Silverfort

CASE STUDY

Major multinational bank extends custom MFA to legacy applications with Silverfort

BASED
Southeast Asia

INDUSTRY
Banking

USERS
50,000+

ENVIRONMENT
22,000 Servers
43 Domain controllers
329 Legacy applications
VDI infrastructure

THE CHALLENGE:

The bank needed to apply end-to-end multifactor authentication (MFA) protection to its legacy applications.

Executive summary

The banking industry powers the world's financial transactions. Because they deal with private information and handle large sums of money, banks have long been viewed as leaders in cybersecurity due to the array of secure and protected systems they have in place. But financial firms are also much more likely to be targeted by malicious actors — up to 300 times more so, according to the Boston Consulting Group.

The need for rapid digitization and the rise of remote work have inadvertently increased the risk of banking systems being compromised through the use of stolen credentials. Although real-time protection exists against malware, data access, and data exfiltration, this has historically not been possible when attackers use stolen credentials for authentication, particularly in the case of legacy applications that lack modern security controls.

Many banks continue to rely on legacy applications in their environment, which presents a security concern as these apps don't natively support MFA protection. Implementing MFA on them involves time-consuming modifications that could expose the institution to downtime and compromise stability. Additionally, traditional MFA solutions require an agent to be installed on the app server, which can strain computing resources. As a result, many banks lack the ability to secure every access request.

This case study is about how a leading financial institution partnered with Silverfort to gain real-time identity protection and visibility into their user access and authentication requests by extending their custom MFA solution to all legacy applications. You will learn about the organizational challenges faced, the specific protection needed, and the bank's positive experience using Silverfort's Unified Identity Protection platform.

Customer overview

About

This multinational financial institution has a focus on consumer banking, asset management, securities brokerage, equity, and debt fundraising with operations across the Asia-Pacific region and thousands of employees working in dozens of markets.

Environment

The bank's environments include more than 300 legacy applications, numerous security products, and a Virtual Desktop Infrastructure (VDI) implemented across its global organization. All employees and contractors are issued a company phone and laptop with a custom app that is used to access various corporate services and also for purposes of authentication.

Why now

The bank wanted to use its own custom MFA app as the single solution for identity verification but encountered difficulties incorporating its internal homegrown apps. This is because these apps don't natively support MFA, so extending coverage to all of them would've required extensive code changes to each individual app. As well, the bank didn't want to disrupt operations with a large number of MFA verifications so they could maintain the efficiency of resource access for thousands of employees around the world. Finally, the bank also needed to comply with local regulations requiring MFA on any system being used to access customer information over the internet.

Finding the right partner

Due to the range of applications in their environment and the proprietary nature of their custom MFA, the bank sought a solution that could integrate with their custom-made app and provide complete visibility into every authentication without having to make any code changes to apps or install any agents on its 43 domain controllers. The deployment of Silverfort was a methodical process that allowed the bank to quickly onboard all 329 of its legacy apps in just a few months and seamlessly extend its custom MFA protection to thousands of users.

