SILVERFORT

Re-evaluate your MFA:

Are You as Protected as You Should Be?

Intro

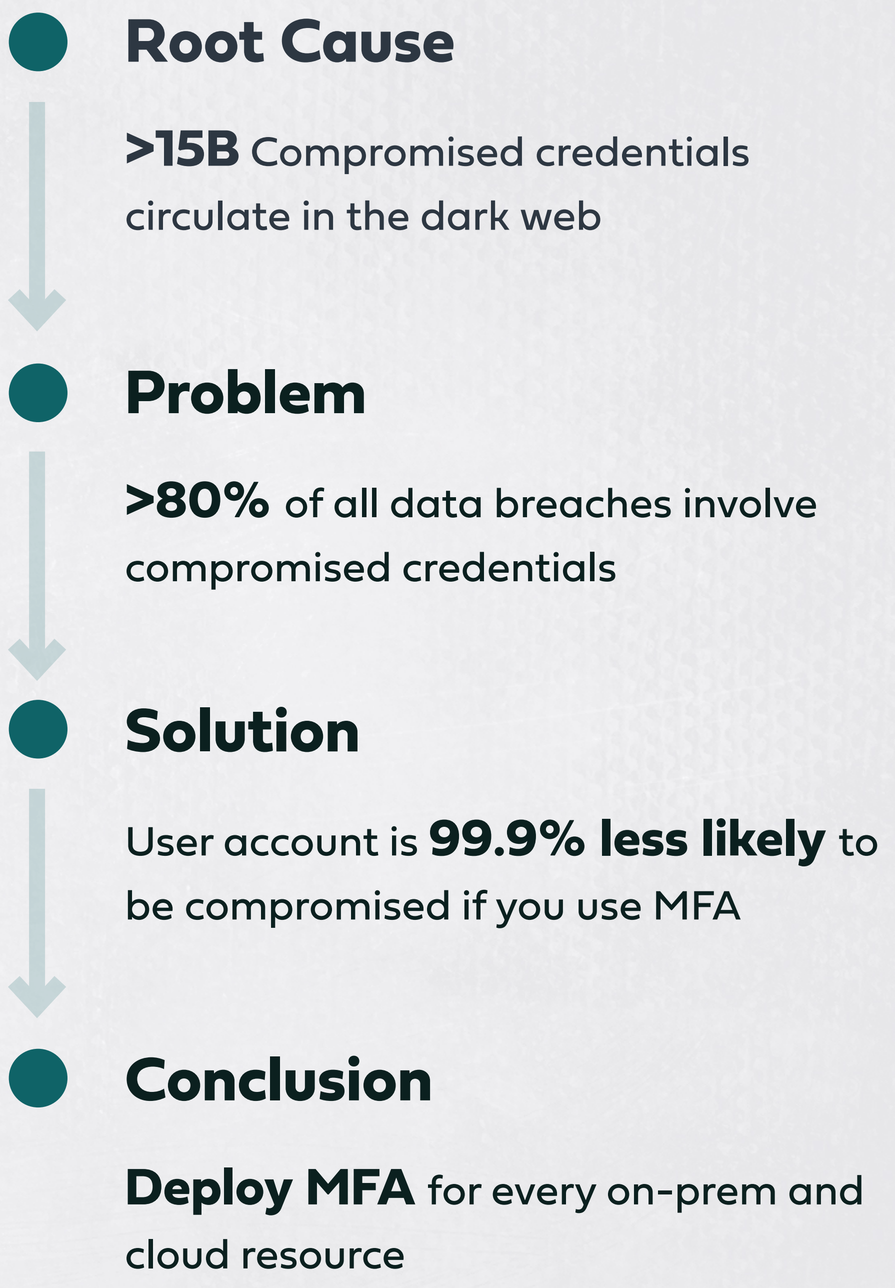
MFA protection is a key component in any organization's security stack. But do common MFA solutions and implementations truly deliver their expected security outcome? In this eBook we'll get to know why the importance of comprehensive MFA protection is increasing, gain insight into the top challenges current MFA solutions confront, and understand the common approaches that organizations implement today.

We'll then explore the new MFA approach introduced by the Silverfort Unified Identity Protection platform and understand how it fundamentally changes and elevates the scope of MFA protection, extending it to practically every sensitive resource within the hybrid organization. We'll conclude with an MFA checklist table that can assist you in assessing your existing protections and understanding your relative risk exposure.

Why is MFA more important than ever?

Identity-based attacks that utilize compromised credentials to access targeted resources are gaining momentum as the #1 cause of data breaches across both on-prem and cloud resources. MFA is the ultimate, proven solution to block such attacks. This leads to the inevitable conclusion that every resource that is accessed with credentials must be subject to MFA protection.

The problem, however, is that truly comprehensive MFA protection – one that covers all network assets - has been exceedingly difficult to achieve, and often isn't even attempted because it does not seem possible.



Root Cause

>15B Compromised credentials circulate in the dark web

Problem

>80% of all data breaches involve compromised credentials

Solution

User account is **99.9% less likely** to be compromised if you use MFA

Conclusion

Deploy MFA for every on-prem and cloud resource

MFA Challenge #1: Relying on Agents & Proxies

The dependency of MFA on either agents or proxies creates an inherent coverage problem

Traditional MFA solutions rely on either installing agents on protected machines, or on placing a proxy in front of a group of machines in a network segment. Both approaches inherently entail coverage gaps.

Agents

As a rule of thumb agents can never be deployed across 100% of the machines in a given environment. The larger the environment is, the more chances that there will be machines out of the deployment scope. Additionally, there are always machines you cannot install agents on due to various reasons.

