Silverfort

Silverfort MFA: Protect the Unprotectable

Drill down into architecture and use cases

Scroll down

Foreword

Silverfort Identity Security platform provides MFA protection that can be easily applied across all users and resources in the hybrid enterprise environment, regardless of type, authentication protocol or access interface. This includes resources and access interfaces that could never have been subject to MFA protection before, including legacy applications, command-line access to workstations and servers, IT infrastructure and many others. T his white paper includes two parts:

This white paper includes two parts:

Silverfort MFA - How is it Different?
This section explains the core technology and architecture principles that enable Silverfort to extend MFA protection to all enterprise resources without blind spots.

Silverfort Use Cases This section includes various examples of common use cases that illustrate Silverfort's advantages over standard MFA solutions.

Enjoy your reading!

.

Part 1: Silverfort MFA - How is it Different?

The Security Challenges of Standard MFA Solution Standard

MFA solutions protect at the resource level. For example, if I want to protect a certain server with MFA, I install an MFA agent on it that would communicate with an MFA server whenever a user logs in to the server. Alternatively, I can also place a proxy in front of a group of servers to gain a similar result. One way or another, this approach entails the following issues:

Operational – The deployment, configuration and maintenance efforts rise in direct proportion to the number of resources I want to protect. The number of MFA solutions I need also increases in proportion to the type of resources I want to protect - SaaS apps, on-prem servers, networking infrastructure, etc.

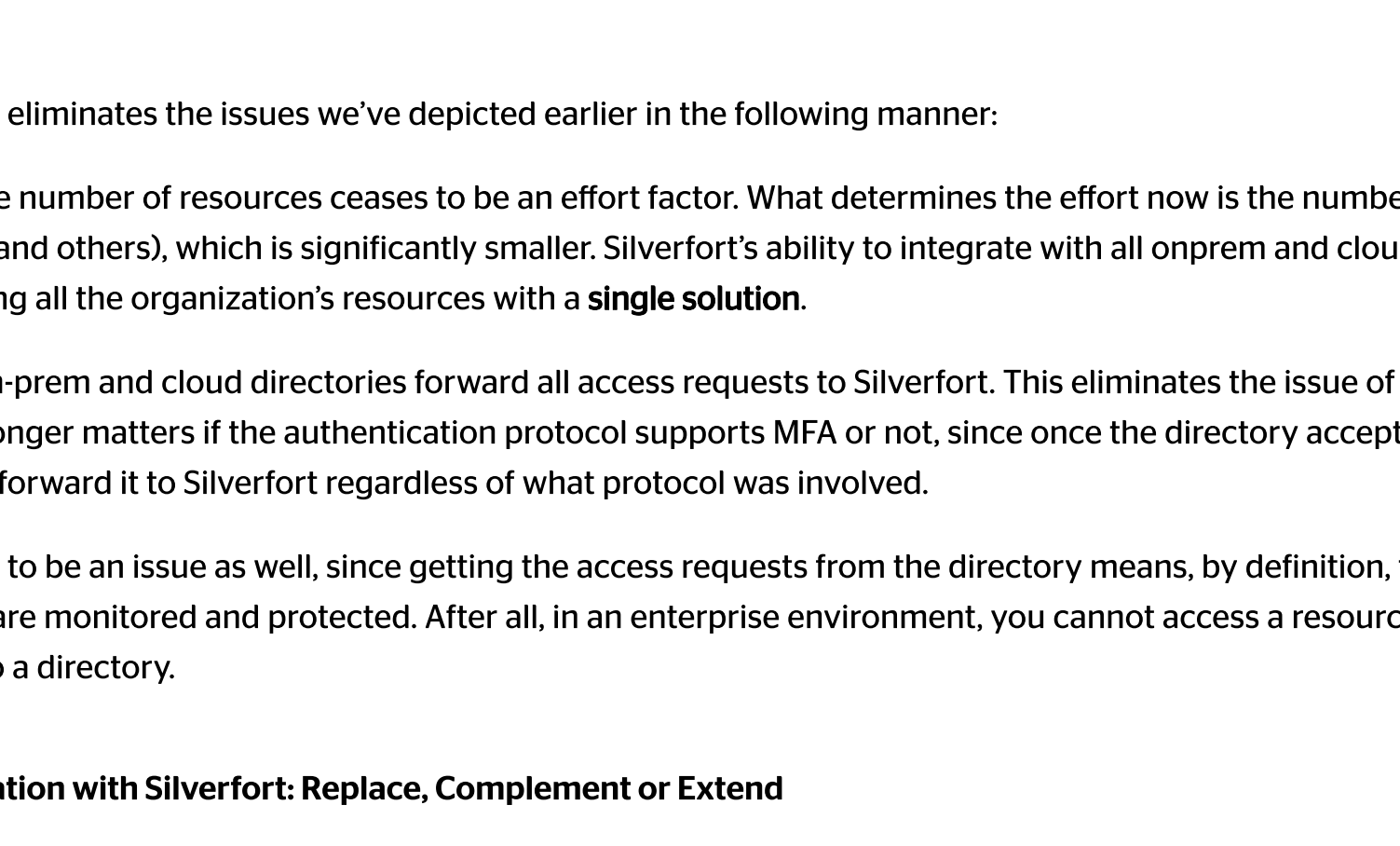
Security – Placing the MFA checkpoint at the resource level limits the protection coverage to authentication protocols that natively support MFA. Since core protocols such as Kerberos and NTLM don't support it, there is a significant gap in the MFA capability to secure all access to the resources that need protection.

Relying on agents and/or proxies would almost always result in some machines remaining unprotected. This would happen due to either an inability to perform agent installation or network complexity that would make complete coverage of all segments with proxies a nearly impossible task.

