Silverfort

T he New Cyber Insurance Requirements:

What to Know & How to Comply

Can you Afford the Risk of not Having Cyber Insurance?

As cyberattacks increase in volume and intensity, organizations rely on the peace of mind provided by cyber insurance. In the case of a successful breach or ransomware attack, the right policy means liability will be limited and losses contained.

But skyrocketing claims in 2020 led insurance companies to drastically rework the criteria for acquiring or renewing cyber insurance. Today, companies face a completely changed landscape, with organizations required to demonstrate the ability to fend off ransomware attacks via a wide array of security controls.

For example, underwriters now require specific identity security measures to be in place, including the ability to enforce multifactor authentication (MFA) across internal and external admin access within the environment as well as monitor and protect all privileged accounts to prevent the lateral movement threat actors perform to spread the ransomware in the targeted environment. The challenge here is that there is no MFA solution that can protect the command-line access tools attackers utilize to launch this lateral movement. Furthermore, there is no built-in utility for the protection of highly privileged machine-to-machine service accounts that attackers typically compromise.

As the rate of ransomware attacks soars – up 71% in the past year and fueled by the billions of stolen credentials available on the dark web – threat actors increasingly make use of lateral movement to successfully spread payloads across an entire environment at once. Major companies including Apple, Accenture, Nvidia, Uber, Toyota, and Colonial Pipeline have all been the victim of recent high-profile attacks resulting from blind spots in identity protection. This is why underwriters have put stringent measures in place that companies must meet before being eligible for a policy. The new requirements have come as a surprise to many organizations, who find themselves struggling both with understanding the technical details and also with finding the right solutions to qualify for a policy. Fortunately, there is a way for companies to address even the most challenging requirements via an approach that is straightforward and lightweight.

Silverfort Identity Security platform uses an innovative architecture – one that requires no modifications to the existing environment or code changes – to address the new cyber insurance requirements in an easy to implement solution. In this eBook, we examine these requirements in depth, discuss the challenges of each, and explain how Silverf-rt enables you to comply.

Examining the New Identity Security Requirements

The goal of the new cyber insurance requirements is to increase the resilience of various attack surfaces within the environment. Zooming in on the identity attack surface, we can identify two key areas:

Requirement 1: Multi-Factor Authentication (MFA) for Administrative Access

Because user accounts are the way that company resources are accessed – including SaaS applications, on-prem servers and workstations, and cloud workloads – attackers relentlessly try to compromise those accounts by making use of the more than 24 billion credentials for sale on the dark web. MFA is the most effective protection against this attack, reducing the effectiveness of malicious access by 99%ץ

Requirement 2: Privileged Account Protection including Service Accounts

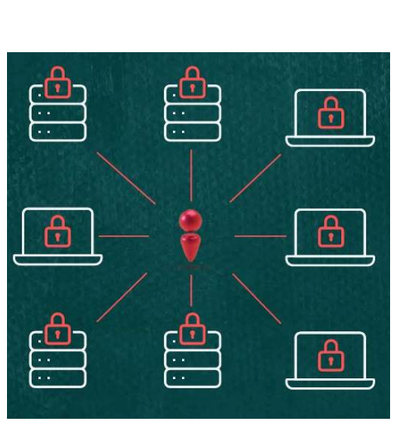
Insurers have recently focused attention on privileged accounts, particularly non-human service accounts used for machine-to-machine communication to run various management, scanning and software maintenance processes. These accounts are often targeted due to their low visibility as well as the fact that they are typically excluded from password rotation. Some policies now require companies to conduct regular inventories of these accounts and put in place security measures to prevent attackers from using them for malicious access.

The Point of the New Requirements: Prevent Ransomware Attacks

Insurance carriers are requiring the additional security measures of MFA, and service account protection in order to increase resistance to ransomware attacks — specifically the stage called lateral movement

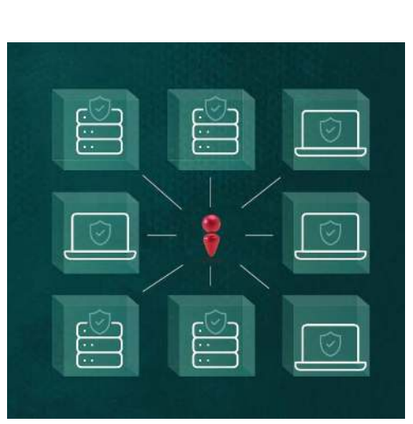
What is Ransomware Lateral Movement?