Proxies

Gaining full MFA coverage using proxies requires placing a proxy in front of each and every network segment without any blind spots. This makes it practically an impossible task whenever the network topology exceeds the most basic levels of size and complexity.

The end result in both cases is partial coverage that leaves critical resources exposed to attack with compromised credentials without MFA protection.

MFA Challenge #2: Coverage Blind Spots

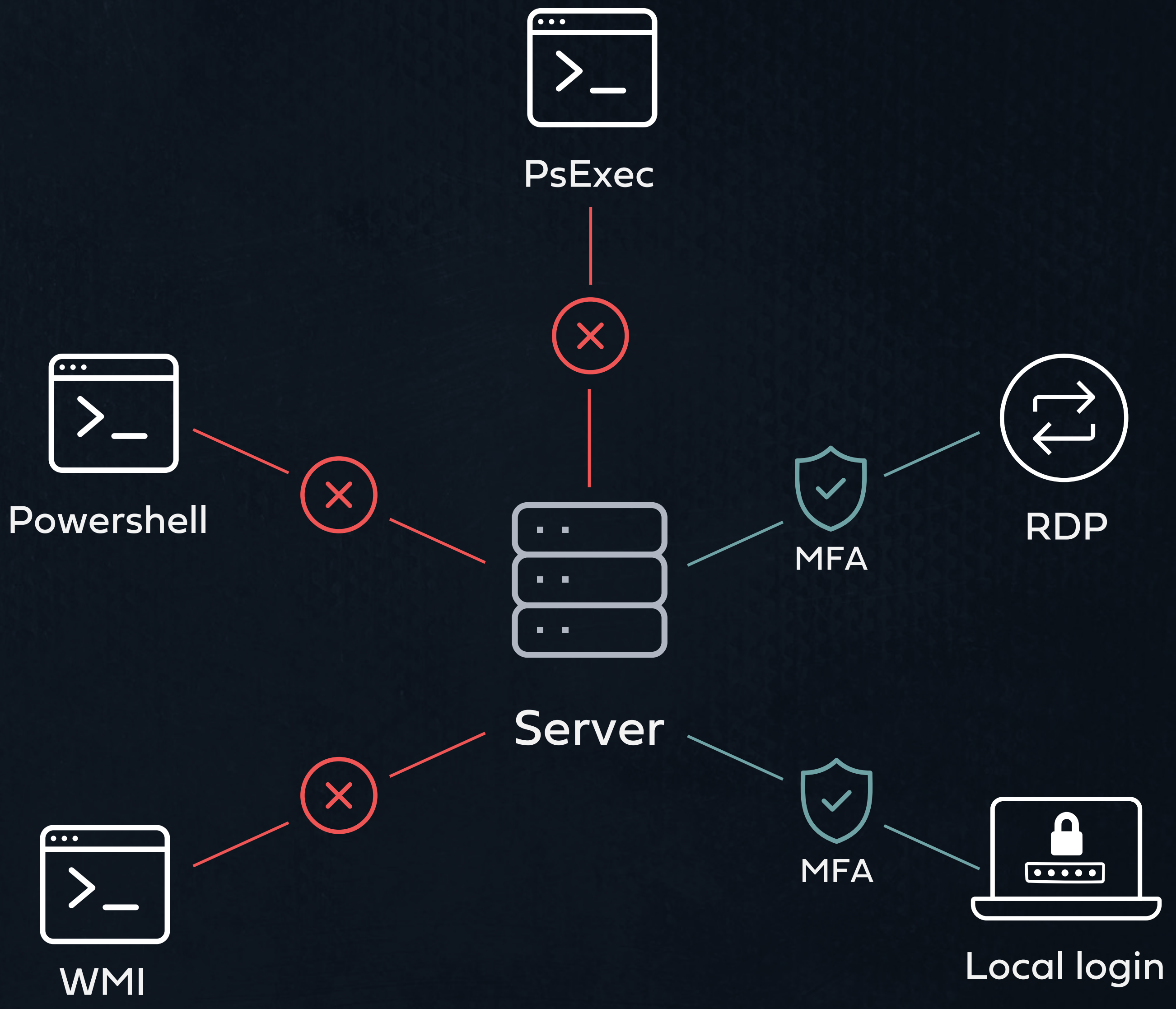
Common access interfaces to critical resources don't support standard MFA leaving them exposed to malicious access via compromised credentials

What are access interfaces?

Access interfaces are various alternatives users can use to access a resource. Different resources vary in the type and number of access interface that they support. For a SaaS application, the main access interface would be browser log in. On the other hand, in the cased of a server (either physical or virtual) many access interfaces are used – RDP, SSH, local login and others.

Why does it matter?

Current MFA solutions are not consistent in their access interfaces' coverage. While some access interfaces support MFA protection, others do not - including frequently used command line access tools such as CMD, remote PowerShell, WMI and others. Attackers intensively utilize these interfaces in lateral movement and ransomware attacks, and the inability to protect them with MFA creates a severe security weakness.



MFA Challenge #3: Fragmentation

Multiple types of network, on-prem and cloud resources, each requiring a dedicated MFA solution.