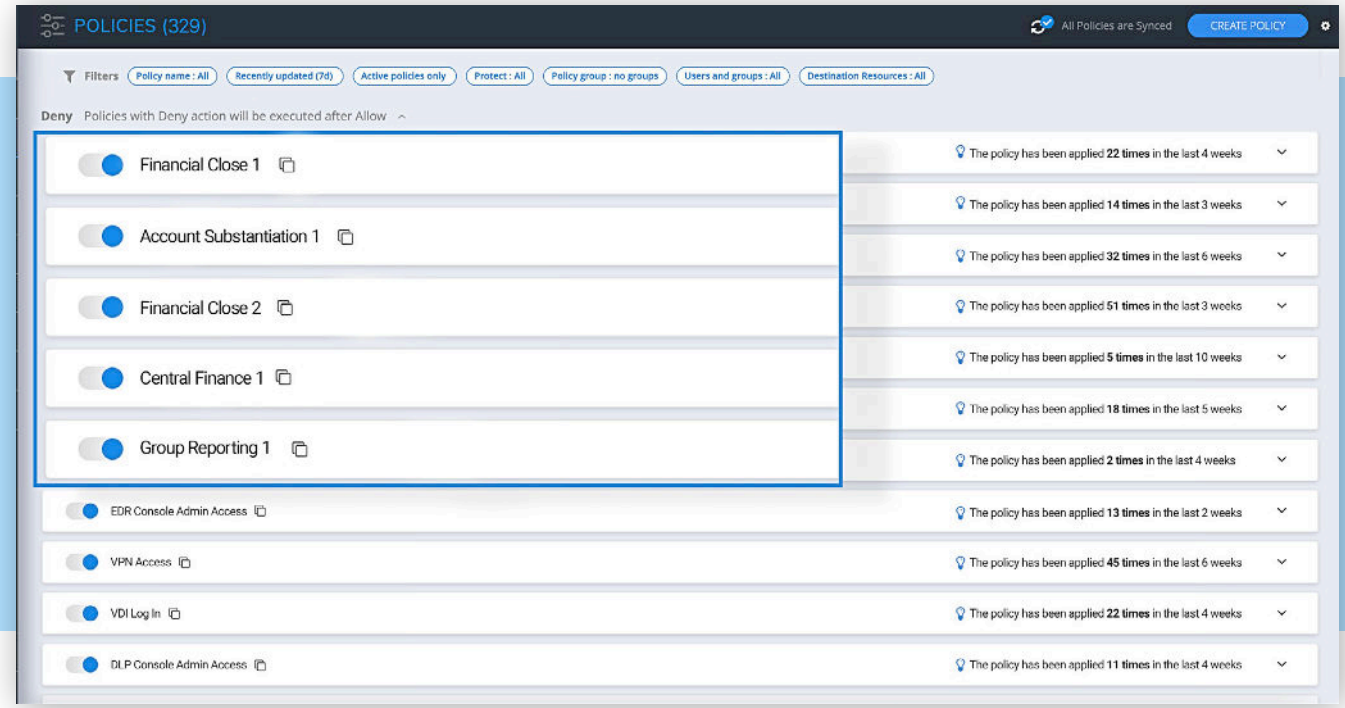
Challenge 1: Protect banking legacy apps that don't support MFA

Enable MFA across 329 legacy homegrown applications

The bank sought a way to enforce MFA on 329 different legacy homegrown applications, which are used for various business processes including payment transfer, ticketing, and internal accounting. Configuring each app individually was not a practical option due to the amount of time and effort this would've required, as well as the fact that any changes to an application's code could've resulted in malfunctions that would have broken the processes that they managed. The bank also did not want to install any agents on the servers of these legacy apps to avoid overloading them with excessive computing.

Protection of the bank's applications and other key assets

Following Silverfort deployment, the bank was successfully able to implement separate MFA policies for each of its legacy applications. Although these applications did not natively support MFA, they did authenticate to Active Directory (AD). Because Silverfort's architecture enables AD to forward every incoming authentication request before granting or denying access, Silverfort could analyze these requests – including ones made to the bank's legacy apps – and, based on the configured policy, determine whether to allow or challenge with MFA. This enabled MFA to be uniformly applied to all apps without having to configure them one by one. In addition, the bank was able to apply Silverfort's MFA on access to its VPN, VDI, EDR, and other segments of its IT and security infrastructure, thus achieving full coverage of its MFA needs with a single solution.



Silverfort's Policies screen displays several of the policies the bank created in order to implement MFA for each of its 329 legacy apps as well as for key components of its IT and security infrastructure, including the EDR console, VPN access, VDI login, and DLP.

