SILVERFORT

Implementing MFA for Cyber Insurance Made Easy with Silverfort

Silverfort enables companies to easily meet the new cyber insurance requirements for MFA protection across all sensitive systems, both on-prem and in the cloud, including legacy systems and admin interfaces that couldn't be protected before.

Ransomware attacks and other cyber incidents are on the rise around the globe. The sheer scale and frequency of these attacks have demonstrated that everyone is vulnerable, including organizations of all sizes, the largest and most respected financial institutions, and even the United States government. This has prompted insurance companies to tighten their requirements for providing cyber insurance and protect themselves against financial exposure in the increasingly likely case that an organization falls victim to a cyberattack.

The new cyber insurance requirements mandate that organizations implement EDR and MFA protection within their environments. Furthermore, state and local government agencies are constantly updating cyber insurance regulations to ensure that cyber insurance helps offset the cost of physical and digital damage from cyber threats and cyberattacks. Specifically, one of the most critical new requirements for organizations to become cyber insurance-compliant is that all resources and devices need MFA protection.

Silverfort: Your One-Stop Identity Security Solution for Cyber Insurance Compliance

The new requirement for MFA protection introduces a severe challenge to small and mid-sized organizations since standard MFA solutions cannot deliver the required coverage and deploying a PAM solution is typically not practical for them.

MFA Protection Everywhere

Silverfort is the only solution that enforces MFA from the backend of identity providers, rather than by adding agents or proxies on the individual endpoint resources. In practice, this means you can deploy Silverfort into an organization's production environment and immediately protect user accounts and resources with MFA.

Not only does Silverfort protect internal and remote admin access in on-prem environments (which no other solution does), but it can also consolidate all MFA protections in a single solution, making it a natural answer to help organizations become cyber insurance compliant.

KEY BENEFITS

Full MFA Coverage for Cyber Insurance
Implement cyber liability policies by checking off all the MFA requirements.

End-to-End User & Device Protection
Enable MFA access control on all on-prem and cloud resources to proactively prevent ransomware attacks.

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

Agentless and Proxyless
Enforce MFA which natively integrates with all your identity providers, rather than applying agents or proxies.

Prevent Ransomware Propagation
Implement MFA protection for the command line tools that ransomware attacks use.

Minimizing Risk Through Identity Access Management

When Silverfort is deployed in an environment, it collects information about authentication requests for all users. This information is used by the risk engine to analyze the risk when a user tries to authenticate to a resource. Silverfort determines whether to allow the user to access the requested resource, deny access, or challenge the user with MFA verification. The IDP grants or denies access from the user based on Silverfort's verdict.

What does Silverfort's MFA Solution for Cyber Liability Compliance Offer?

An all-in-one identity-protection solution that is flexible and can be tailored for all insurers' cyber risk policies. Silverfort uses agentless and proxyless technology to extend MFA to all users and resources included in the new cyber insurance requirements:

- **Email**
- **Remote network access**
- **Internal and external admin access**
- **Networking infrastructure**
- **Directories**
- **IT & Security Management**
- **Servers & Workstations**

MFA Requirements		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 3rd party service providers	✓
Internal & Remote Admin Access	All internal & remote admin access to directory services (Active Directory, LDAP, etc.)	✓
	All internal & remote admin access to network backup environments	✓
	All internal & remote admin access to network infrastructure (firewalls, routers, switches, etc.)	✓
	All internal & remote admin access to the organization's endpoints/servers	✓

With cyber security insurance requirements becoming more and more difficult to fulfill, now that providers have added so many new requirements for compliance, finding the right solution is not easy. Protecting every company asset with MFA, and getting users on board with large-scale changes, often within short timeframes, is a major challenge for most organizations.

However, these changes signal a substantial shift towards a future where enterprises are much better prepared against cyberattacks. Implementing MFA across all resources in the organization is a huge step towards an improved security posture. And it doesn't have to be painful – Silverfort makes the process of extending your current MFA solutions to cover all resources in your organization quick and straightforward.

To learn more, request a demo here.