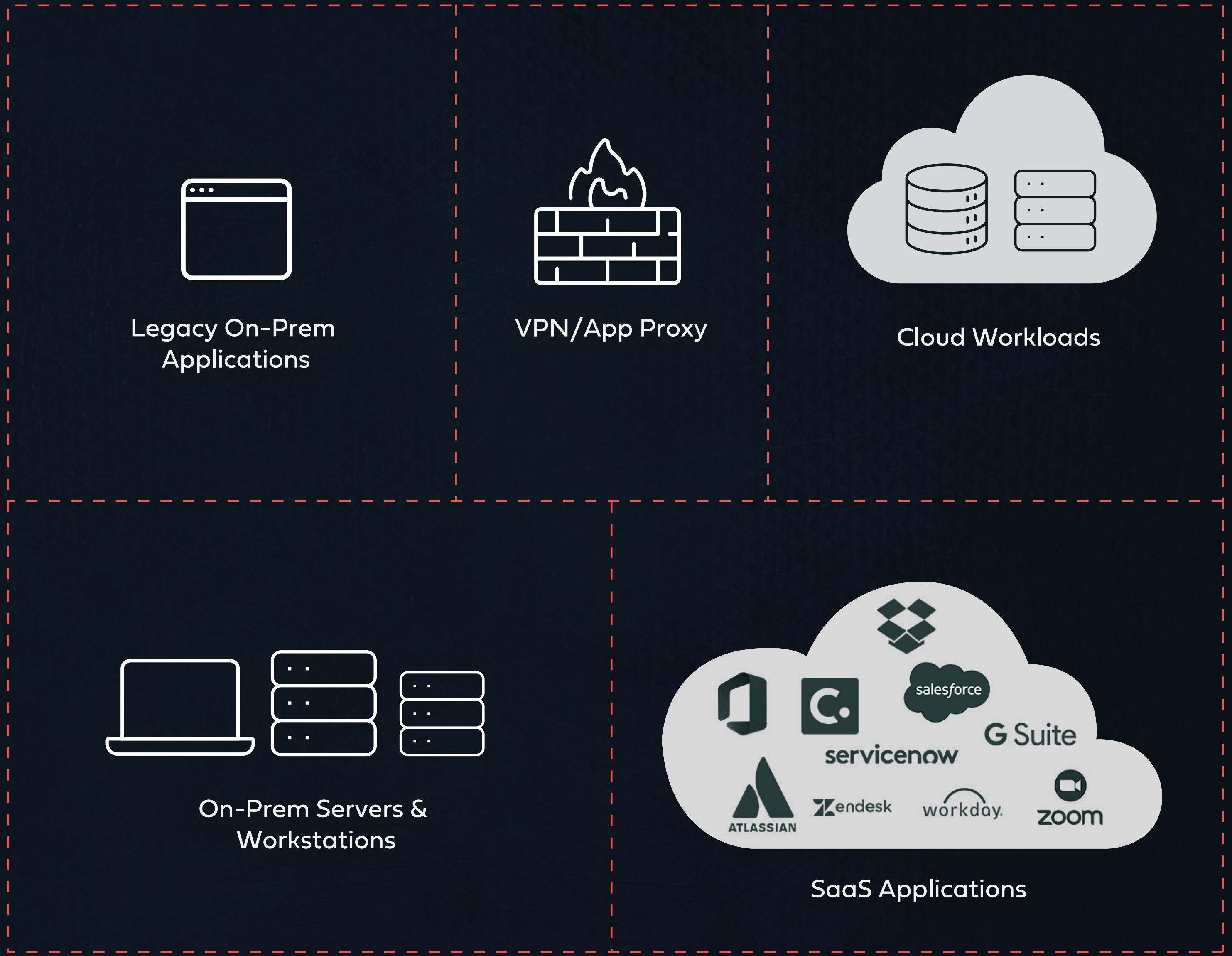
Today's IT environment is extremely versatile: VPN remote access, SaaS applications, RDP to on-prem machines, cloud workloads, and much more. Each of these often requires a different MFA solution (if more than one cloud IAM is used so there would also be a different MFA for each). The derived use of multiple MFA solutions entails operational complexities that directly degrades both:

User experience

Navigating through various products with different user interface is bound to create pushbacks from users and reduced coverage

Level of protection

Using several different products, each with different risk calculation logic makes it diffucult to maintain consistent protection level across all access policies



Legacy On-Prem Applications

VPN/App Proxy

Cloud Workloads

On-Prem Servers & Workstations

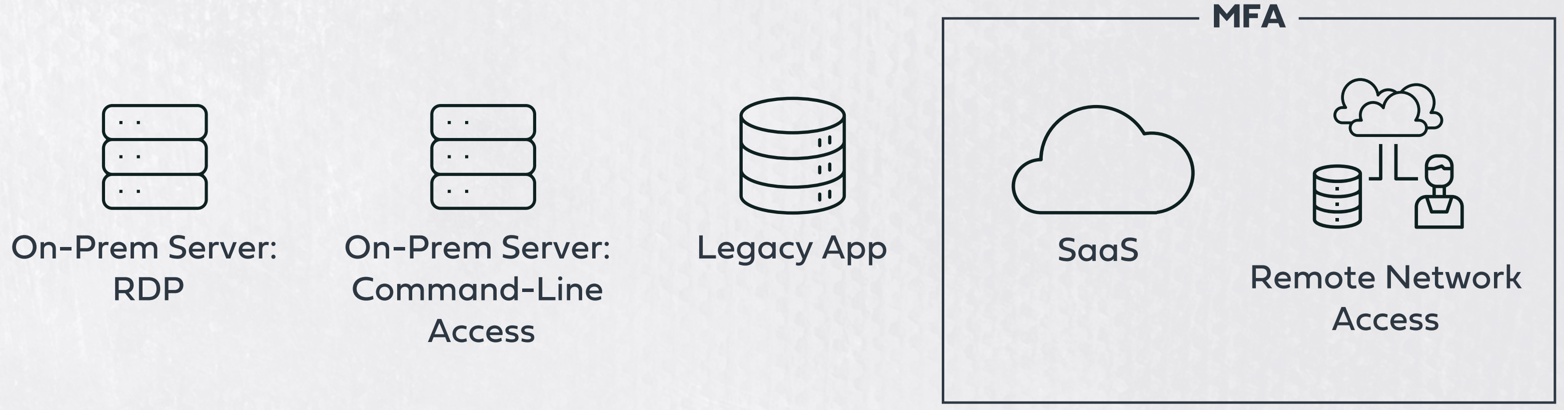
SaaS Applications

The Three Approaches to MFA

Organizations today have three main alternatives to confront the MFA challenges described above , with each approach featuring a different balance between security and operational considerations.

