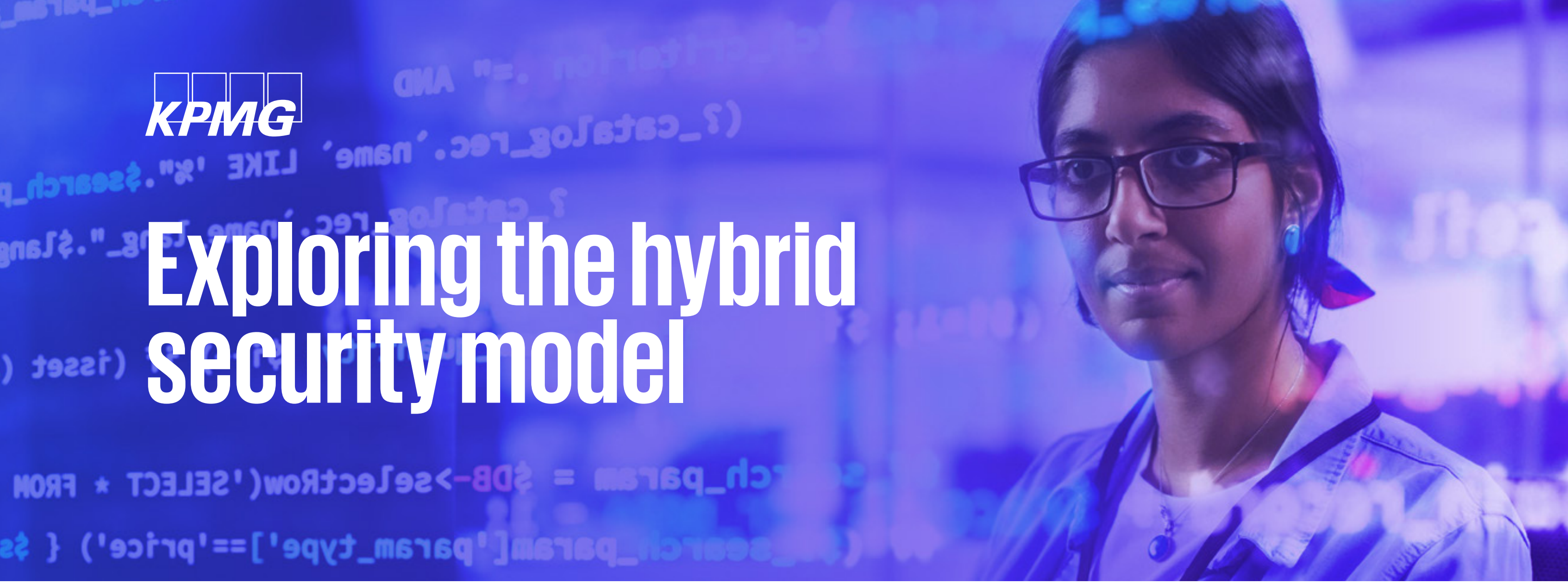


Exploring the hybrid security model

Modern cloud platforms—think Amazon, Google, Microsoft and Oracle, for example—can arm you with an array of remarkably powerful features that can simplify and accelerate the development of cutting-edge, cloud-native solutions: infinitely scalable, non-SQL object storage, microservices and containerization, machine learning and more.

Of course, the appeal of the cloud isn't limited to such groundbreaking features. Migrating from a legacy on-premise application to a modern, software-as-a-service (SaaS) alternative can be like upgrading from a Model T to a modern electric vehicle. Even just "lifting and shifting" a legacy application to the cloud can offer many benefits—enhanced security and availability chief among them.

On the other hand, migrating a legacy app can be an expensive, challenging and disruptive endeavor. "If it ain't broke, don't fix it" is still an important guiding principle for any technology leader, but especially for those in government where the decision to migrate or not can be influenced by dozens of factors including security and regulatory constraints that most commercial organizations will never face.

As a result, government agencies' legacy solutions will continue to coexist with their modern cloud-based cousins for the foreseeable future. But it doesn't mean that these apps must live in two completely separate worlds when it comes to security—and identity and access management (IAM) in particular. These hybrid cloud environments are now well supported with modern security standards and technologies designed to integrate the old with the new.