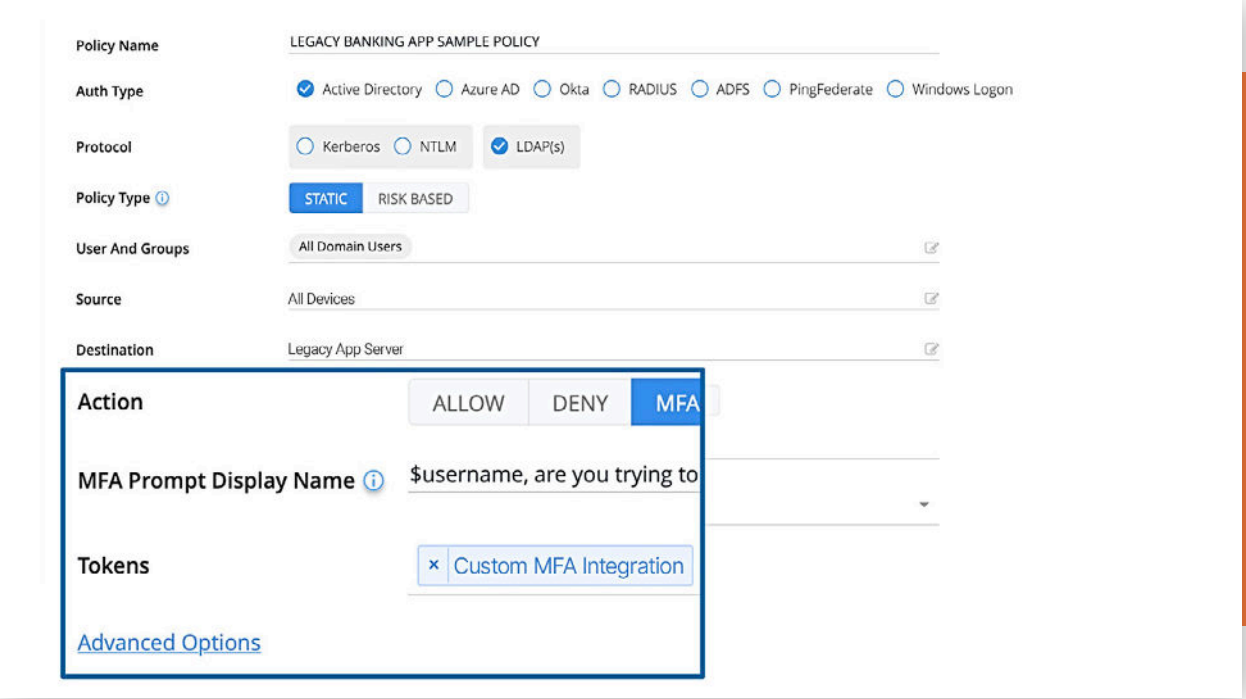
Challenge 2: Integrate seamlessly with in-house MFA

Need for integration with the bank's own MFA

The bank had developed its own MFA application, initially intended for customers when accessing banking services. The bank wanted this same MFA to be applied internally to its workforce when accessing apps and other resources in order to give users a unified experience across all devices and in every environment.

Fast integration and custom MFA coverage for every application

Working with the bank's developers, Silverfort was able to integrate its authenticator with the in-house MFA via API calls. This meant that, although Silverfort still analyzed each access request to determine whether MFA was required, it did not use its own MFA solution but rather triggered the bank's in-house MFA. As a result, end users received MFA notifications via the bank's own app for every access request.



This screen shows an example of how the bank used Silverfort to enforce its own custom MFA on all LDAP authentication requests coming from Active Directory, via an integration with Silverfort's authenticator.