Silverfort MFA Technology and Architectural Change

Silverfort overcomes these inherent challenges by introducing a native integration with all the on-prem and cloud directories in the protected environment. For cloud directories such as Azure AD, Okta, etc. this is achieved via a dedicated API, while for Active Directory Silverfort utilizes a patented technology that enables it to read AD authentication traffic without needing to decrypt it. Let's illustrate Silverfort's protection flow with an Active Directory authentication. The numbers in the sentences refer to the flow in Figure 1 below.

.



This architecture eliminates the issues we've depicted earlier in the following manner:

Operational – The number of resources ceases to be an effort factor. What determines the effort now is the number of directories (DCs and others), which is significantly smaller. Silverfort's ability to integrate with all onprem and cloud directories enables protecting all the organization's resources with a **single solution**.

Security – The on-prem and cloud directories forward all access requests to Silverfort. This eliminates the issue of the protocols. It no longer matters if the authentication protocol supports MFA or not, since once the directory accepts the access request it would forward it to Silverfort regardless of what protocol was involved.

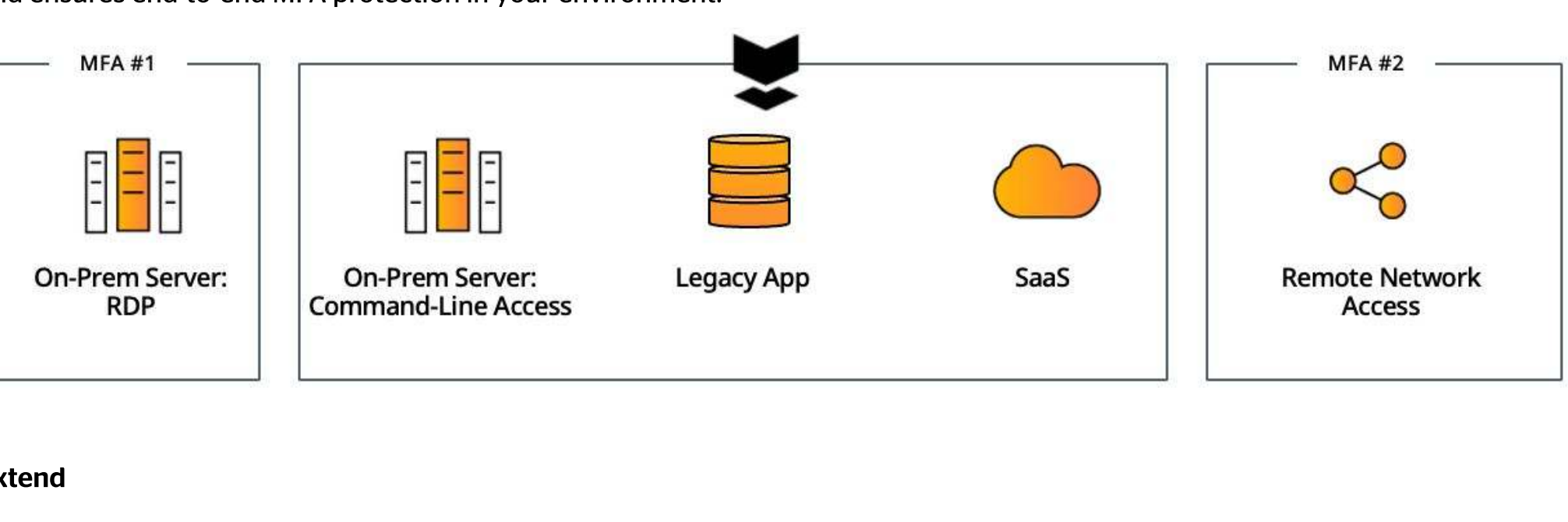
Coverage ceases to be an issue as well, since getting the access requests from the directory means, by definition, that all authentications are monitored and protected. After all, in an enterprise environment, you cannot access a resource without authenticating to a directory.

The MFA Application with Silverfort: Replace, Complement or Extend

In terms of the actual MFA application to use, there are three operation modes that Silverfort supports:

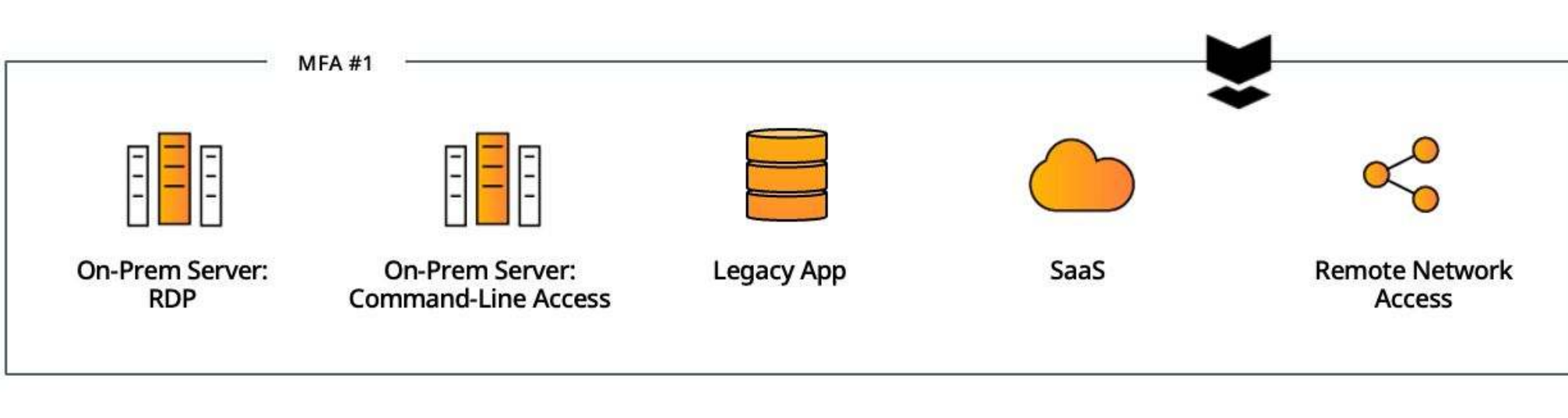
Replace

Use Silverfort as the single MFA solution in your environment for all 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.