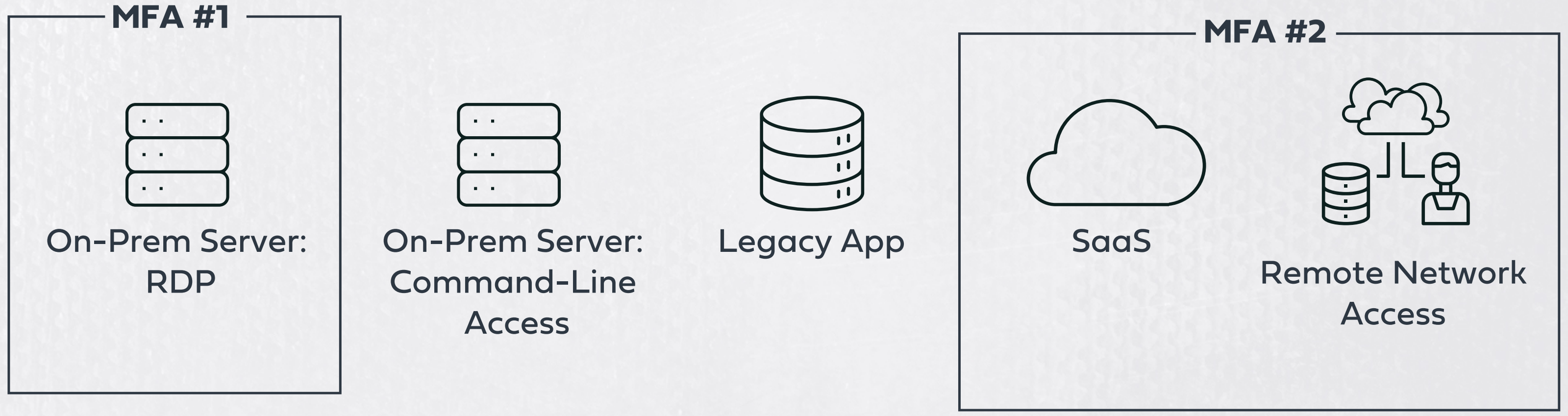
Single Solution

Simple to deploy but suffers from critical coverage gaps, enabling attackers to utilize compromised credentials and access resources.



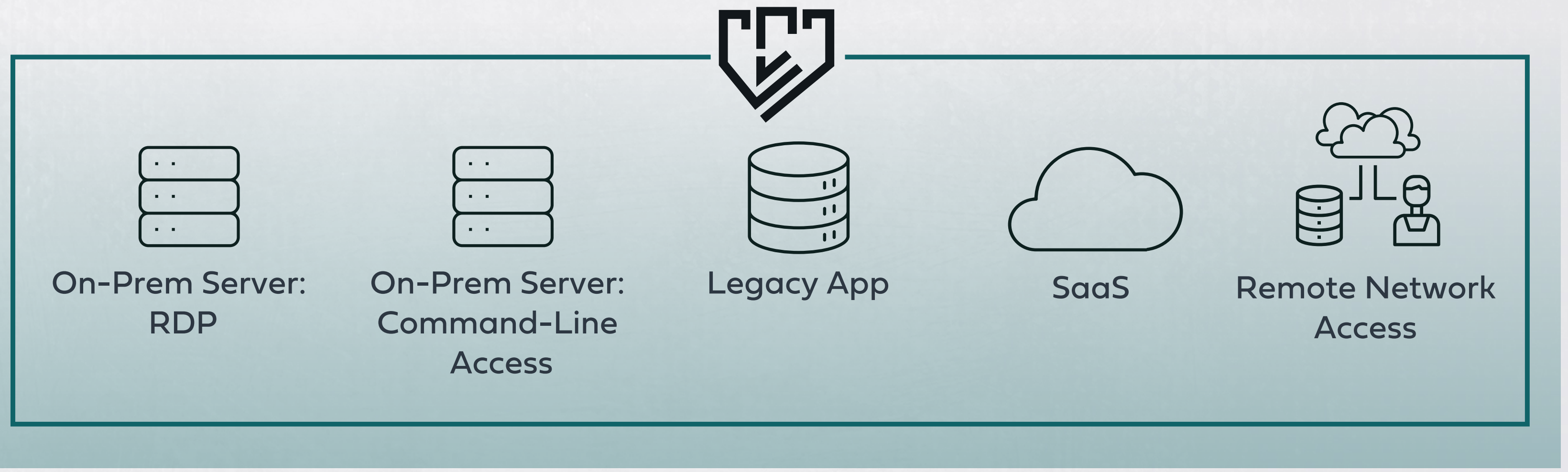
Multiple Solutions

Wider protection but complex to manage, resources without native MFA support are still exposed.