The initial delivery of ransomware to a user's machine enables its execution on this machine alone. "Lateral movement" refers to the stage after the initial delivery, in which the attackers use compromised credentials to access as many machines as possible and maximize the attack's payoff by encrypting all of them at once. MFA and service account protection are instrumental in preventing this lateral movement



How do MFA and Service Account Protection Prevent it?

Since lateral movement is carried out by logging in with compromised user credentials, enforcing MFA on these access attempts can thwart them altogether. If the attackers are utilizing a compromised service account, monitoring this account's activity and blocking its access whenever it deviates from its standard activity would have the same effect.



The Cyber Insurance Checklist: Operational & Security Challenges

Organizations find that meeting the new MFA and service account protection requirements is extremely challenging. Let's take a deep dive into the specific requirements to understand why

MFA Requirements

Cloud-Based Email

"All employees when accessing email through a website or cloud-based service."

⚠ MFA is natively integrated into the email service by its provider but cannot cover any other resources.

Remote Network Access

"All remote access is provided to employees, contractors, and third-party service providers."

⚠ MFA is natively integrated into the remote connection by its provider but cannot cover any other resources.

Admin Access

"All internal and remote admin access to: directory services (Active Directory, LDAP, etc.) network backup environments network infrastructure (firewalls, routers, switches, etc.) workstations and servers"

⚠ These access vectors are not covered by standard MFA solutions.

Service Account Requirements

Inventory

"There is an inventory of all privileged service accounts' names, privilege level and activities updated at least quarterly."

⚠ There is no utility that can generate a report of current service accounts.

Monitoring

"Specific rules are in place for service accounts to alert your SOC of any abnormal behavior."

⚠ Configuring policies to monitor service account activity is extremely labor intensive.

Protection

"Steps are taken to mitigate any exposure the service account configuration creates that could result in credential harvesting."

⚠ Rotating passwords of service accounts can break critical processes.

Options for Compliance

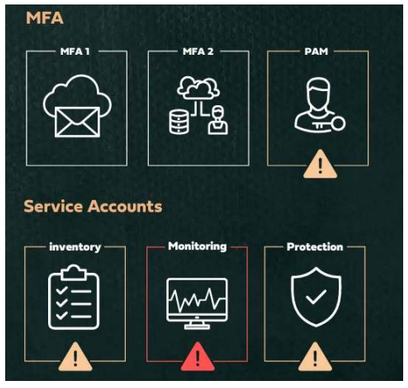
Insurance carriers are requiring the additional security measures of MFA, and service account protection in order to increase resistance to ransomware attacks — specifically the stage called lateral movement

Multiple MFA Solutions + Manual Service Account Monitoring

Protect email and remote network access with native MFA, then tailor an additional MFA solution to the admin access requirements, and manually search for all privileged service accounts in your environment. For MFA, this approach entails operational complexity in managing multiple solutions, For service accounts, this is resource-intensive and may not reveal all accounts.

Multiple MFA Solutions + Privileged Access Management (PAM) + Manual Service Account Monitoring

Protect email and remote network access with native MFA then implement a PAM solution for the admin access. This approach will prove impractical for most organizations due to the lengthy deployment processes and management resources that PAM solutions require. For service accounts, follow the same procedure as at left.



