appgate

CASE STUDY

FINANCIAL SERVICES INSTITUTION PROTECTS LEGACY ASSETS

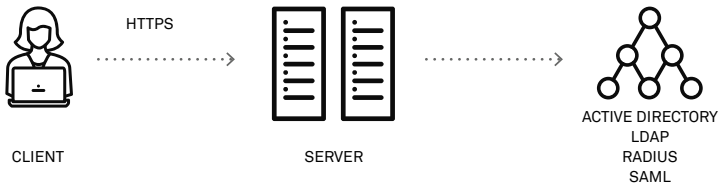
BACKGROUND

A multinational banking and financial services corporation undertook multiple network security and compliance initiatives to reduce operational complexity and risk.

The financial institution faced a number of challenges. First, legacy applications and infrastructure run numerous core business operations. These legacy applications were unable to integrate with modern identity and access management (IAM) platforms including modern methods of user authentication (such as SAML and RADIUS). Next, the institution needed to move 2 million firewall rule sets handling north/south traffic off the internal data center firewalls. Managing this with firewall rule sets was becoming resource intensive and error prone. Finally, the company wanted to benefit from the cloud, but required a consistent secure access solution across its hybrid IT environments.

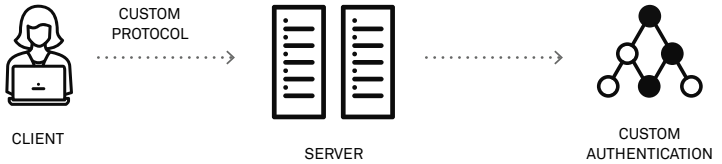
CHALLENGES

Legacy applications, whether built internally, purchased or inherited through mergers and acquisitions (M&A), are often difficult to modify and impossible to decommission. These legacy systems are usually out of date and cannot support modern security technologies that did not exist when the systems were developed. However, these legacy systems must comply with modern regulatory and compliance requirements.



MODERN APPLICATIONS SUPPORT STANDARD AUTHENTICATION

While modern applications support standard authentication and network protocols, and single sign-on and multi-factor authentication platforms are easily able to integrate, legacy apps are resistant to such changes. There is no “hook” for modern identity or authentication providers to integrate.



LEGACY APPS REQUIRE CUSTOM AUTHENTICATION

The organization required a solution to protect access to its legacy assets, ensure consistent access to on-premises and cloud resources and support third party access to systems.

INDUSTRY

Financial services

CHALLENGES

Provide modern identity and access management (IAM) for legacy apps

Address current security and regulatory compliance controls

Ensure consistent security across hybrid IT

Cope with unmanageable and static firewall rules

SOLUTION

Appgate SDP

BENEFITS

Extend the life of legacy applications without rewriting / refactoring

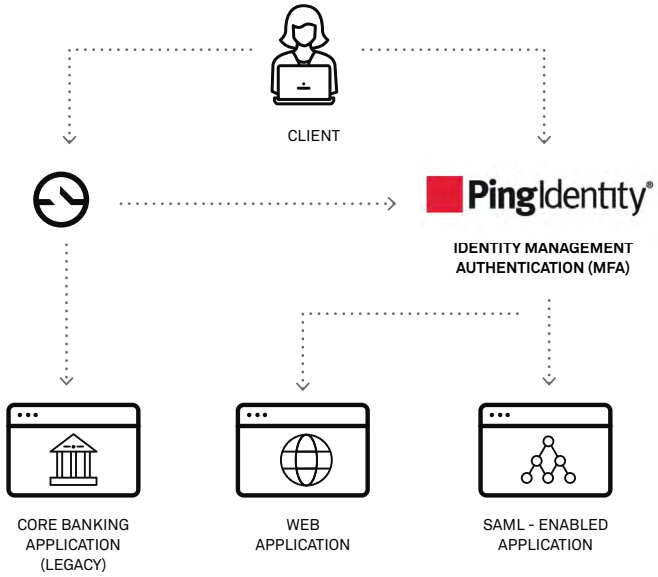
Succesfully comply with regulatory controls and requirements

Deliver consistent security for the organization to adopt the cloud

Reduced operation complexity and risk

SOLUTION

Appgate SDP was selected to secure access to the institution's mission-critical legacy applications. Serving as a pass-through black box, Appgate SDP integrated with the organization's IAM solution to secure access between its legacy and modern applications and comply with regulatory requirements.



Appgate SDP provides the financial institution with the ability to control user access from a single solution across both their legacy on-premises infrastructure and cloud environments. The solution has allowed the business to rapidly enforce multi-factor authentication (MFA) across critical applications, meet regulatory compliance standards, reduce risk, and provide assurance that the right level of security is always met.

BENEFITS

PROTECT LEGACY ASSETS

With Appgate SDP, the institution applied modern security to its legacy applications without modification. This extended the life of the legacy assets helping to reduce costs and risk.

REDUCE FIREWALL STATIC RULES & COMPLEXITY

The company needed to move 2 million user rule sets handling north/south traffic off the internal data center firewalls. The internal team was unable to manage these and required a third party program to validate rules and traffic. Appgate SDP Live Entitlements feature was used to replace its static access rules with dynamic, context-sensitive access policies. Live Entitlements dynamically change security based on what users are doing, where and when.

ACHIEVE REGULATORY COMPLIANCE

Appgate SDP provides compensating controls for new and legacy applications, extending multi-factor authentication and granular, least-privileged access capabilities to mission critical workloads.

CONSISTENT SECURE ACCESS ACROSS HYBRID IT

Appgate SDP provided consistent security across all applications – new, legacy, on-premises and cloud.

REDUCED ATTACK SURFACE

Using Appgate SDP, the institution enforced the zero-trust model so that anyone attempting to access a resource must authenticate first. Zero trust ensures that once proper access criteria is met, a dynamic one-to-one connection is generated from the user's machine to the specific resource needed. Everything else is completely invisible. This applies the principle of least privilege to the network and completely reduces the attack surface.

FUTURE

A global business, the institution initially rolled out Appgate SDP in two countries. Following the successful implementation, Appgate SDP will continue to be rolled out across other regions.