Why modern government is important

Government agencies in the U.S. must modernize in order to keep up with changing user needs, regulations, and health and public safety requirements. Leaders of modern governments rethink business processes and service delivery models to more effectively achieve their mission. This article is one of a series that features how modernizing affects the government workforce and the user experience, improves security and public trust, and accelerates the digital journey. KPMG team members offer insights intended to help guide governments in their modernization efforts to encompass all processes, technologies, policies, and the workforce so each works together to create connected, powered, and trusted organizations.

The advantages of a hybrid IAM model are clear and compelling, including:

- Greatly enhanced security with fewer attack surfaces, and the ability to add modern security controls that most legacy applications lack, including multifactor authentication, adaptive authentication, continuous authentication and enforced password complexity
- Reduced administrative costs, with a single, centralized solution for provisioning and de-provisioning users across all applications, including automated onboarding
- A better user experience through single sign-on, including automated forgotten password resets
- Improved intelligence through usage pattern analysis across all systems, cloud and on-premise
- Reduced complexity for other digital transformation initiatives, including legacy-to-SaaS migrations.

There is some complexity and effort involved with integrating legacy apps into a modern hybrid security environment. As of yet, there is no "drag-and-drop" solution. The location of the legacy application is largely immaterial, too. A legacy app that's been "lifted and shifted" to the cloud doesn't automatically become part of your IAM ecosystem; it still must be manually integrated.

In this paper, we'll explore the hybrid IAM security model, the technologies that enable it and the options you have for integrating your legacy applications.

A hybrid approach to identity and access management

The evolution of application security has provided developers and architects with standard security protocols such as OpenID Connect (OIDC), Open Authentication (OAuth) and Security Assertion Markup Language (SAML) that are designed to give users seamless, secure access to applications regardless of where the application is hosted. These protocols define how a user is authenticated, where the authentication is performed, and how the user's identity is propagated across security boundaries by defining a circle of trust both inside and outside of the organization. Additionally, these protocols can provide data about the user to determine resource authorization and entitlements.

Despite these standards, there is no one-size-fits-all approach to integrating a legacy app. There are a variety of options to choose from, and what works in one case may not work in another. Some IT organizations rely on integration features offered by their cloud providers. Others turn to well-known third-party cloud security or IAM companies. Some use a combination of the two, while yet others add open-source software solutions to the mix, such as the Apache mod_auth_openidc or NGINX nginx-openid-connect web server plug-ins.

Rather than explore each of these hybrid security models in detail, we'll describe a technology-agnostic, standards-based approach for building a hybrid access management solution.

The basic hybrid model

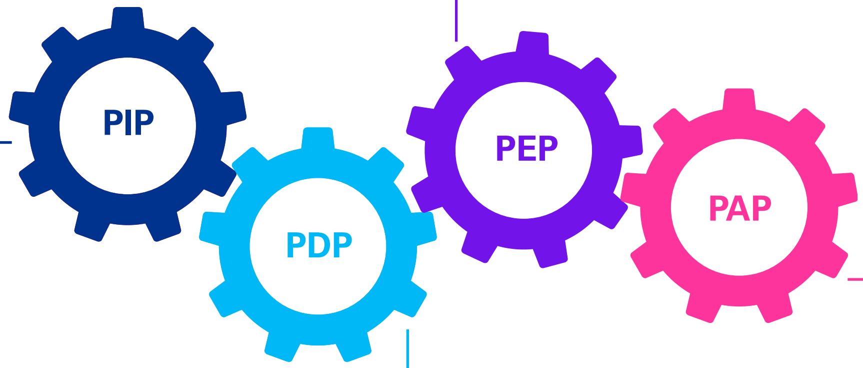
At a high level, most every integration involves placing an intermediary or "proxy" component—typically a software plug-in, agent or proxy server—in front of the legacy application. On one side, the proxy component uses modern, standard protocols to communicate with the centralized, cloud-based IAM system. On the other side, it communicates with the legacy app (or a legacy access management system used by the app) by whatever means the app expects (or can support) for user authentication and authorization, such as:

- Http headers with the user ID in a name-value pair
- Http cookies
- JSON Web Tokens (JWTs) or identity assertions
- Other custom code.

If we look a bit closer, we can see that there are actually four components:

Policy Information Point (PIP)—The logical structure where policy data is defined and stored.

