Silverfort

CASE STUDY

Leading telecom provider extends MFA protection to custom legacy applications

BASED

Southeast Asia

INDUSTRY

Telecom

USERS

15,000+

ENVIRONMENT

13,000 Servers
22 Domain controllers
15 Core on-prem homegrown applications

THE CHALLENGE:

The telecom provider needed to apply end-to-end multifactor authentication (MFA) protection to their custom legacy telecom applications.

Executive summary

The telecommunications industry keeps the world interconnected. Telecom providers build, operate, and manage complex network infrastructures which store vast amounts of sensitive data. This makes them a top target for malicious actors. The sector has seen a 51% rise in the number of attacks in 2022 making it the third most targeted sector. One of the main motives of malicious actors launching attacks on the telecom providers sector is that a successful data breach can provide access to data on millions of customers.

In many successful attacks on the telecom industry, compromised credentials are used to access enterprise resources by malicious actors. In fact, nearly 80% of data breaches are caused by compromised credentials. While real-time protection exists against various attack types – malware, data access, and data exfiltration to name a few – it is absent when attackers authenticate with valid but compromised credentials. This is especially true when it comes to protecting legacy applications against identity-based attacks.

A key challenge for telecoms is the use of custom or homegrown applications that don't natively support MFA protection. To integrate MFA coverage into legacy applications, organizations would need to make changes to the application's code which could disrupt their operational continuity. This lack of identity protection makes it extremely difficult for organizations to secure their users' access requests to their legacy applications.

This case study is about how a leading telecom provider partnered with Silverfort to gain real-time identity protection and visibility into their user access and authentication requests. You will learn about their identity protection challenges, the protection needed, and their positive experience using the Silverfort platform.

CUSTOMER OVERVIEW

About

An international telecommunications provider headquartered in Southeast Asia and operating in over 20 countries. It offers internet service provision, mobile phone networks, and fixed-line telephone services, as well as services such as data and internet solutions, information technology, engineering, and more.

Environment

The telecommunications provider operates with 15 core business homegrown legacy applications integrated throughout its organization. Their suite of legacy applications was developed specifically for their telecommunication needs. One prominent example is their custom CRM system used across the company, enabling employees to access customer data. There are two categories of users accessing these applications regularly: internal users (comprising support teams, IT personnel, and other staff members) and external users from third-party vendors.

Why now

The telecom provider needed to apply end-to-end multi-factor authentication (MFA) protection to their custom legacy telecom applications. When their employees requested access to view customer data from an application, there was no process in place to verify the user.

Finding the right partner

Due to the many identity protection challenges and the awareness of their evolving threat landscape, the telecom's security team sought a solution that would provide them with advanced MFA protection capabilities, complete visibility, and security into their user and authentication requests across their environments. The telecom provider examined several identity security offerings before deciding on the Silverfort platform, which they felt was the best option to solve their MFA protection needs. The deployment of Silverfort was a smooth month-long process where they enrolled over 15,000 employees with proper MFA protection.