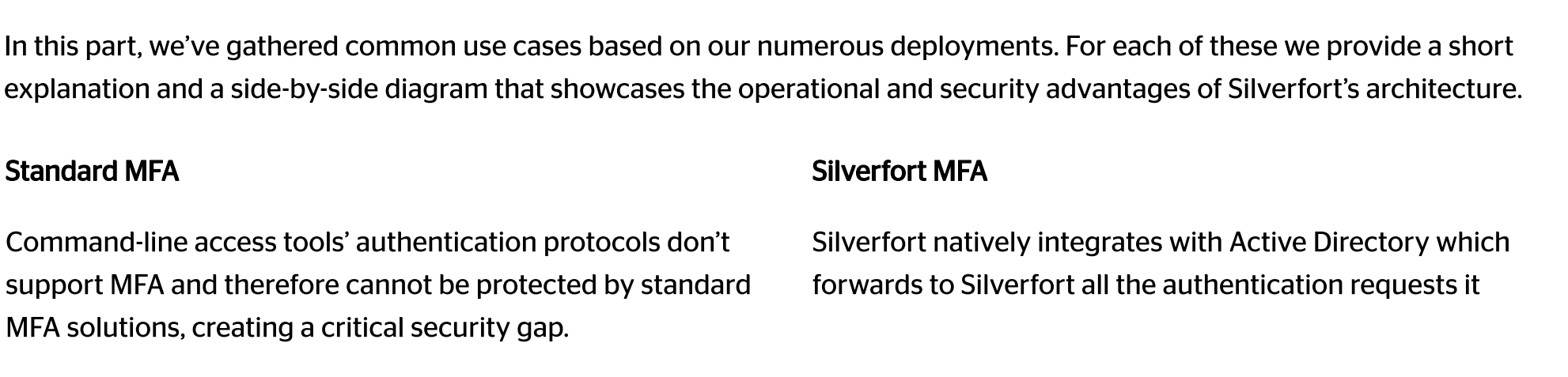
Complement

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 delivers immediate coverage to all the resources that are currently exposed and ensures 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 a consistent user experience regardless of what resource they attempt to access.



Part 2: Common Use Cases

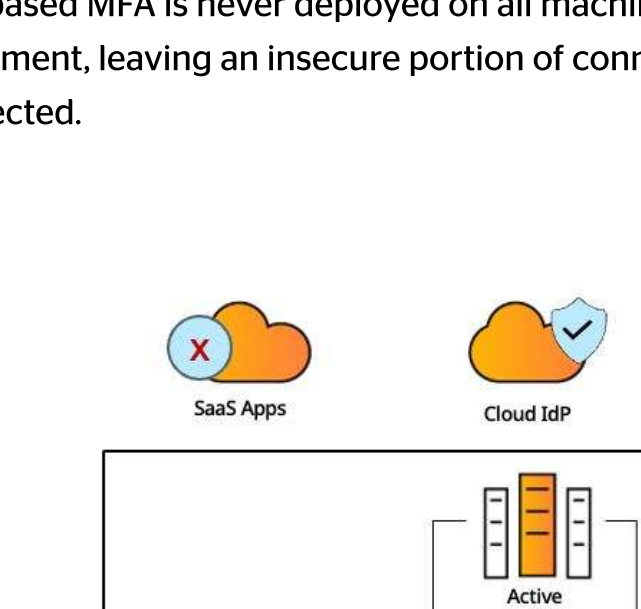
In this part, we've gathered common use cases based on our numerous deployments. For each of these we provide a short explanation and a side-by-side diagram that showcases the operational and security advantages of Silverfort's architecture.

#1 - Command-Line Admin Tools

In this part, we've gathered common use cases based on our numerous deployments. For each of these we provide a short explanation and a side-by-side diagram that showcases the operational and security advantages of Silverfort's architecture.

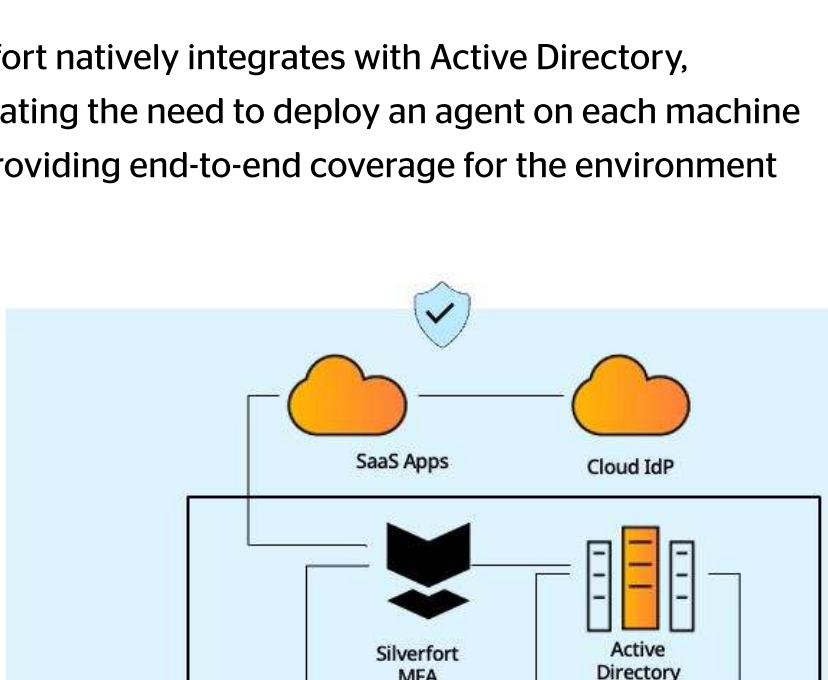
Standard MFA

Command-line access tools' authentication protocols don't support MFA and therefore cannot be protected by standard MFA solutions, creating a critical security gap.



