts to stop the lateral movement that leads to ransomware spread.

The challenge here is that there is no MFA solution that can protect every system and access interface, including the command-line access tools that attackers routinely use for lateral movement.

As well, there is no utility that can identify – much less protect – all of the highly privileged service accounts that attackers relentlessly seek to compromise.

Silverfort: Your One-Stop Solution for Cyber Insurance Renewal

While these requirements have come as a surprise to many organizations, there is in fact a way to address them via an approach both straightforward and lightweight. **Silverfort's Unified Identity Protection** platform uses an agentless and proxyless architecture that requires no modifications to the existing environment or any code changes.

When Silverfort is deployed, the solution monitors every authentication request, passing it to a risk engine that can immediately determine the legitimacy of that request – approving it, denying it, or challenging it with MFA. Based on Silverfort's verdict, the identity provider (IdP) will then either grant or deny access to the user.

KEY BENEFITS

End-to-End Protection
Enforce MFA across all on-prem and cloud resources to proactively prevent ransomware attacks.

Secure Every Identity
Identify every user in the environment (both human and non-human), see every authentication request, and enforce access policies.

Prevent Ransomware
Implement MFA protection for command-line tools that threat attacks use for lateral movement.

Rapid Time to Value
Deploy a scalable solution that can be installed in the production environment quickly.

Agentless & Proxyless
Easily integrate MFA with any IdP without the need for modifications or code changes.

MFA Everywhere

Silverfort is the only solution that can enforce MFA from the backend of any IdP, rather than through the addition of agents or proxies on individual endpoint resources. This means you can immediately protect any user account and resource with MFA — including legacy and homegrown applications, command-line access tools that admins regularly use (such as PsExec, PowerShell, and WMI), industrial and healthcare systems, file shares, and databases.

Service Account Protection

Silverfort's visibility into every authentication request enables it to automatically discover every service account in the environment, since those accounts display highly predictable behavior. This allows organizations to easily conduct inventories of these privileged non-human accounts and create policies to block access or send alerts in the case of any abnormal access attempt — therefore preventing threat actors from using them in lateral movement attacks.

Meet All MFA and Service Account Requirements

Required Solution	Capabilities	Silverfort
	MFA	
Cloud-Based Email	All employees when accessing email through a website or cloud-based service	✓
Remote Network Access	All remote access to the network provided to employees, contractors, and third-party service providers	✓
Internal and Remote Admin Access	All internal and remote admin access to directory services (Active Directory, LDAP, etc.)	✓
	All internal and remote admin access to network backup environments	✓
	All internal and remote admin access to network infrastructure (firewalls, routers, switches, etc.)	✓
	All internal and remote admin access to the organization's endpoints/servers	✓
	PRIVILEGED SERVICE ACCOUNTS	
Inventory	Regular inventories of all service accounts including name of account, privileges of each, software product supported, hosts authenticated to, and why entitlements are required	✓
Monitoring	Rules in place to monitor service account activity and alert SOC of any abnormal behavior	✓
Protection	Policies to automatically block access in case of service account compromise	✓

How Does Silverfort's Solution Streamline Compliance?

Silverfort's identity protection platform gives companies the ability to fast-track the cyber insurance renewal process through a comprehensive solution that meets every requirement from underwriters.

While cyber insurance requirements have become more difficult to fulfill, these changes actually point toward a future where enterprises are much better prepared against cyberattacks.

Implementing MFA across all resources and protecting all privileged accounts are essential steps towards an improved security posture. Silverfort makes this easy and fast.

To learn more, request a demo here.