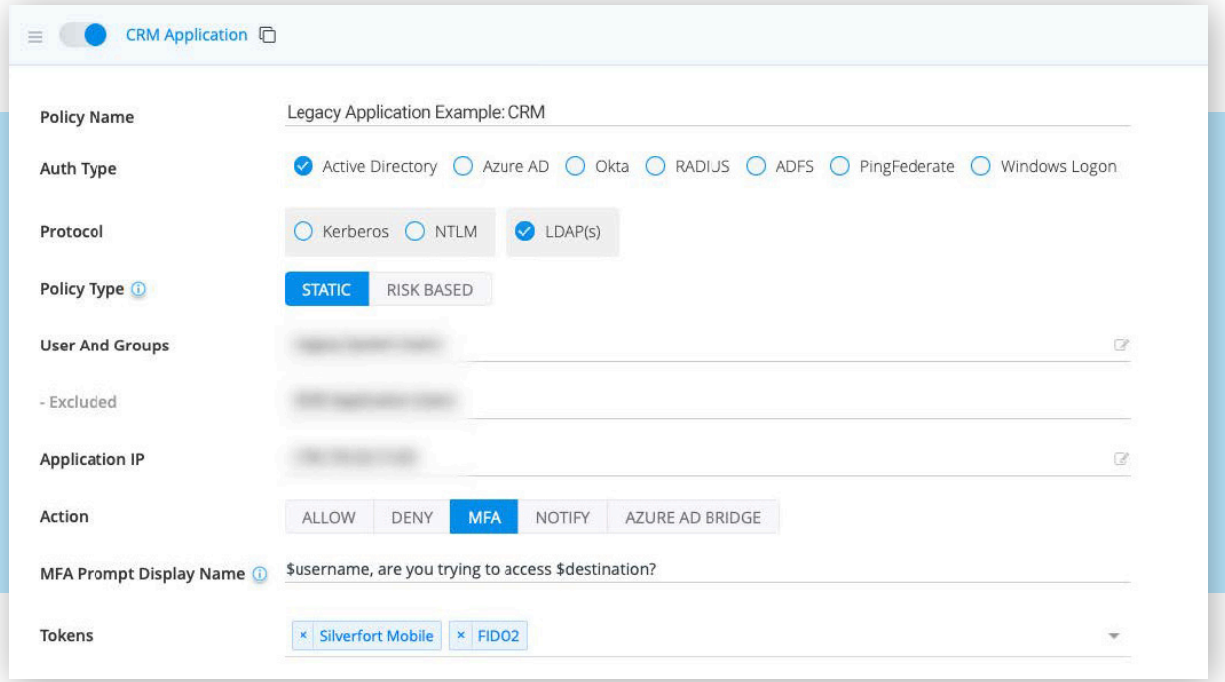
Challenge 1: Protect telecom legacy apps that don't support MFA

Lack of user authentication to custom CRM application

The telecom provider has many different stores across Southeast Asia. Their sales teams need to gain access to customer data regularly through their custom-built customer relations management (CRM) application, which runs through an LDAP protocol. When an employee at their store requests access to the CRM, they would not be verified with MFA. This gap in proper security controls for user authentication made the telecom provider realize that the sensitive data in their CRM and their employees were at risk of being targeted in potential identity-based attacks. This new security challenge became a top security priority due to the telecom's critical importance in securing all its environments and resources with multi-factor authentication (MFA).

Smooth authentication process across environments

The telecom provider deployed the Silverfort platform on 22 domain controllers and implemented seven MFA access policies to ensure their users will be able to verify their identity with MFA. After fully implementing Silverfort into their production environment, the telecom provider achieved full MFA protection while gaining complete visibility and real-time monitoring of all their user authentication requests. When users are trying to gain access to their custom CRM application, they are now required to be verified with Silverfort's MFA or via Silverfort's integration with Yubico during the login process. The telecom provider is using over 1,000 Yubico keys to authenticate their users via Silverfort native integration. This has allowed their employees to have a seamless authentication process while safely gaining access to customer data from their CRM application.



The telecom provider's business application is an LDAP protocol policy that requires all access requests to LDAP-based applications to be verified with MFA. During LDAP authentications, they see which application they trying to access and the IP address of users.