Silverfort MFA

Silverfort natively integrates with Active Directory which forwards to Silverfort all the authentication requests it receives for risk analysis and MFA protocol..

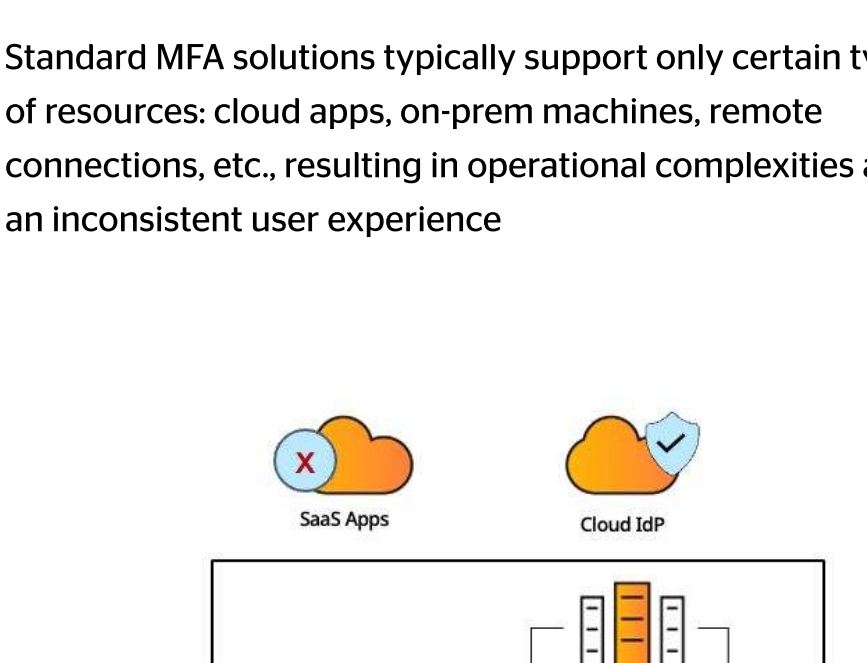


#2- Remote Desktop Protocol (RDP)

RDP is the default UI-based remote connection tool. Since the vast shift to working from home, it has become a common access method not only for IT admins but also for everyday users as well, making MFA protection a necessity.

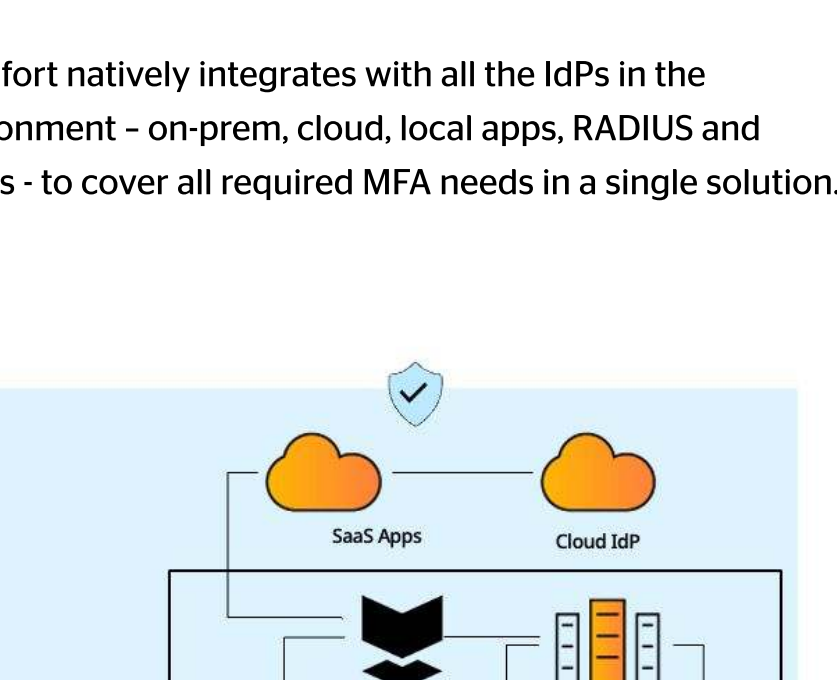
Standard MFA

Agent-based MFA is never deployed on all machines in the environment, leaving an insecure portion of connections unprotected.