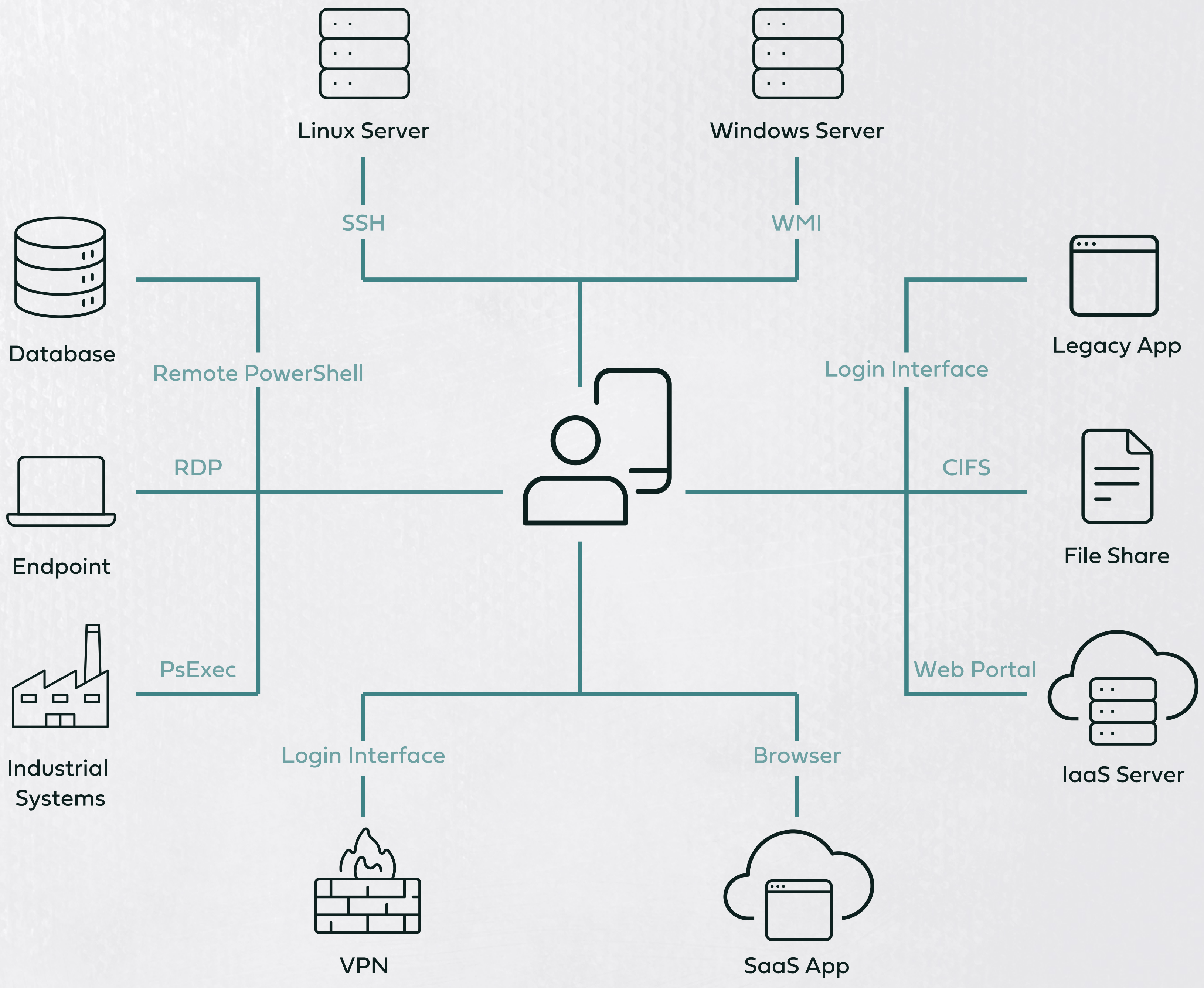
Unified Identity Protection Platform

Single solution covering all resources and access interfaces.



The Silverfort MFA Approach: Unified Identity Protection

Silverfort utilizes 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.