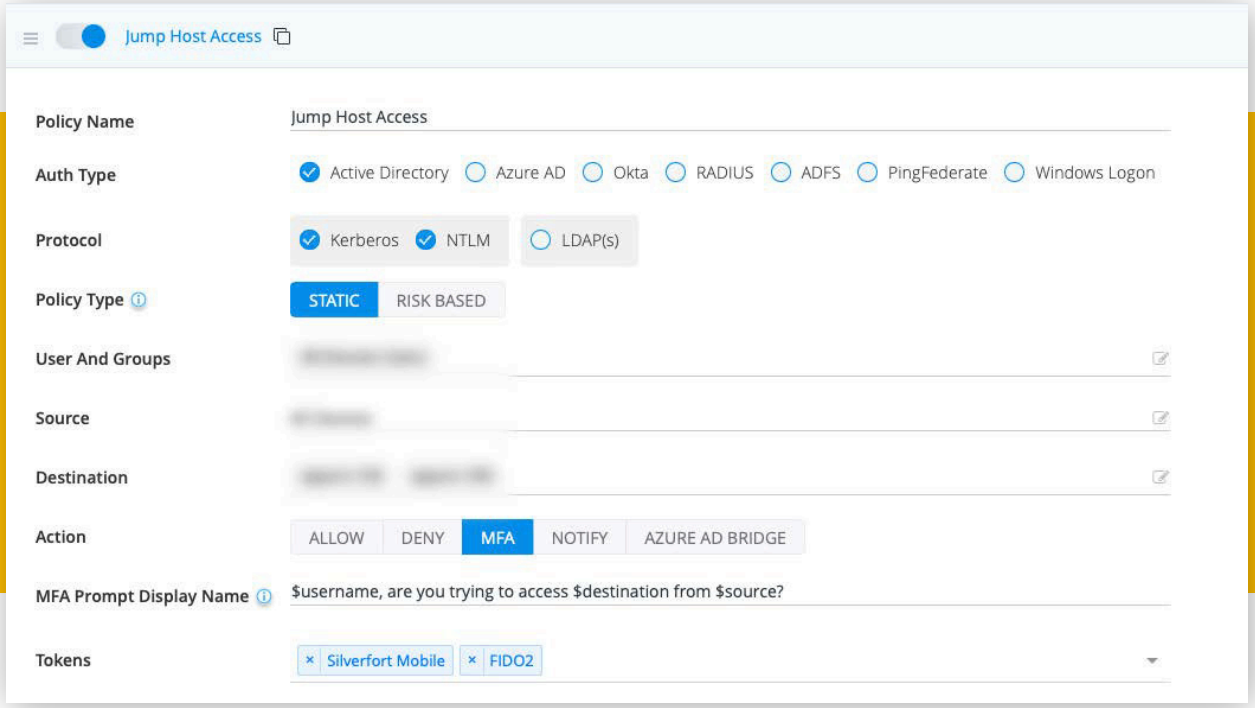
Challenge 2: Enforce MFA to users without a mobile device

Support team users need to be authenticated

The telecom provider's customer support team works in offices where the employees are not allowed to bring any mobile devices. Their customer support team needs to gain access to the telecom provider's support applications which are only accessible in these secured offices. This created major operations and security challenges. Without the option of bringing devices into the customer support room, they needed to find an alternative solution to provide secure access to every member of their customer support team. With many of the traditional MFA solutions not being able to authenticate this type of use case and users, they were not an option. This forced the telecom provider to get creative.

Clean room users authenticated with FIDO2 keys

To solve the challenge of authenticating employees who are not near their devices, Silverfort enabled the telecom provider's customer support team to be verified when working in the support offices by deploying Silverfort's integration with Yubico keys. The initial pairing process for each Yubico key with Silverfort was very straightforward as their keys were paired and ready to use pretty quickly. Once integrated with Silverfort, when a customer support member needs to be authenticated to gain access to one of the customer support applications, they would need to bring a Yubico key to verify their identity.



The jump host access policy is used by the telecom provider user's admin to access the Windows servers through a Windows jump host. Once gaining access to the jump host, users will need to verify their identity with YubiKeys before gaining access to the customer support resources.