Silverfort MFA

Silverfort natively integrates with Active Directory, eliminating the need to deploy an agent on each machine and providing end-to-end coverage for the environment

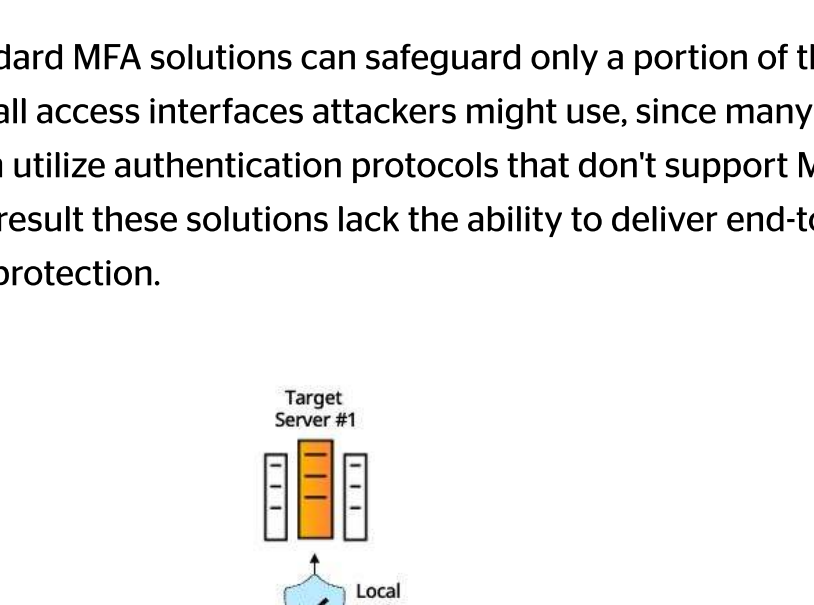


#3 - Hybrid Environment

Organizations today feature hybrid environments with various types of resources requiring MFA protection. Consistent user experience and operational efficiency are imperative to maximize MFA's security potential.

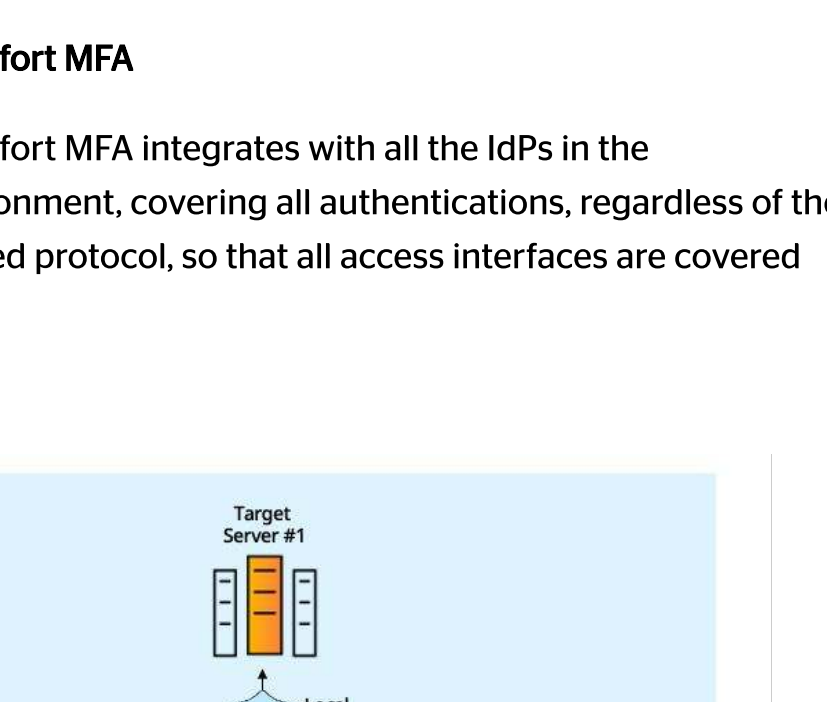
Standard MFA

Standard MFA solutions typically support only certain types of resources: cloud apps, on-prem machines, remote connections, etc., resulting in operational complexities and an inconsistent user experience



Silverfort MFA

Silverfort natively integrates with all the IdPs in the environment – on-prem, cloud, local apps, RADIUS and others - to cover all required MFA needs in a single solution.

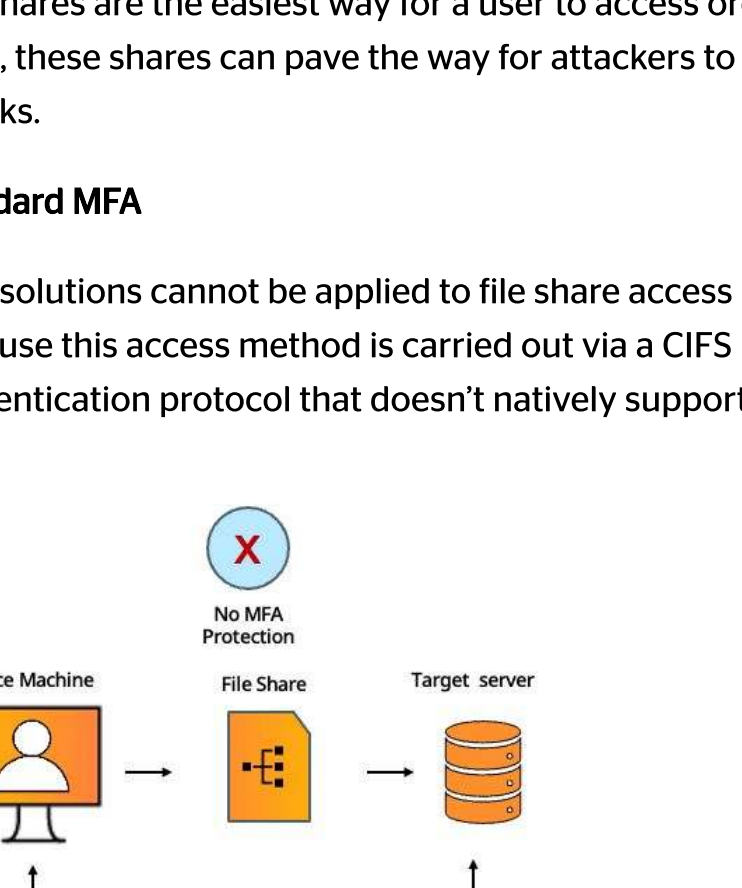


#4 - Internal & External Admin Access

Admin accounts are threat actors' prime targets and therefore should be carefully secured against a compromised credentials scenario, across all access interfaces they typically use

