Modernizing Citizen Experiences With Cloud Identity

MARKET TRENDS REPORT

govloop okta

Introduction

The explosion of devices and communication channels in recent years presents the federal government with a serious dilemma: How do agencies interact with citizens who increasingly rely on smartphones and tablets for public services?

Citizens expect government agencies to meet them on their terms, and today that means a quality customer experience (CX) that's digital, seamless and unfolds on any channel, device or platform they choose.

More importantly, customers also expect their business with agencies to be private and secure. Agencies that can't meet these demands risk losing citizens' confidence and trust, but developing secure, frictionless CX is easier said than done.

Currently, many agencies use outdated technology for their **customer identity and access management (CIAM)** needs. CIAM frameworks manage the identities of customers who access digital channels such as websites or mobile applications, so a poor CIAM strategy can lead to experiences that are fragmented and full of friction for employees and the citizens they serve.

Fortunately, cloud computing can modernize an agency's CIAM offerings. For this report, GovLoop partnered with Okta, a cloud-based CIAM software provider, to explore how agencies can strengthen their CIAM programs, with a focus on the four capability pillars of a modern CIAM approach.

The CIAM Timeline

2009

The Federal Identity, Credential and Access Management (FICAM) Roadmap and Implementation Guidance debuts, aiming to establish federal identity, credential and access management (ICAM) standards.

Source: Federal Chief Information Officer (CIO) Council

2011

The Federal CIO Council updates the FICAM Roadmap to include more detailed implementation guidance for agencies, such as establishing governing bodies for ICAM standards.

Source: Federal CIO Council

2019

The Office of Management and Budget (OMB) updates the FICAM policy to require that agencies create their own ICAM teams.

Source: OMB

2019

Eighty-one percent of U.S. adults owned smartphones in 2019, underscoring why agencies must include them in their digital outreach.

Source: Pew Research Center

Identity Management on the Agenda

In a 2019 memorandum, OMB described "a common vision for identity as an enabler of mission delivery, trust, and safety of the Nation."

"Accordingly, identity management has become even more critical to the Federal Government's successful delivery of mission and business promises to the American public," OMB adds.

THE CHALLENGE
Legacy CIAM

CIAM is a complex undertaking, requiring agencies to manage user logins, self-service registration and identity databases at scale. Unfortunately, the public is not inclined to give agencies a break when it comes to CIAM. Fair or not, public expectations have been defined by the private sector, which has shown that CIAM can be simple, private and secure.

Although that's true of modern CIAM tools, many agencies use outdated ones, which are often inflexible, costly to maintain and difficult to secure. These shortcomings often produce a dissatisfying CX.

"Doing identity, especially the legacy way, is hard," said Peter Zavlaris, CIAM Product Marketing Manager at Okta. "It's tons of workflows and procedures. It's high-cost and high-complexity, and it makes for a poor CX."

Developers are the first people to face trouble from legacy CIAM. They need more energy, funding and time to update their CIAM tools. "If you're not efficient, you don't get to market or iterate fast," Zavlaris said.

Legacy CIAM also presents management challenges for agencies. For instance, aging CIAM databases are often complex and require significant maintenance and upkeep. As a result, one software patching cycle can take staff away from more important projects for months.

Legacy CIAM is often custom-built without considering security features such as multi-factor authentication, threat detection and reporting. Without these, agencies are more vulnerable to cyberthreats. "There's a multitude of different vulnerabilities that exist," Zavlaris said. "One of the most common application vulnerabilities on the internet, for example, is broken authentication."

Finally, older CIAM tools tend to produce fragmented experiences such as multiple applications that require customers to create unique credentials for each. "How do you make sure you're not asking people the same questions about themselves?" Zavlaris asked. "People will not want to interact with the services that you're creating."

THE SOLUTION: CLOUD-BASED CIAM

CIAM thrives when four capabilities exist: frictionless user experiences, accelerated speed-to-market development, centralized access management and internet-scale security.

Fortunately, these four capabilities can be achieved with cloud computing. Cloud's agility, flexibility and scalability make it an ideal platform for modernizing CIAM. "Bringing in a cloud-based identity solution takes a massive burden off the developers," Zavlaris said.

First, cloud-based CIAM can help enable **frictionless user experiences** that are consistent, convenient and pleasing. It can also provide agencies with a unified profile view of citizens by granting an interface for collecting and storing authoritative first-person profile information that can be accessed across channels.

Next, cloud-based CIAM's adaptability allows **developers to quickly deploy** new or updated tools, such as social authentication, so that they reach citizens faster.

After that, cloud-based CIAM can provide agencies with **centralized access management** for their users. That makes managing agencies' applications smoother and more straightforward, and ultimately, agencies' CIAM grow more efficient, effective and nimble.

Lastly, cloud-based CIAM can **reduce the cybersecurity risks** for agencies and citizens alike by simplifying agencies' compliance with security regulations and updating their cyberdefenses.

BEST PRACTICES
Connecting Cloud and CIAM

1. Reduce your user friction

When customers have difficulty using public services, they avoid them. CIAM can help increase engagement by reducing friction, first by meeting citizens on the devices they prefer to use. Citizens appreciate access to digital public services on their laptops, smartphones and other devices.

Accessibility and convenience are equally important for CIAM. For instance, uncomplicated logins are attractive to citizens who aren't tech-savvy. By simplifying engagement, CIAM allows agencies to reach as many citizens as possible.

2. Select a secure cloud vendor

When moving CIAM to the cloud, security should be a defining requirement, not an afterthought. Agencies should pick a vendor that can meet their security needs from Day 1 – a vendor with a proven track record in government. Without a secure vendor, agencies risk exposing sensitive citizen data to cyberthreats.