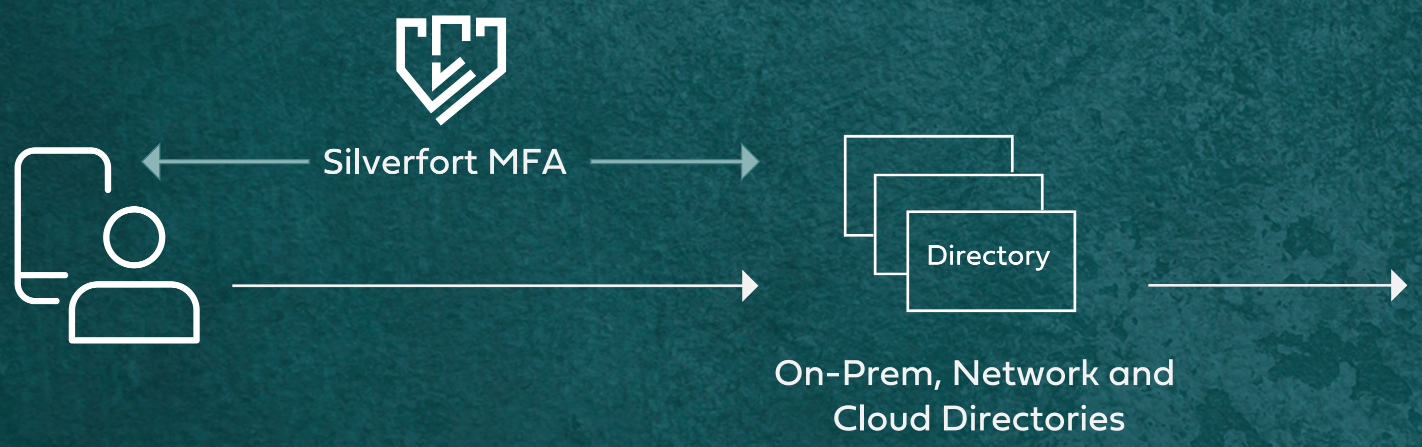
🟦 ACCESS INTERFACES ■ RESOURCES

Agentless and Proxyless Architecture to Protect all Resources

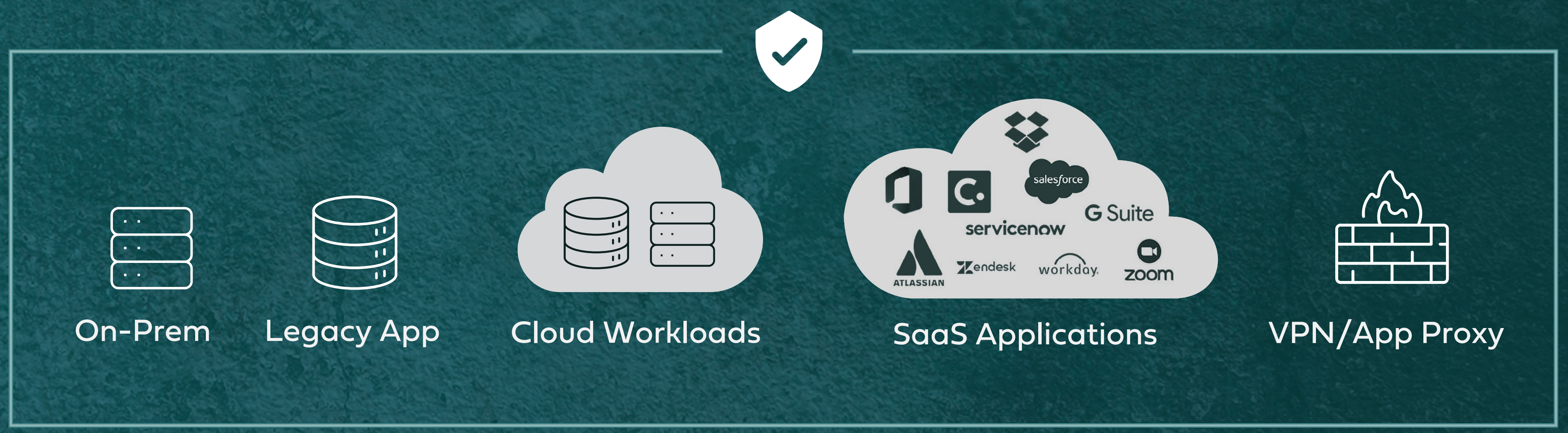
Unify MFA on both cloud and legacy identity providers.
Eliminate the need for agents or proxies.
Gain centralized protection for all resources.

Enforcing MFA from the backend of all identity providers rather than on the individual resource means that MFA is applied to any resource that authenticates to a directory, regardless if it is a SaaS application, on-prem server, legacy system or any other. Apart from the operational simplicity entailed in managing only one solution, this architecture eliminates the need for agents and proxies, enabling full MFA coverage across all network, on-prem, and cloud resources in the hybrid environment.

MFA VERIFICATION PROCESS



PROTECTION OF ALL ON-PREM AND CLOUD RESOURCES



How Does That Work in Practice? Verification Flow Example Zoom-In

Step-by-step walkthrough of Silverfort MFA for accessing on-prem server with remote Powershell in an Active Directory environment.