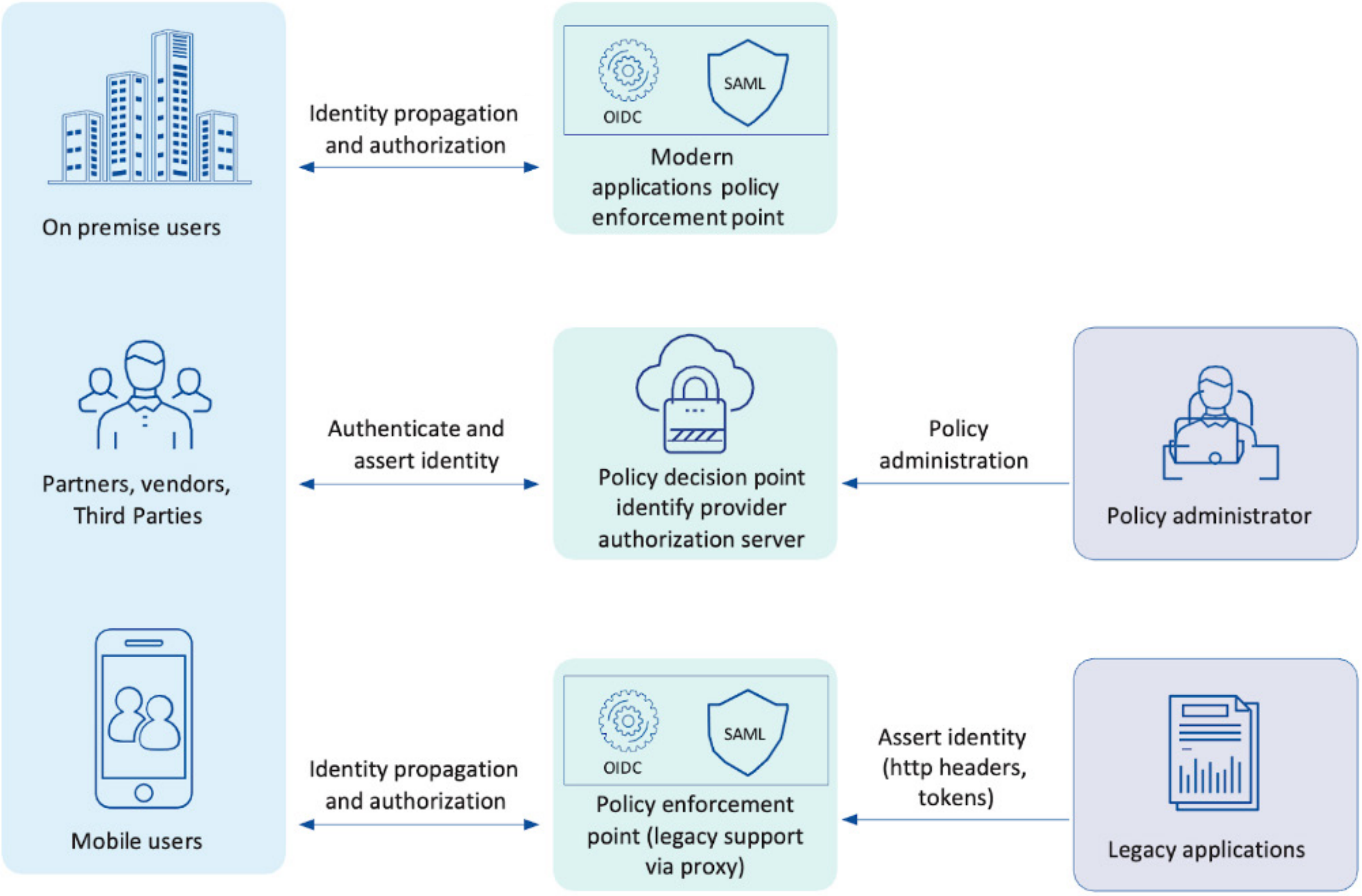
Policy Enforcement Point (PEP)—The interface where the security policy is enforced. This can take the form of an agent, plug-in, proxy server, or embedded code within an application.



Policy Decision Point (PDP)—The interface used to interpret the security policy and provide the authoritative decision whether the policy is satisfied or not. Typically, this provides a true or false response.

Policy Administration Point (PAP)—The location where administrators define security policy.

Figure 1 illustrates how this hybrid model might work. The four components described above are represented in the diagram, along with their functions, possible data flows and integration points.



