appgate

DATA SHEET

SECURING LEGACY ASSETS

Extending the life of applications and systems

Today's modern enterprises are evolving. While today's applications are developed using modern trends, there are also a large segment of enterprise applications that companies inherent from mergers and acquisitions or find too costly to refactor using modern application development tools.

But the enterprise cannot abandon these applications; they are running the core business functions for many enterprises – trading platforms, airline ticketing, core banking suites. These applications are accessing highly valuable data across networks to provide essential business functions.

Most of these critical legacy applications are not being secured by modern security protocols. Instead, security is through opaque, unchangeable and closed protocols with no support for modern single-sign solutions, such as RADIUS or SAML. The result is increased risk for the enterprise as core mission-critical assets are open to attack.

The enterprise is searching for a solution to bridge the gap between legacy assets and modern security solutions. Designed around the user and built to support today's modern workforce, Appgate SDP provides organizations with secure access to all network resources including legacy applications.

USE CASE: FINANCIAL SERVICES ORGANIZATION SECURES ACCESS TO MISSION-CRITICAL APPS

A large financial services organization relied on legacy applications for day-to-day business operations. However, these legacy applications could not readily integrate with modern identity and access management (IAM) platforms. The organization was challenged with ensuring secure access to the high value legacy applications that complied with regulatory requirements, including modern methods of user authentication (such as SAML).

Appgate SDP provided a Software-Defined Perimeter solution to secure access to this organization's mission-critical legacy applications. Serving as a pass-through black box, Appgate SDP natively integrated with the organization's IAM solution to secure access between the organization's legacy and modern applications and address compliance and regulatory requirements.

BENEFITS

Fully managed identity-centric, network-enforced perimeter security for every user, device, location, and application

Extend life of legacy assets without refactoring for modern security solutions

Address compliance gaps with universally accepted compensating security controls

Fine-grained, individualized access reduces potential attack surface, protects critical resources

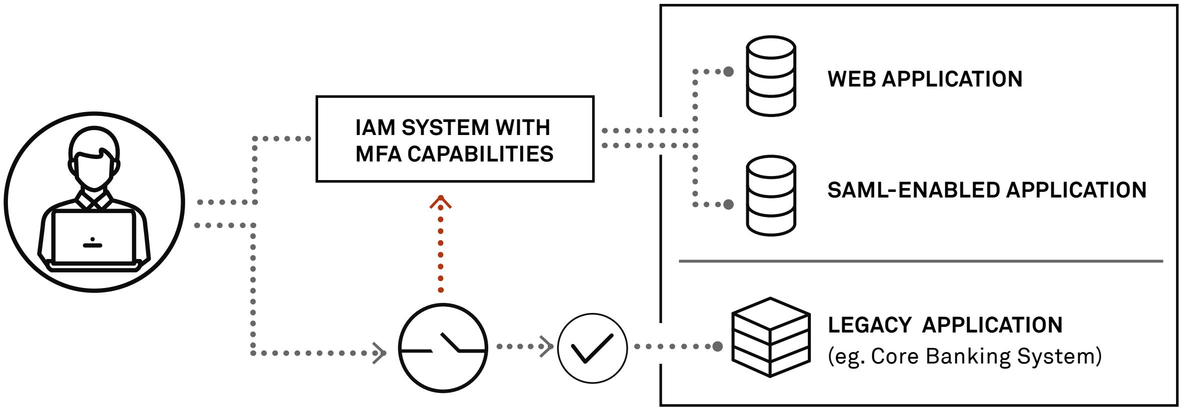
Provide consistent access control across hybrid environments

Securely connect remote users to legacy assets using patented multi-tunnel capabilities

SECURING LEGACY ASSETS WITH APPGATE SDP

The financial services organization's employee requires access to a legacy application that cannot consume SAML authentication – in this case, Ping Identity.

- To access the application, the employee is authenticated and authorized to access specific network resources with Appgate SDP.
- Appgate SDP consumes the SAML authentication. The user is authenticated and granted access to the legacy application.
- The only pathway to access the legacy application is through Appgate SDP.
- It protects the system from network access through any other means, ports or connections.



HOW APPGATE SECURES LEGACY APP

Extends the lifespan of applications that either cannot be refactored, or are too costly to refactor to take advantage of modern security mechanisms.

Acts as a compensating control for application authentication, addressing regulatory compliance concerns.

Improves the overall security of the enterprise, extending beyond the single legacy application use.

Empowers the enterprise to gradually end-of-life legacy applications in a thoughtful and deliberate manner when appropriate, while still operating day-to-day normal business.

appgate