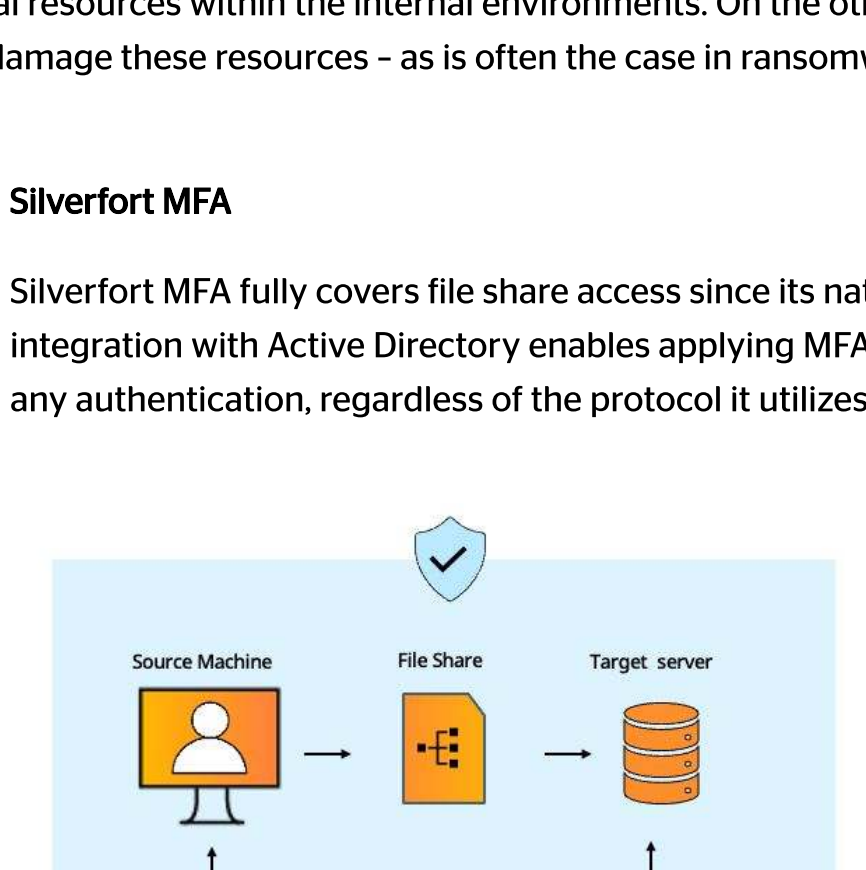
Standard MFA

Standard MFA solutions can safeguard only a portion of the overall access interfaces attackers might use, since many of them utilize authentication protocols that don't support MFA. As a result these solutions lack the ability to deliver end-to-end protection.



Silverfort MFA

Silverfort MFA integrates with all the IdPs in the environment, covering all authentications, regardless of the utilized protocol, so that all access interfaces are covered

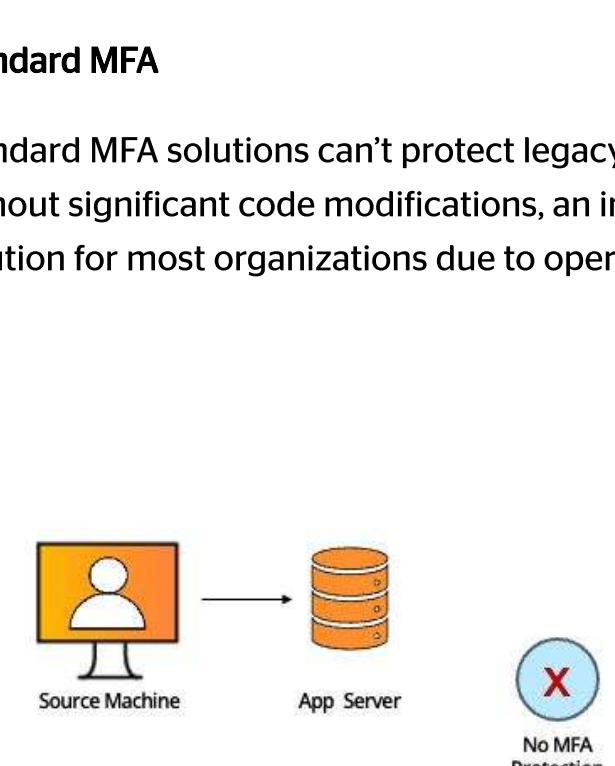


#5 - File Shares

File shares are the easiest way for a user to access organizational resources within the internal environments. On the other hand, these shares can pave the way for attackers to access or damage these resources – as is often the case in ransomware attacks.

