A MODERN APPROACH TO IAM

Centralized identity and access management streamlines user access to agency applications and strengthens system security controls.

—By FedScoop Staff

Federal agencies continue to wrestle with the challenge of trust: how to ensure those engaging with their IT systems are who they say they are and only have access to the information to which they are entitled.

That's all the more important as agencies expand into multi-cloud environments and embrace agile development. Applications routinely live in different locations, making it critical to have proper access controls that work across a variety of locations and devices.

Getting the identity management foundation right is a critical element of government cybersecurity initiatives and a cornerstone of IT transformation.

That element gained greater importance over the past year when the Office of Management and Budget released its draft policy for Identity, Credential and Access Management (ICAM), aimed at ensuring "the right individual [has] access [to] the right resource, at the right time, for the right reason."

But ICAM also plays a key role in the administration's "Cloud Smart" strategy, released in September. Not only does it streamline how users access information in a multi-cloud world, it also supports modern agile development skills on the back end that are essential if agencies are "to realize the scalability, stability, and speed to market benefits of cloud infrastructure," according to strategy documents.

BENEFITS OF STREAMLINING ACCESS MANAGEMENT

In practice, this means agencies will need to evolve towards a purpose-built, centrally managed identity solution that can give agencies stronger identity and access control — and replace the identity suites that come with various applications. Deploying a modern identity and access management (IAM) platform provides several benefits to agencies, says Jeff Brooks, vice president, U.S. Public Sector at ForgeRock, a leading global supplier of IAM solutions. A centrally managed platform:

- **Supports IT transformation**, by consolidating stove-piped identity management systems to a common platform that can support all application requirements.
- **Delivers a quick return on investment and cost savings**, both in systems and in manpower, by simplifying the tasks for system administrators and support desks to manage and maintain access privileges.
- **Improves the user experience**, providing single sign-on capabilities to improve internal and external user authentication journeys.
- **Provides a path for cloud migration** that doesn't interrupt services while maintaining users' familiar experiences.

"Having a modern, centralized IAM platform that was easy to integrate with the back-end systems... [is an] essential step in moving from a stove-piped experience to a customer experience."

—Chris Keel

The advent of modern, cloud-based IAM platforms makes the task of centralizing identity and access management controls easier for CIOs.

Government officials in Norway, for instance, launched a public portal that enables the country's 5 million citizens and more than 500,000 businesses to communicate with more than 300 municipal, regional, and national government agencies, all of which are accessible using a central authentication and single sign-on service developed by ForgeRock.

Deloitte Consulting, meanwhile, is currently working with Texas state officials to bring 52 different applications together into a single statewide government portal, using ForgeRock's IAM platform. According to Chris Keel, principal at Deloitte Consulting, having a modern, centralized IAM platform that was easy to integrate with the back-end systems of multiple agencies was pivotal to that effort, and essential step in moving from "a stove-piped experience to a customer experience solution," Keel said.

The scalability of modern IAM platforms was also demonstrated at HSBC, the global financial group, which reduced nearly 200 internally managed identity management systems down to less than a dozen, using ForgeRock's platform, according to Brooks, significantly reducing the group's costs as well as its threat surface.

EVALUATING IAM OPTIONS

While the logic of moving to a centralized IAM platform is compelling, the challenge for most agencies usually boils down to determining the best way to move forward.

Agencies should start by looking at solutions that work with both legacy systems and emerging technologies, supports both people and the internet of things, and can scale easily in the future, Brooks suggested.

Additionally, agencies should carefully consider the scale and complexity of the customer bases they serve and the number of systems and applications they hope to consolidate before selecting a solution. And they should look not just at what's needed today, but what's going to be needed to meet future requirements and cyber challenges.

Agency leaders generally appreciate that the more password and logon requirements employees and citizens have to juggle, the greater the opportunities for security risks and vulnerabilities. A centralized IAM platform directly addresses the password plague. And it provides a powerful tool to map users against the applications, databases, and services to which they are allowed access, resulting in superior security and on-line citizen experiences, Brooks said.

It also makes it easier to change access privileges and restrictions quickly — an important consideration where users' roles and responsibilities can change on short notice for any number of reasons.

FACTORING IN OPEN STANDARDS FOR DEVOPS

Another key consideration when evaluating prospective vendors' solutions is how readily they can integrate with existing systems. "Unless you can integrate those with the business systems that require them, all you've got is another layer of technology to be managed," said Spiros Angelopoulos, principal solutions architect at ForgeRock.

The ability to integrate a centralized IAM solution with existing applications depends in part on the prevalence of open source standards, such as the REST API, which establishes essential rules for uniform interfaces, he said.

But it's also important to look for modular development platforms that can automate development, testing and production processes. And it's important those platforms can support IAM requirements for all applications as well as internal and external users who will need to access to those applications now and in the future.

"Organizations and agencies are under pressure to quickly embrace DevOps and move workloads to the cloud in order to accelerate growth and meet citizen demands," said Jessica Morrison, vice president for product and industry marketing at ForgeRock. She cited Gartner estimates that 75 percent of organizations will have deployed a multi-cloud or hybrid cloud model by 2020.

"With this opportunity also comes significant challenges for identity teams, including a lack of resources and skill-sets to deploy identity in DevOps environments. That can result in lengthy and expensive deployments," she said. "Without an identity platform that can automate and integrate seamlessly into continuous delivery environments, while also supporting multi-cloud deployments — whether on AWS, Google, Microsoft Azure, etc. — it will be difficult for agencies to meet internal needs and scale for citizen demand."

"A modern identity and access management platform that supports open standards will save agencies time, money and resources over the long run."

—Jeff Brooks

NEXT STEPS TO IMPROVING ACCESS MANAGEMENT

Brooks recommended several steps agencies should take to improve their approach to identity and access management:

- **Analyze help desk costs.** Look for opportunities to initiate a basic self-service capability with user identification that corresponds to the value of the assets being protected.
- **Start with high-impact/low-risk projects,** rather than "boiling the ocean." Agency leaders and end users may see the benefits of a well-designed identity and access management environment in the abstract but may not appreciate the effect it can have on established processes and culture. Starting small and succeeding lays the groundwork to elevate the system's use more broadly.
- **Look at web-based opportunities,** and identify where a web interface would benefit from applying a modern IAM technology to its core functions.
- **Pick a systems integrator that understands IAM and your agency's mission needs.** The best use of security technology — and a seamless, fully integrated IAM system — is when it balances mission and technical needs against the capabilities of the new system. A good systems integrator can translate and map out the necessary steps to make the implementation a success.

Until recently, government agencies in the U.S. and elsewhere have focused mostly on playing technology catch-up. That is beginning to change. Agencies are increasingly looking simultaneously to improve the quality of service delivery to citizens. Modern IAM platforms are essential to delivering on both.

A modern identity and access management platform that supports open standards, says Brooks, will save agencies time, money and resources over the long run. It will also help them future-proof their technology upgrades. □

This article was produced by FedScoop and sponsored by ForgeRock. Learn more about how modern IAM platforms can future-proof your agency's IT investments.

fedscoop FORGEROCK