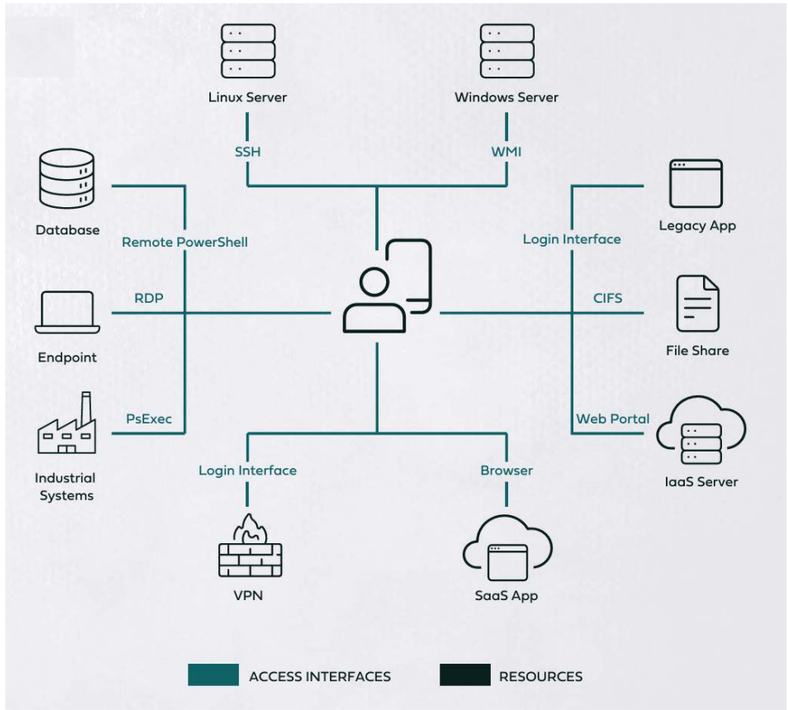
Silverfort Identity Security Platform

MFA protection for email, remote network access, and admin access in a single solution as well as automated discovery, monitoring, and protection of all service accounts without the need for password rotation

Silverfort Identity Security Platform: Universal MFA

Silverfort uses its proprietary Runtime Access Protection (RAP)technology to extend MFA to any resource and access interface across the on-prem and multi-cloud enterprise environment. This includes assets that could not 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.

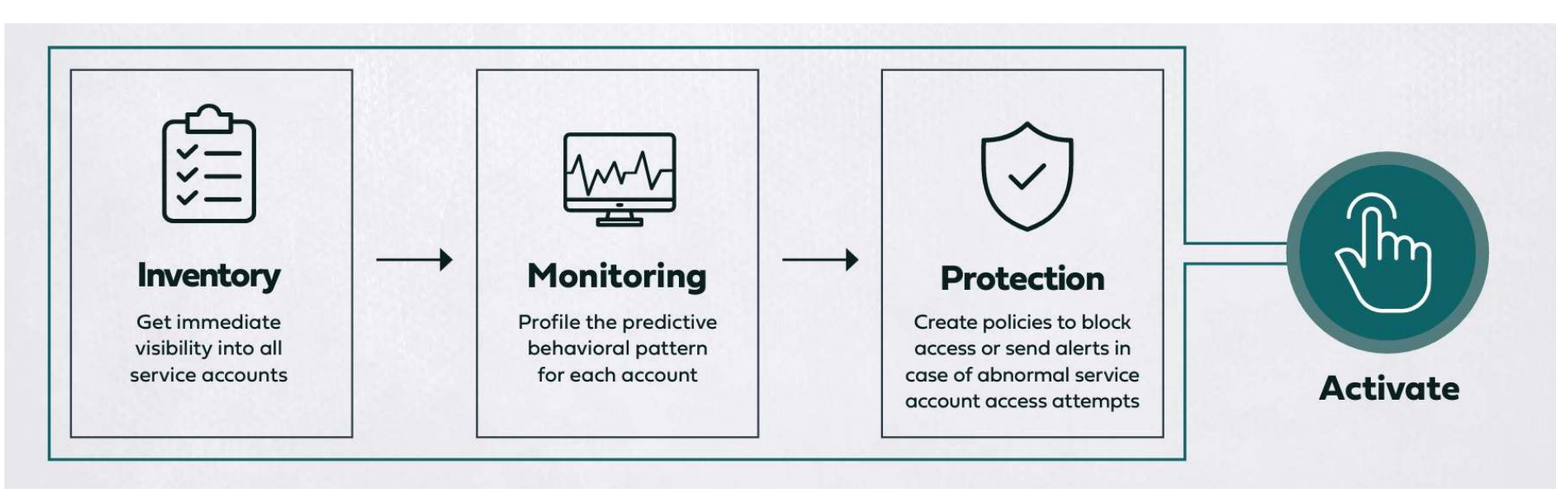
This makes Silverfort an ideal solution to meet the cyber insurance requirements for MFA