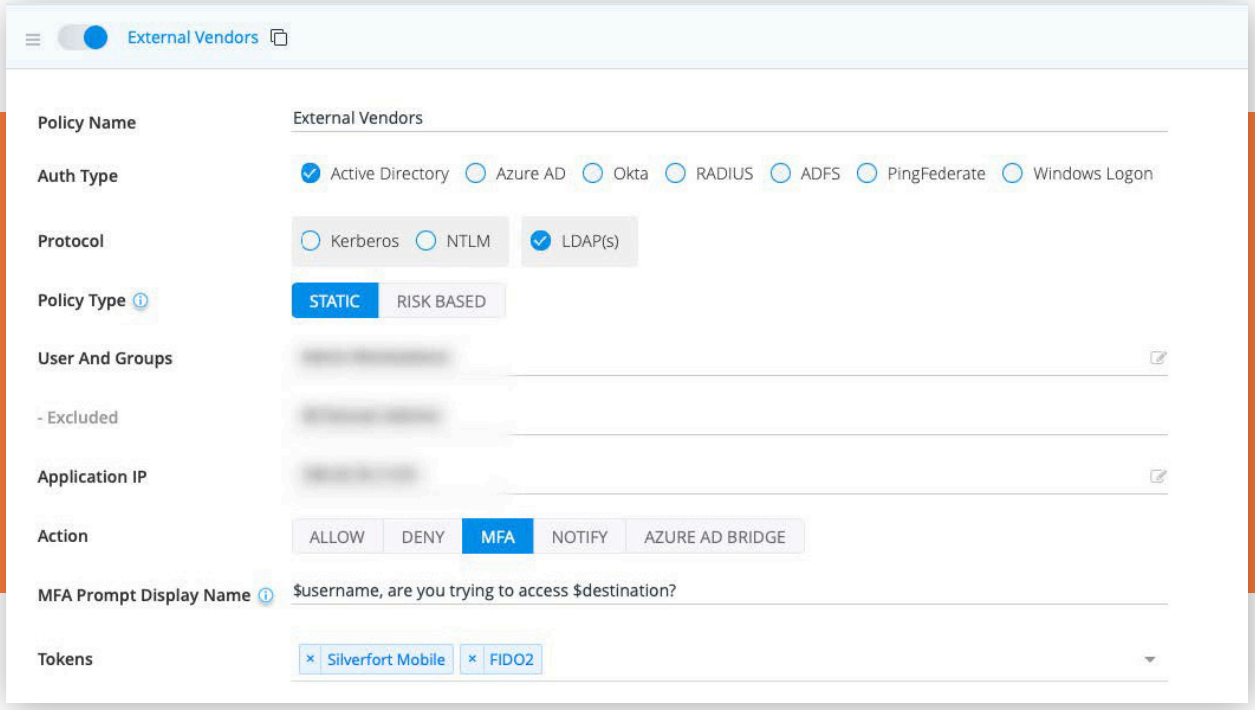
Challenge 3: Secure third-party access

Authentication for third-party access

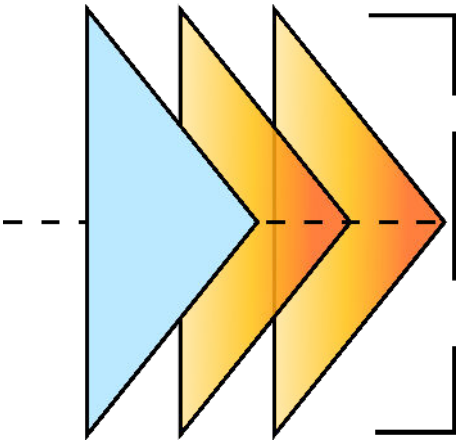
Like many major telecommunication companies, the telecom provider is using third-party vendors across its organization for operational services. Similar to their internal employees, third-party users were not required to be authenticated after logging in with their credentials in order to gain access to an app or resource. This created a major security challenge in securing third-party users' remote access. By not having an authentication process in place, the telecom provider had limited visibility into the third-party vendor users' actions and the risks they are subject to beyond their direct connection to its environment.

Protecting third-party access with MFA protection

The telecom provider's ability to deploy advanced MFA protection across all their environments and resources helped improve their organizational security posture, including securing third-party access. By having the proper security controls in place, they can properly monitor all access requests and authentication logs of their external vendors. Before a third-party vendor can gain access, they must be authenticated with MFA. This is done by the external users being authenticated via RDP sessions to the network before they can access the telecom provider's system. Due to the large number of users requesting access to its environments, they created a vendor domain just for this specific group of users. By segmenting their third-party access with proper authentication processes, the telecom provider decreased the access points for potential incoming identity-based attacks.



The telecom provider's third-party access policy is deployed by their external vendors who request access to their network and resources to manage third-party applications. Every third-party user must verify their identity with MFA.



Moving forward

Since deploying Silverfort, the telecom provider has been empowered with advanced MFA protection and visibility into all user authentication requests across all custom applications.

The initial phase to enforce proper security controls across their environments was a substantial step forward in their security roadmap. Over the years, Silverfort and the telecom provider have worked together to proactively strengthen their security posture with complete identity protection across its ever-evolving environments.

This customer case study shows that deploying proper identity protection takes focus and resources, but the results are worth the investment. The telecom provider initiated this project to enhance and solidify the identity aspects of its security posture. Now, they have a much more robust set of countermeasures in place to mitigate the threat of malicious actors utilizing compromised credentials to perform unauthorized access to their critical systems.

About Silverfort

Silverfort secures every dimension of identity. We deliver end-to-end identity security that is easy to deploy and won't disrupt business operations, resulting in better security outcomes with less work. Discover every identity, analyze exposures, and enforce protection inline to stop lateral movement, ransomware, and other identity threats.

Learn more