Why a Platform Approach to Identity Management Should be Part of Digital Transformation

The case for upgrading legacy systems onto the cloud has been made ad nauseum by now. The cloud offers flexibility and scalability, and is a pay-as-you-go alternative that makes government IT more efficient and effective.

Often overlooked in the digital transformation equation, though, is the fact that a shift to a modern, interoperable architecture offers government IT leaders a unique opportunity to consolidate and rationalize identity.

Let's explore how a platform approach to identity gives end users a more seamless experience, speeds cloud implementation and can help shore up an organization's cyber-defense posture.

THE IDENTITY LEGACY

Identity management has been a sore spot within many legacy government IT systems. Large agencies may have deployed homegrown identity management systems across their on-premises architecture, but these systems typically lack standardization. They don't extend across other government entities and they aren't sufficiently open for agencies to integrate new capabilities.

Smaller agencies face an even greater challenge. Here, identity management often is a manual task, with administrators creating accounts, activating or deactivating users, altering permissions and so on using a labor-intensive, error-prone methodology.

Clearly agencies need a better solution. Cloud-based modernization offers a unique opportunity for agencies to put a more effective system in place. At the same time, a solid identity infrastructure can help IT leaders maximize their cloud investment.

WHY A PLATFORM?

To understand the value of a platform approach to identity, it helps first to step back and consider the role of identity itself in the enterprise. In legacy systems, identity has been treated as an ancillary feature to append to applications. Identity has been undervalued and often ineffectively addressed across legacy systems. The unifying force of a cloud modernization invites government IT leaders to rethink identity as a central business function, a thing unto itself. Viewed objectively, that's how identity behaves: It isn't a part of any one application or a piece of any one on-premises system. Rather, identity pervades the government IT enterprise, and a portal approach offers a means to exploit and leverage that pervasiveness.

A modern approach to Identity management aggregates many directories into a single, definitive source of information. Biographical data, vacation days, benefits and more can and should be consolidated in a way that makes it easy for responsible parties to access and manage that data, regardless of the application.

Unifying identity on a platform leads to significantly improved efficiencies, especially through automation. Take the "new employee" scenario as a typically labor-intensive example. In the old way of doing things, an admin would likely create or provision that employee's identity multiple times across disparate applications. A portal automates this process, requiring just a single iteration for all appropriate accounts and permissions to be activated. This automation is not only more efficient, but it also helps agencies avoid manual errors.

MORE EFFECTIVE MANAGEMENT

Beyond the efficiencies of automation, a portal approach to identity increases flexibility. As an employee moves within an agency, or between different city or state agencies, new roles and permissions can be easily implemented based on the shared, readily accessible identity.

Upgrading from on-premises to cloud-based systems makes the adoption of such capabilities especially intriguing for many organizations. In a siloed IT enterprise, proprietary systems make it difficult to adopt a platform posture to identity, whereas the inherent nature of the cloud is such that even within a complex organization, an agency can implement a new system relatively quickly and inexpensively.

Perhaps most importantly, a move to the cloud practically demands a re-think of fundamental security notions and we know that identity is a key element in enterprise security.

- By definition, the cloud puts new security concerns into play. The old firewall that used to protect your data center is no longer the central facet of the security apparatus.

- Rather than patrol the perimeter, security now must be based on the user, which means controlling access through identification.

This kind of identity-based security conception is a natural feature of an identity management platform.

KEYS TO THE CLOUD

An effective approach to identity management is key to leverage the benefits of the cloud. Organizations that move proactively on this front "can reduce their identity management costs and, more importantly, become significantly more agile in supporting new business initiatives," Gartner reports. The converse is also true: Insufficient care around identity management can be one of the biggest roadblocks to effective digital transformation.

- With masses of workers moving to cloud applications, government faces a heavy transition lift. It's impractical to apply old manual methodologies to shift all those identities from legacy applications to the cloud. Such processes will likely introduce error, are labor intensive and extremely costly. Identity management is thus a key driver in the success of any digital transformation.

- An open and interoperable identity management system invites IT leaders to make the most of their cloud investment. Developers can access such a platform to easily implement new services, adding web and mobile applications while still ensuring a seamless user experience.

- Proactively mastering identity management maximizes the potential for future enhancements. Change management is faster and easier when underlying identity is unified and interoperable.

THE BOTTOM LINE

Why go to the cloud? Government spends the vast majority of its IT budget supporting outdated, siloed and inflexible legacy systems. Digital transformation offers a more cost-effective, flexible approach.

How to get there? IT needs to take a measured approach as it migrates a host of applications to a modern infrastructure. Identity should be at the core of these considerations. As a pervasive element that cuts across all users and applications, identity demands thoughtful attention. In an ideal solution, IT managers can make identity shareable across the enterprise; they should be able to automate many or even most of the routine tasks associated with identity management; and they should have the flexibility to apply identity to new and emerging uses as their systems evolve.

Judged in this light, an identity portal may offer an ideal foundational approach for government IT leaders who are looking to move effectively to the cloud and who hope to get the greatest possible payback for their modernizations efforts.

This piece was developed and written by the Center for Digital Government Content Studio, with information and input from Okta.

PRODUCED BY: CENTER FOR DIGITAL GOVERNMENT

SPONSORED BY: okta

The Center for Digital Government is a national research and advisory institute focused on technology policy and best practices in state and local government. The Center provides public- and private-sector leaders with decision support and actionable insight to help drive 21st-century government. The Center is a division of e.Republic, the nation's only media and research company focused exclusively on state and local government and education. **www.centerdigitalgov.com**

Okta is the leading independent provider of identity for the enterprise. The Okta Identity Cloud connects and protects employees of many of the world's largest enterprises. It also securely connects enterprises to their partners, suppliers and customers. With deep integrations to over 5,000 applications, the Okta Identity Cloud enables simple and secure access for any user from any device. Thousands of customers, including 20th Century Fox, Adobe, Dish Networks, Experian, Flex, LinkedIn, and News Corp, trust Okta to help them work faster, boost revenue and stay secure. Okta helps customers fulfill their missions faster by making it safe and easy to use the technologies they need to do their most significant work.

Learn more at: **www.okta.com**