Silverfort Identity Security Platform: Service Accounts

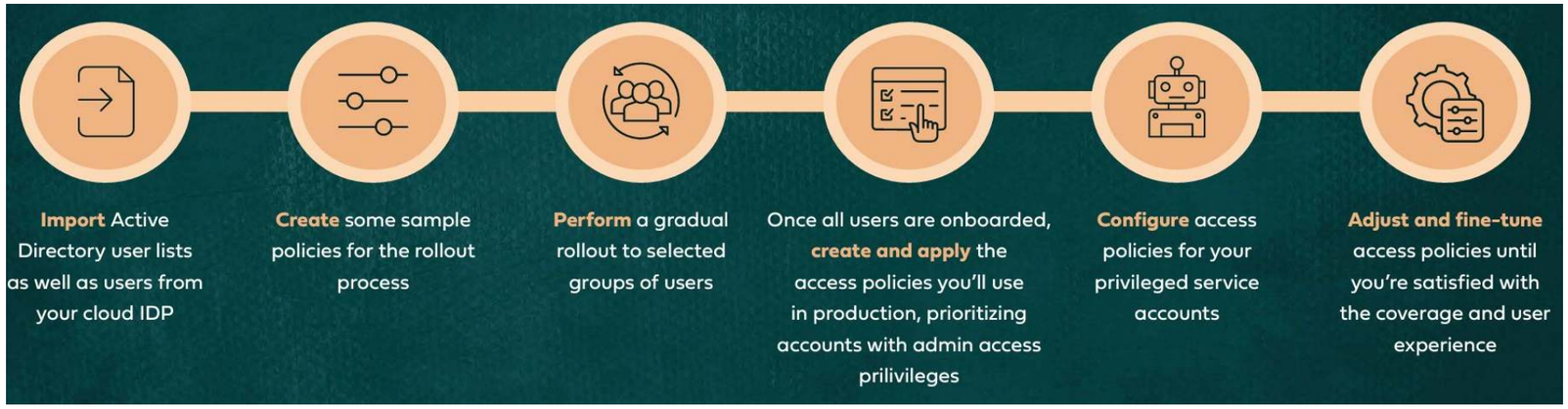
Silverfort enables organizations to automatically discover all service accounts, giving IT teams real-time visibility into every non-human identity and machine-to-machine authentication. Silverfort comes with ready-to-use Zero Trust access policies, tailored to each account's exact behavior, in order to prevent threat actors from using them in lateral movement attacks.

This makes Silverfort an ideal solution to meet the cyber insurance requirements for service accounts.



Get Started Quickly with Silverfort

The Silverfort deployment process is straightforward. The fact that no agents need to be installed on individual machines (or proxies in front of them) simplifies and accelerates the process. Once the Silverfort platform is installed, you can configure policies for any user that authenticates to your Active Directory, fully meeting the requirement for internal and external administrative access



How to Know if Silverfort is Right for Your Environment

1. **Assess** your environment to discover any gaps in your MFA resource protection and any roadblocks to monitoring service accounts.
2. **Shortlist** several solutions based on the specific requirements of your underwriter.
3. **Conduct** a POC on a limited deployment (size varies according to the number of users in your organization.
4. **Test** essential elements, including MFA on desktop login, command line access RDP, VPN, networking infrastructure, as well as the ability to get insights into the full behavioral profile of key service accounts.
5. **Choose** the solution that best meets your needs and addresses all requirements

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 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	✓
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	✓

About Silverfort

Silverfort secures every dimension of identity. We are the first to deliver end-to-end identity security across the entire IAM infrastructure, eliminating gaps and blind spots, giving businesses visibility into their identity fabric and extending protection to resources that previously could not be protected. This is all done via a patented technology that natively integrates with your entire IAM infrastructure, Runtime Access Protection™ (RAP). It is lightweight, easy to use and deploy, and won't disrupt business operations, resulting in better security outcomes with less work. Discover every identity across every environment, analyze exposures to reduce your attack surface, and enforce security controls inline to stop lateral movement, ransomware propagation, and other identity threats.

To learn more, visit www.silverfort.com