1 The user attempts to log in to a server with Powershell Enter-PSSession command.

2 Active Directory forwards the request to Silverfort.

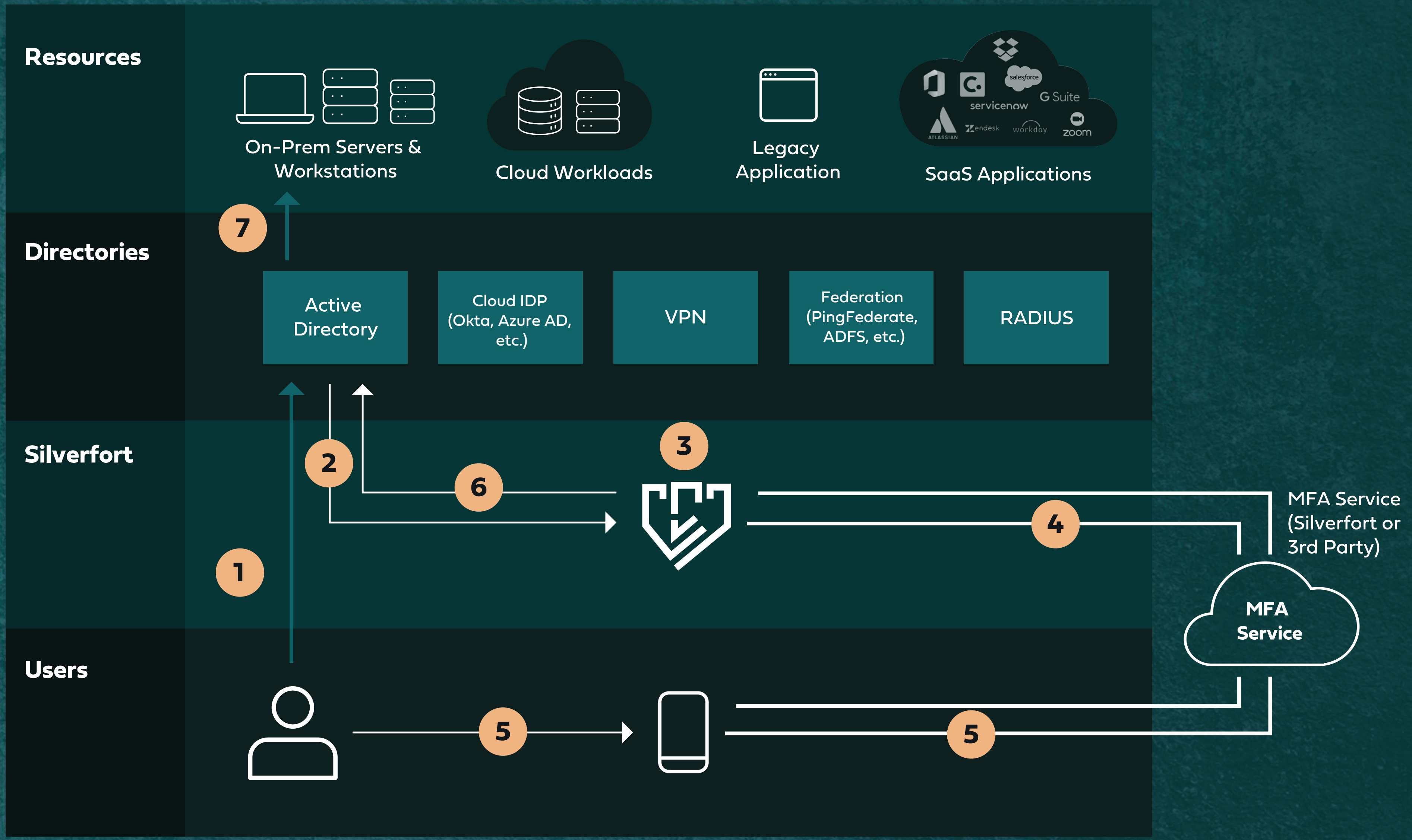
3 Silverfort analyzes the risk of the access request.

4 Based on access policy, Silverfort utilizes either its own or a 3rd party MFA service to verify the user's identity.

5 The user accepts the challenge and approves his/her identity.

6 Silverfort informs Active Directory that the user can be trusted to access the server.

7 Active Directory returns the response to the unaware client/server and grants the user access.

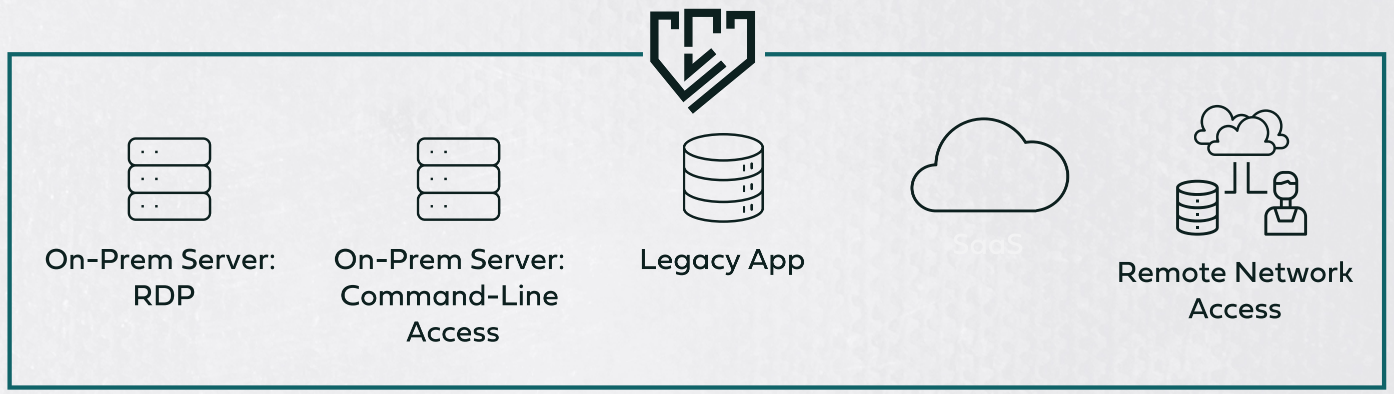


*A similar flow would apply upon attempting to access any other resource – the only change is the respective directory.

