SILVERFORT

Help your clients qualify for cyber insurance coverage with Silverfort

Silverfort enables clients 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.

Cyberattacks are a fact of life. Every organization is being targeted in some manner, from ransomware to supply chain attacks to malicious account takeovers. Just as brokers provide physical theft, D&O, and GLI insurance, there is a huge demand to offer cyber insurance to protect organizations against financial loss in the case of a cyberattack data breach or ransomware claim. According to a report by Deloitte, the global cyber insurance market size is projected to grow from $7.8 billion in 2020 to $20.4 billion by 2025, due to data breaches and the surge in mandatory cybersecurity regulations and legislations.

The challenge is that "three out of four companies do not meet [our] requirements for cyber security", according to the global cyber underwriting lead at Allianz. Since 2016, cyber claims have increased more than tenfold, with ransomware and DDoS topping the list. Insurance providers have responded with more stringent and specific security requirements, 40+ page detailed attestation forms, external pen tests, increasing premiums to adjust for the higher risk, and in many cases have declined to offer coverage at all.

Why is the new expanded MFA requirement a challenge?

Organizations are moving quickly to meet new security requirements to qualify for cyber insurance. One area where insurance providers have raised the bar is multi-factor authentication (MFA). MFA is familiar for us as consumers, for example, there is the additional step-up authentication or MFA (ie. text, email, or one-time-passcode) required to verify identity before granting access when we authenticate to our online banking website.

In corporate security, MFA is also very important. Especially for system administrators and users with elevated privileges. These are the identities that attackers are seeking. However, according to CISA (Cybersecurity & Infrastructure Security Agency) in May 2022, MFA not being enforced is the #1 weak security control that hackers are exploiting for initial access. Attackers are bypassing traditional MFA and flying under the radar using low-level system admin interfaces such as PSExec, PowerShell, WMI, and RDP to steal credentials and propagate ransomware.

Account takeovers, malicious remote connections, and mass ransomware propagation are prominent examples. Gartner ranked these "Identity Security" attacks as the #2 top cyber trend for 2022. Cyber insurers have also taken note and have added new very specific requirements to require MFA for system administrators directly accessing corporate systems.

MFA Availability Gaps: Drill Down

Cloud/Web-based email

Available from the email provider

Remote access connection

Available from the remote access provider

Internal & external admin access

Not properly addressed by any MFA solution

If MFA is universal, what then is the problem? The challenge is that many of these system admin interfaces, and legacy applications do not natively support MFA, and MFA just for VPN logins is no longer enough to meet most cyber insurer requirements. The requirements listed by major insurers are:

MFA for all internal & remote admin access to the following:

Directory services
(Active Directory, LDAP, etc)

Network backups

Network infrastructure
(firewalls, routers, switches, etc)

Endpoints & servers

One large organization called these “unprotectable applications” because they just don’t natively support MFA. Impractical workarounds such as installing server or end-point agents, implementing network changes such as proxies, or making code changes on the individual legacy applications – are also usually non-starters.

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	✓

What does the Silverfort MFA solution offer for cyber liability compliance?

Silverfort uses agentless and proxyless technology to extend MFA to any resource and access interface across the on-prem and multi-cloud enterprise environment. This includes assets that could never have been protected with MFA before, such as legacy and homegrown applications, command-line access tools, industrial and healthcare systems, file shares, databases, and more. This makes Silverfort unique in helping organizations meet cyber insurance policy requirements to qualify for coverage.

The Silverfort Insurance Broker program includes the following partner types:

1. **Recommending partners** – Expedited access to Silverfort experts for your clients.
2. **Referral partners** – Receive a rebate or referral fee for each client enrolled.
3. **Resell partners** – Brokers that package Silverfort along with EDR, email phishing, and other security tools to help clients meet cyber security posture requirements.

Silverfort Identity Security Dashboard

Contact Silverfort’s Insurance Broker partner team or sign up to become a partner for more information