On premise users
Partners, vendors, Third Parties
Mobile users
Identity propagation and authorization
OIDC
SAML
Modern applications policy enforcement point
Authenticate and assert identity
Policy decision point identify provider authorization server
Policy administration
Policy administrator
Identity propagation and authorization
OIDC
SAML
Policy enforcement point (legacy support via proxy)
Assert identity (http headers, tokens)
Legacy applications

Figure 1—Logical Technology-Agnostic Integration Pattern

As illustrated in Figure 1, the concept includes a central policy for applications that are integrated and several methods for integration. This model shows integration using industry-standard protocols with the policy decision point (PDP) where user authentication and policy decisions are made. The integration of legacy components is handled via the proxy component, which on one side can integrate with the PDP using modern protocols and on the other can handle various methods for back-end legacy integrations.

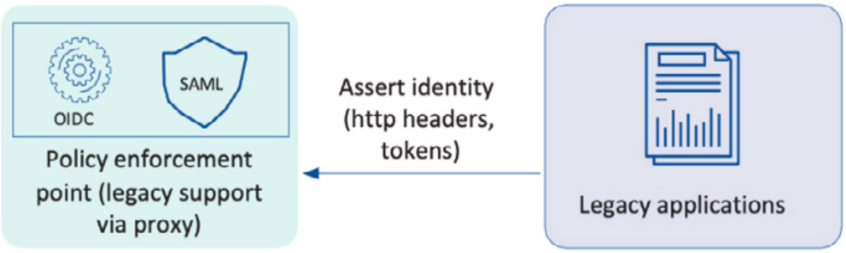

OIDC
SAML
Policy enforcement point (legacy support via proxy)
Assert identity (http headers, tokens)
Legacy applications

Figure 2—Proxy Layer with Legacy Application

As shown in Figure 2, the proxy layer serves as an identity translator after the user is authenticated and authorized by the primary PDP. After the proxy validates the authenticated request as the policy enforcement point (PEP), the user identify and entitlement information can be extracted and transformed into a format that the back-end legacy application can consume.

Advanced features, too

While the above examples focused on the basic authentication and authorization process, keep in mind that the very same components and mechanisms can be used to implement more advanced security controls, including multifactor authentication, device management, adaptive authentication and continuous authentication. Many of these advanced controls would be difficult or impossible to integrate without the flexibility of modern protocols and standards.

Conclusion

Government agencies are often required to maintain legacy applications, and so they must find a sustainable and secure way to integrate those legacy applications with modern cloud models. Standards-based IAM offerings from cloud providers, third-party security technology providers and open-source technologies offer a variety of options for integrating these legacy applications. By enabling modern and legacy technology to coexist, they can help you mitigate the risks associated with running older software platforms, lower costs, reduce complexity and provide a better user experience.

If you'd like to know more about these options or how KPMG can help, get in touch. We'd be happy to discuss how we can help you and your agency make the leap into a modern and secure hybrid environment.

About KPMG

KPMG has worked with federal, state, and local governments for more than a century, so we know how agencies work. Our team understands the unique issues, pressures, and challenges you encounter in the journey to modernize. We draw on our government operations knowledge to offer methodologies tailored to help you overcome these challenges and work with you from beginning to end to deliver the results that matter.

The KPMG team starts with the business issue before we determine the solution because we understand the ultimate mission. When the way people work changes, our team brings the leading training practices to make sure your employees have the right knowledge and skills. We also help your people get value out of technology while also assisting with cloud, advanced analytics, intelligent automation, and cybersecurity. Our passion is to create value, inspire trust, and help government clients deliver better experiences to workers, citizens, and communities.

Contact us

Joseph Klimavicz
Managing Director, Federal CIO
Advisory Leader
KPMG LLP
703-795-8999
jklimavicz@kpmg.com

Kathy Cruz
Director, Government
Cybersecurity Practice
KPMG LLP
916-792-3976
kathycruz@kpmg.com

read.kpmg.us/modgov

kpmg.com/socialmedia

Some or all of the services described herein may not be permissible for KPMG audit clients and their affiliates or related entities.

The information contained herein is of a general nature and is not intended to address the circumstances of any particular individual or entity. Although we endeavor to provide accurate and timely information, there can be no guarantee that such information is accurate as of the date it is received or that it will continue to be accurate in the future. No one should act upon such information without appropriate professional advice after a thorough examination of the particular situation.