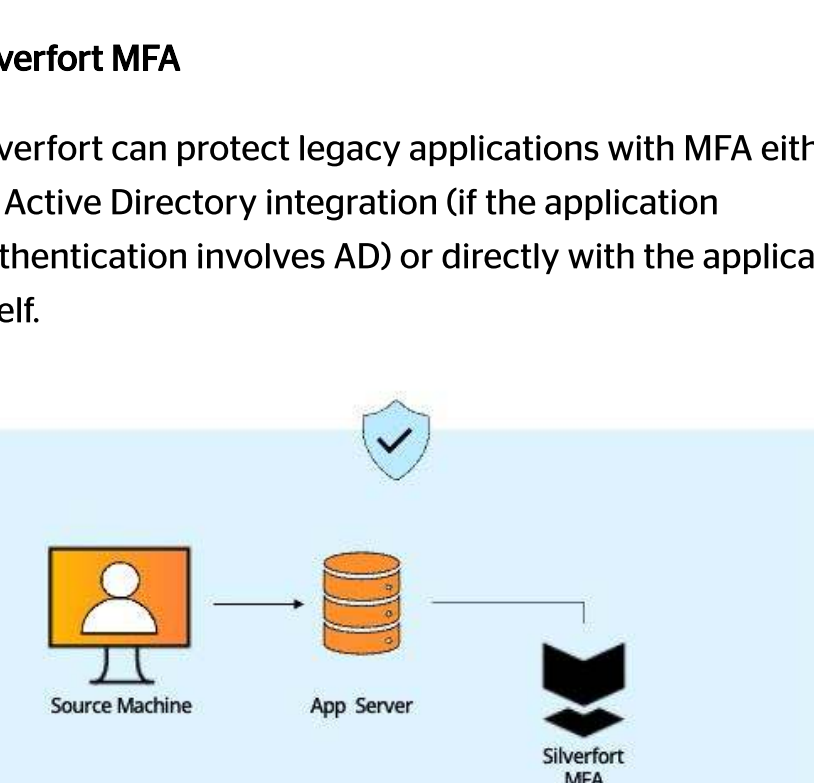
Standard MFA

MFA solutions cannot be applied to file share access because this access method is carried out via a CIFS authentication protocol that doesn't natively support MFA.



Silverfort MFA

Silverfort MFA fully covers file share access since its native integration with Active Directory enables applying MFA to any authentication, regardless of the protocol it utilizes

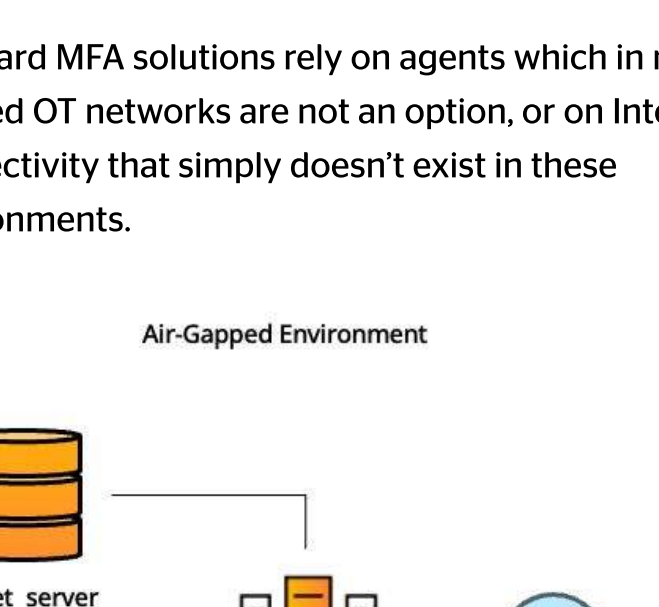


#6 - Legacy Applications

Legacy applications support core business and production processes in many companies. In many cases, these applications were written before modern MFA was available and as a result cannot be subject to the protection MFA renders.

Standard MFA

Standard MFA solutions can't protect legacy applications without significant code modifications, an impractical solution for most organizations due to operational concerns.



Silverfort MFA

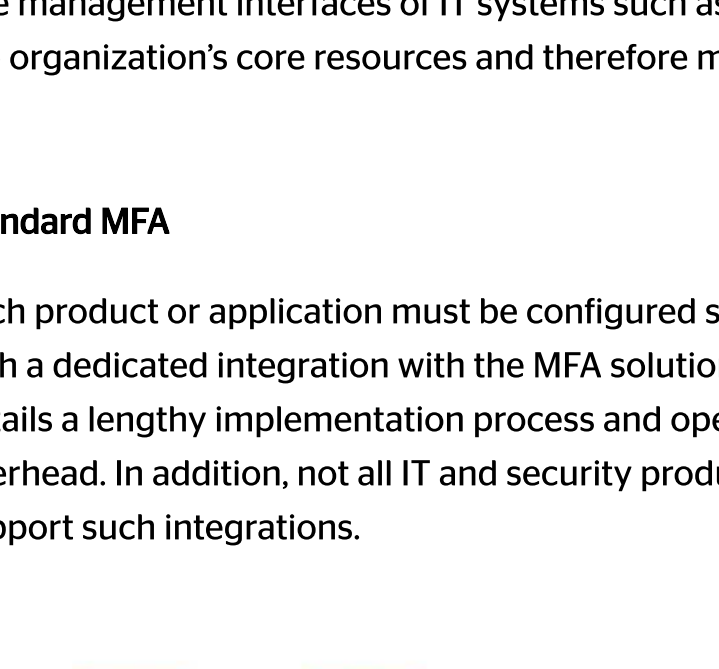
Silverfort can protect legacy applications with MFA either via its Active Directory integration (if the application authentication involves AD) or directly with the application itself.

#7 - Air-Gapped Active Directory Environments

Many organizations have Active Directory in their air-gapped networks – whether at OT networks that require separation from the IT network Prominent examples are OT networks as well verticals with hardened security requirements such as Government, Finance etc.