Initiatives such as the Federal Risk and Authorization Management Program (FedRAMP) help provide a common approach to cloud security. FedRAMP standardizes security and risk assessment for all federal cloud products and services. Although useful for consistently shielding data across agencies, complying with this framework can be cumbersome.

Fortunately, cloud can help shoulder some of this burden. Solid cloud solutions typically comply with all relevant regulations out of the box, saving agencies the extra step of meeting those regulations themselves. Vendors that earn authority to operate (ATO) certifications prove they can meet the stringent requirements set for government cloud security. ATOs grant vendors permission to provide services such as cloud to agencies.

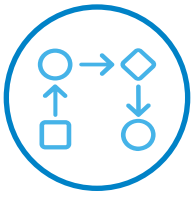
To further validate the security of their potential cloud vendors, agencies can look at certifications such as a FedRAMP ATO. They can also examine non-federal audits such as Health Insurance Portability and Accountability (HIPAA) certifications for additional peace of mind. Passed in 1996, HIPAA stipulates how the healthcare industry protects the personally identifiable information (PII) it maintains from fraud and theft.

Ultimately, citizens must trust agencies with private information such as their addresses, or they'll lose faith in those who can't protect their delicate details.

3. Reduce reliance on legacy CIAM systems

Cloud can ultimately help agencies leave their legacy CIAM systems behind. Not only are older CIAM systems costlier and harder to maintain, they're also more frustrating for employees and users. It's three times more expensive for agencies to manage and maintain CIAM internally, Zavlaris said.

Over time, agencies that cut ties with legacy CIAM systems save energy, money and time formerly spent on maintenance. They also produce experiences that are more pleasant for everyone involved.



4. Boost developer efficiency

Cloud isn't just about revamping agencies' technology, but also about making the workflows for their developers easier. Developers who build CX shouldn't get bogged down with complex identity projects. Instead, using code samples, documentation and how-to guides created in their programming language of choice, they can become far more efficient. Gradually, cloud can make customizing CIAM systems simple and straightforward for developers.

CASE STUDY
Directorate of Defense Trade Controls

Cloud's impact on a State Department (DOS) component shows how it can play a vital role in modernizing CIAM.

The Directorate of Defense Trade Controls (DDTC) ensures that the commercial export of defense articles and services advances U.S. national security and foreign policy objectives. When DDTC recently decided to digitize its paper-based case management system, the agency realized modernizing its CIAM component might prove demanding.

DDTC has over 13,000 external organizations that are registered as manufacturers, exporters, and brokers for defense services and defense articles. These organizations submit license applications to allow exports and temporary imports of munitions and technical data on the US Munitions List (USML). Before utilizing cloud, DDTC struggled to get a grip on managing CIAM for so many collaborators. Cloud enabled DDTC to deliver CIAM in a fraction of the time had they decided to build it themselves.

DDTC condensed its 8 legacy identity databases into one that it could use for all its CIAM needs. Cloud transformed the digital experience for defense contractors going through the licensing process. It made the system significantly more secure while delivering a seamless experience. Now DDTC knows who sees what and gets the 360-degree-view across all its applications."

DDTC's experience with cloud suggests it can help agencies centralize their CIAM management en route to mission success

HOW OKTA HELPS

Cloud can become the springboard that propels agencies' CIAM into the 21st century. Partnering with vendors such as Okta, agencies can provide cloud-based CIAM to citizens that's confidential, straightforward and safe.

By powering CIAM with cloud, agencies can develop and debut tools, such as fresh login portals, in record time. Furthermore, cloud's on-demand computing can help agencies save funds by paying for only the resources they need.

More importantly, providers such as Okta can provide private, secure cloud platforms that can help ensure agencies give citizens gratifying CX. "We understand not just how to make a system more scalable, extensible and user-friendly, but also more secure, as we're the identity experts," Zavlaris said.

Learn more here: Okta, Inc.'s Cloud-Based CIAM

Conclusion

The commercial world has conditioned citizens to demand private, secure and easy-to-use identities online. Agencies that can't deliver these attributes should consider modernizing CIAM a cornerstone of their digital transformations.

Although upgrading CIAM can be challenging, cloud can ease the transition. It can help agencies develop and launch CIAM products and services faster than ever, centralize management of CIAM services, and better serve citizens.

Perhaps most importantly, cloud's benefits can also produce CIAM that's more delightful for citizens. For agencies, there's no better reward than a job well done.

okta

ABOUT OKTA

The Okta Identity Cloud is an independent and neutral platform that securely connects and enables government to achieve simple and secure access from any device at any time, allowing its workforce and citizens to accelerate their missions with modern, Zero Trust identity. Okta holds FedRAMP moderate ATO and has been a consecutive leader in both the Gartner Magic Quadrant for Access Management and Forrester Wave Identity-As-A-Service (IDaaS) for Enterprise reports. Many agencies such as DDTC, CMS, FCC, and the Air Force are using Okta to fulfil their missions faster by making it safe and easy to use the technologies they need to do their most significant work.

For more information visit **okta.com/solutions/government**.

govloop

ABOUT GOVLOOP

GovLoop's mission is to "connect government to improve government." We aim to inspire public-sector professionals by serving as the knowledge network for government. GovLoop connects more than 300,000 members, fostering cross-government collaboration, solving common problems and advancing government careers. GovLoop is headquartered in Washington, D.C., with a team of dedicated professionals who share a commitment to connect and improve government.

For more information about this report, please reach out to **info@govloop.com**.

1152 15th St. NW Suite 800
Washington, DC 20005

P: (202) 407-7421 | F: (202) 407-7501

www.govloop.com
@GovLoop