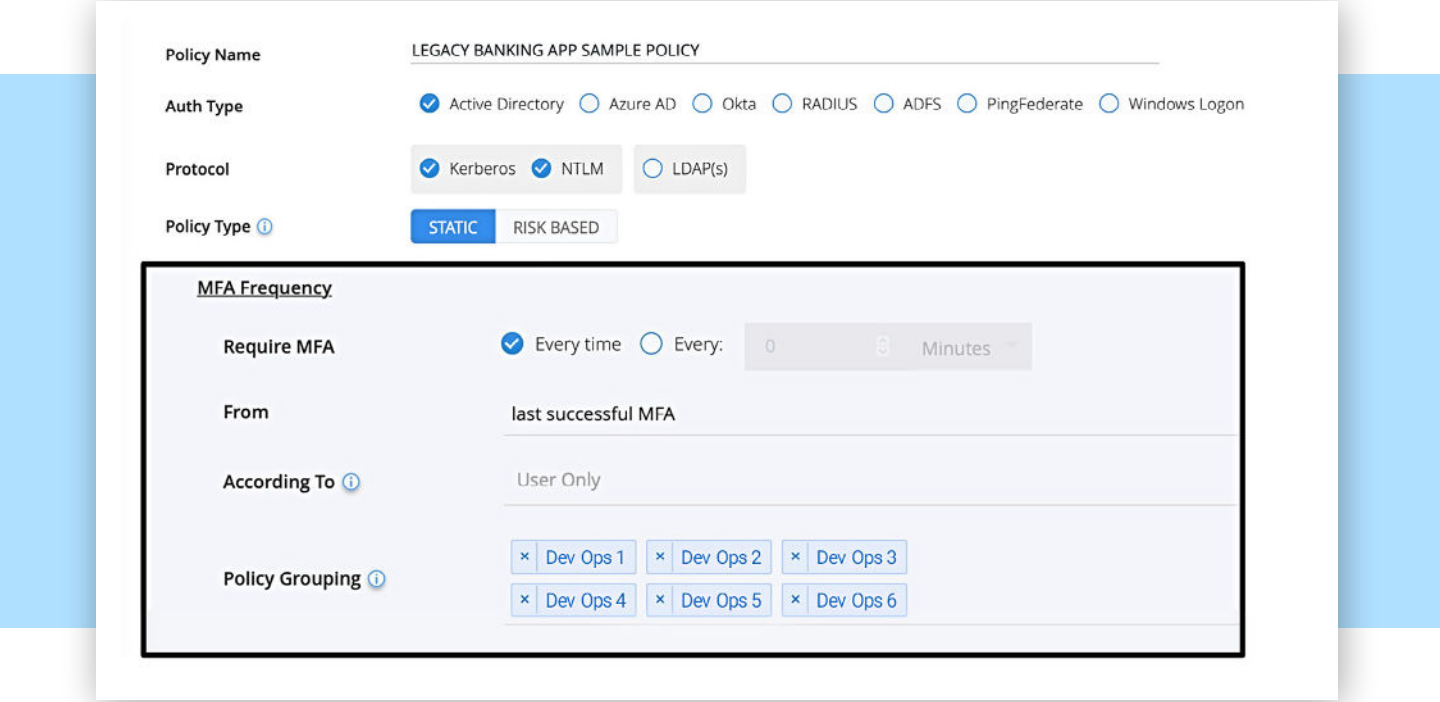
Challenge 3: Improve user experience

Reduce number of MFA authentications

With tens of thousands of employees spread across different regions, it was important for the bank to streamline operations. So an additional challenge was how to improve overall security efficiency by reducing the number of times users were required to authenticate with MFA. For example, users reported MFA fatigue when requesting network access via VPN due to a process requiring both username-password and a six-digit OTP. The bank's developers also needed a way to access suites of DevOps applications without being prompted for MFA multiple times.

Streamlined MFA for all systems

Working with Silverfort, the bank was able to reduce the total number of MFA alerts sent to each user and speed up the process for securing access. For VPN authentications, Silverfort was able to push all MFA notifications directly to the bank's mobile app, allowing for faster verification. Silverfort also enabled users to get access to several apps at once following a single verification, thus facilitating access requests from developers and other key user groups.



This screen shows how the bank used Silverfort to create a policy enabling a suite of related apps to be grouped together under a single MFA policy. As a result, users needed to authenticate only once to get access to all apps included in the grouping, reducing MFA fatigue.

Challenge 4: Comply with local regulations

Need to comply with regulations mandating MFA

The bank was subject to local regulations mandating that strong user authentication be applied via MFA to any system used to access customer information over the internet. The need to comply with this regulation was an important incentive for the bank to improve identity protection across its organization.

Bank achieves compliance with the help of Silverfort

By implementing a comprehensive and unified MFA protection solution across its environments, the bank was able to strengthen the authentication process for all users. By securing its legacy homegrown applications with MFA protection, this allowed the bank to become compliant with the local regulatory requirements.