Choose the Silverfort MFA PATH that Aligns Best with your Needs

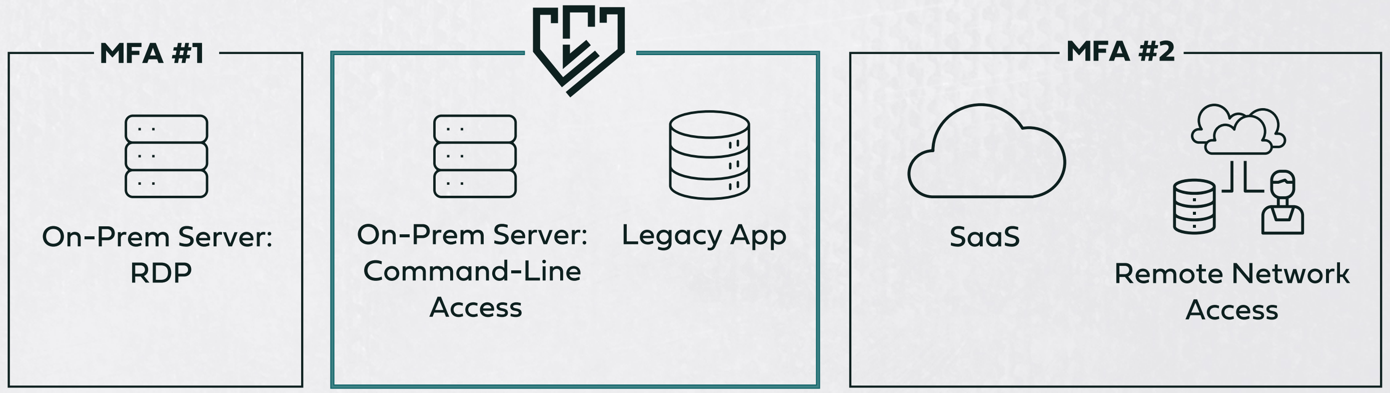
Replace

Use Silverfort MFA as the single MFA provider in the protected environment to protect all your on-prem and cloud resources. This provides both comprehensive protection and operational simplicity with a single interface to manage and configure all access policies to your resources without agents or proxies.



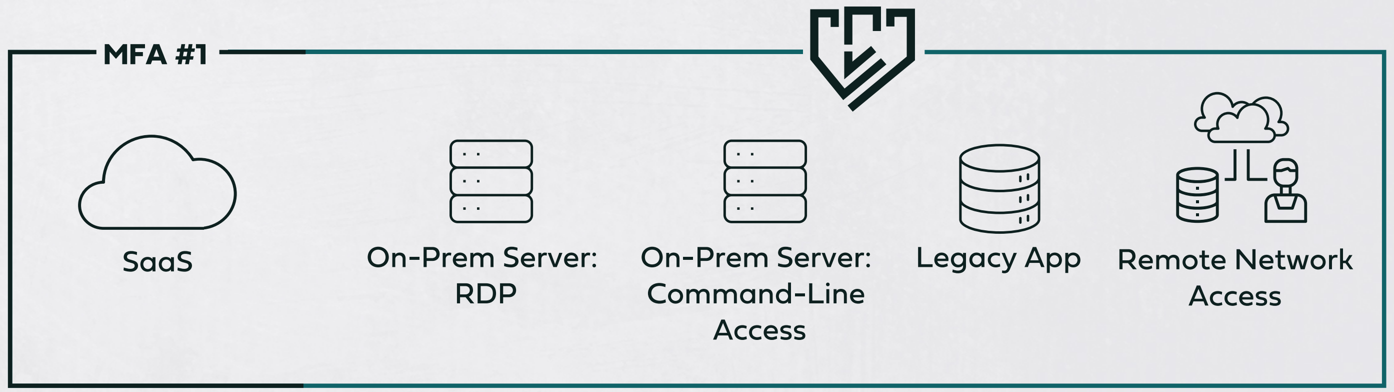
Add

Keep your existing solutions in place and implement Silverfort for the resources that couldn't have been protected before. While not reducing operational complexity, this would deliver immediate coverage to all the resources that are currently exposed and ensure end-to-end MFA protection in your environment.



Extend

Choose one of your MFA solutions as the prime provider and use Silverfort to augment your chosen solution's protection to all the resources it doesn't natively support. The common choice would be the MFA solution that already protects your SaaS applications. With this model, Silverfort would integrate with the current MFA service to challenge your users with MFA, providing them with consistent user experience regardless of what resource they attempt to access.



Assess your Protections

The Ultimate MFA protection checklist

The table below summarizes the main resources in your organization that are prime target for attackers utilizing compromised ceredentials and must be protected with MFA

Resource Type	Access Method	What's the Risk?	Do you have MFA protection?	Silverfort MFA
On-Prem Servers\Workstations	Local login	On-prem lateral movement, ransomware propagation		✓
	RDP/SSH	On-prem lateral movement, ransomware propagation		✓
	CMD/Remote Powershell/PsExec/etc.	On-prem lateral movement, ransomware propagation		✓
Legacy systems	Native login	Malicious access, data exfiltration		✓
Virtualization management (vSphere\vCenter\Hyper-V)	Login interface	Full control on all VMs in your environment		✓
Security and IT products' management consoles (Firewall, SIEM, EDR etc.)	Login interface	Downgrade of security level		✓
File Shares		On-prem lateral movement, ransomware propagation		✓
Databases		Malicious access, data exfiltration		✓
IaaS Instances	RDP/SSH	Account takover, lateral movement, data exfiltration		✓
SaaS apps	Web Login	Account takover, lateral movement, data exfiltration		✓
On-prem Web Apps		Malicious access, data exfiltration		✓
Remote Network Access (VPN)	VPN login interface	Malicious access to company intranet		✓
VDI\Citrix Sessions		Account takover, lateral movement, data exfiltration		✓
PAM	Web portal/PSM proxies	Attackers gaining access and control of privileged accounts		✓
Industrial Systems	Local\remote login	Sabotage systems, ransomware propagation		✓

About Silverfort

Silverfort has pioneered the first-ever Unified Identity Protection platform, which protects enterprises against identity-based attacks that utilize compromised credentials to access enterprise resources. Using innovative agentless and proxyless technology, Silverfort natively integrates with all existing IAM solutions, to extend secure access controls such as Risk-Based Authentication and MFA across all on-prem and cloud resources. This includes assets that could never have been protected in this way before, such as homegrown/legacy applications, IT infrastructure, file systems, command-line tools, machine-to-machine access, and more. Silverfort continuously monitors all access attempts by users and service accounts, and analyzes risks in real-time using an AI-based engine to enforce adaptive access policies.

To learn more, visit www.silverfort.com