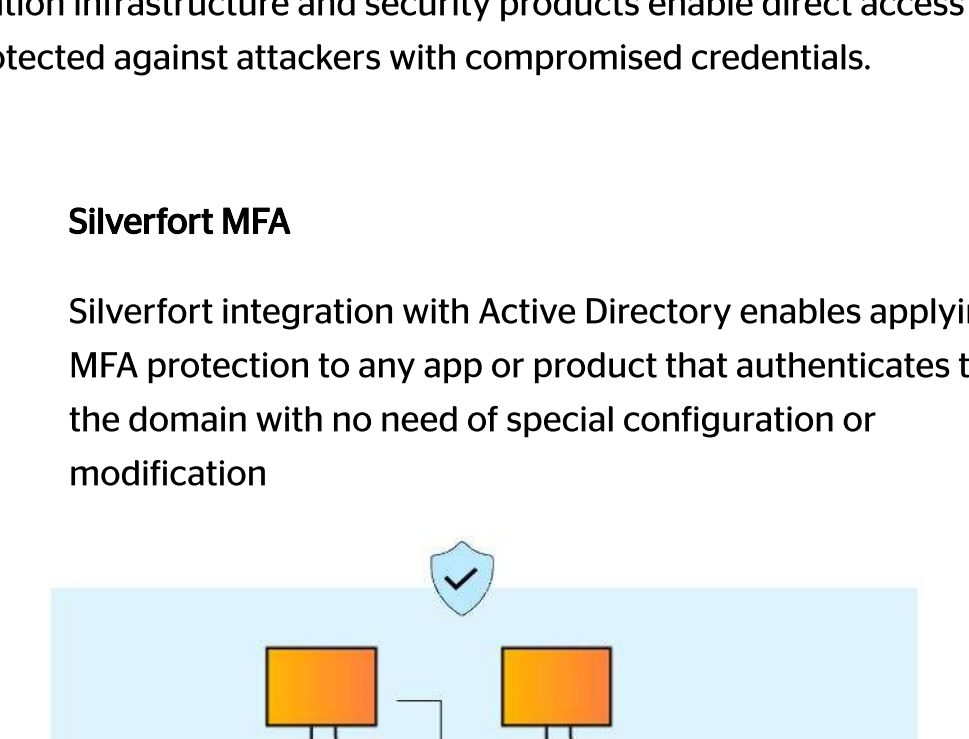
Standard MFA

Standard MFA solutions rely on agents which in many air-gapped OT networks are not an option, or on Internet connectivity that simply doesn't exist in these environments.



Silverfort MFA

Silverfort doesn't require installation of agents and can be fully operated without network connectivity by using FIDO2 hardware tokens.

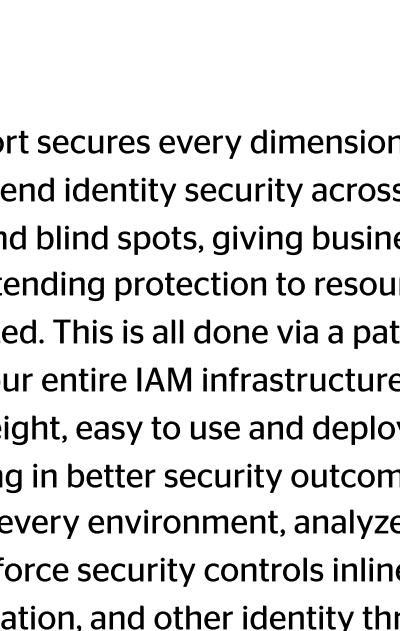


#8 - IT Infrastructure

The management interfaces of IT systems such as virtualization infrastructure and security products enable direct access into the organization's core resources and therefore must be protected against attackers with compromised credentials.

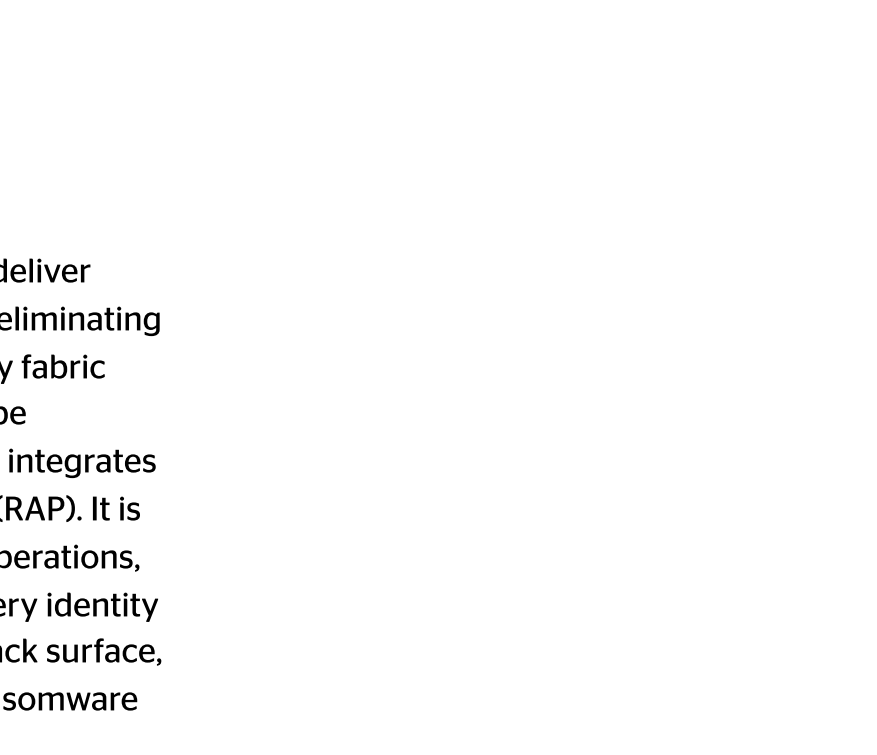
Standard MFA

Each product or application must be configured separately with a dedicated integration with the MFA solution, which entails a lengthy implementation process and operational overhead. In addition, not all IT and security products support such integrations.



Silverfort MFA

Silverfort integration with Active Directory enables applying MFA protection to any app or product that authenticates to the domain with no need of special configuration or modification



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