Cloud Modernization

From Fragmented Identity to a Unified Cloud

Summary of Roundtable, hosted by ATARC in October 2022

WHITE PAPER

For the past two decades, Federal agencies have worked diligently to maintain high levels of security across networks. But as technology advances, agencies continue to face challenges with outdated and siloed identity and access management. According to a 2018 report issued by the Office of Management and Budget (OMB) and Department of Homeland Security (DHS), the identity, credential and access management (ICAM) process remains one of the most significant security concerns resulting from the government's current decentralized and fragmented IT landscape.

ATARC hosted a roundtable discussion with Federal IT experts to discuss ways agencies can modernize cloud operations and ICAM management without compromising security. Panelists shared challenges with existing identity and authentication management practices, and how Zero Trust will make unified cloud modernization possible.

Current Status of Cloud Modernization

Roundtable participants describe cloud modernization as moving operations to the cloud, while taking advantage of cloud native technologies, such as identity services and Zero Trust. While progress has been made, agencies are still struggling to establish certain levels of trust across environments. Day-to-day tasks remain the same, whether operating in the cloud or on-premise, but privilege access management differs depending on the environment.

As the cloud introduces more users into the environment, agencies find that some authentication models are not as secure or user friendly as others. With the influx of users, agencies are continually balancing security levels with user experience, particularly when it comes to data sharing and identity access. However, cloud modernization and Zero Trust are making it possible for agencies to streamline security measures and remove steps that are often ineffective and hinder the user experience, like passwords.

Break Identity Silos and Automate Identity in the Cloud

Roundtable participants noted the difference between internal and external identity management, and the different methods agencies must consider when external constituents, partners and customers request access to secure environments. Often the ICAM process for external stakeholders is more extensive and time consuming, which can interrupt workflows and delay response times for some agencies. However, all agree that login.gov is a successful example of an external federated identity service.

"All roads are leading to Zero Trust."

Roundtable Participant

Most agencies still rely on the Personal Identification Verification (PIV) card system, used to authenticate a person's identity and strengthen security to secured areas. Because PIV cards remain a mandated method to authenticate identity for many agencies, individuals will often travel to have their identity authenticated in person. Challenges also arise when PIV cards are the only form of identity access management available for contractors, many of whom work remotely as a result of the pandemic.

With advancements in technology, roundtable participants are certain there are alternative methods to authenticate identity that are more efficient, yet equally secure. Methods such as security keys, credentialing through PKI on mobile devices, and authenticator apps are not only secure, but provide a better user experience. Agencies not only have an opportunity to create efficiencies in ICAM processes, but also benefit from federated, shared identity services. Instead

 info@atarc.org

of implementing individual ICAM and badging systems, roundtable participants suggest that agencies begin accepting the security credentials and utilize the infrastructure of other agencies.

"Risk management and risk avoidance are two different things."

Roundtable Participant

While a cooperative federated identity service would require buy-in from multiple agencies, roundtable participants believe it's a needed service that many agencies would adopt. To reach the point of federated services, a concerted shift away from older methods of identity management will be required. However, one of the biggest impediments to internal identity federation is the lack of a parent agency to operate such a service, although roundtable participants suggest that the General Services Administration (GSA) may be best equipped to lead the effort, as they already manage the external federated services of login.gov.

Balance Resource Accessibility with Security

As agencies continue to modernize and implement Zero Trust practices, roundtable participants urge agencies to reframe how they approach risk management, in order to simplify business processes and continue making progress on their Zero Trust journey. However, this would require agencies to begin accepting risk in areas where risk was not accepted before.

An example of a risk worth taking, agencies may want to consider reducing the number of people with highest level access, while expanding constituencies at lower levels, understanding that not everyone needs a high level of clearance. Streamlining access would simplify business processes and reduce the administrative burden for high level validation requests. However, roundtable participants note that currently, many agencies struggle with knowing what level of assurance is appropriate for different information systems.

Modernizing Identity in the Cloud

As for cloud access, agencies should consider the specific data that needs protection and where it could be exposed. This methodology is at the heart of Zero Trust, which will allow agencies to dial into the appropriate trust level for any given situation. The level of user access depends on the attributes agencies prioritize to establish that trust level. Agencies should also consider the level of assurances when sharing data, particularly through APIs. But as cloud services modernize, agencies will have access to various assurance requirements in different environments and will be able to build variations into systems at scale.

"If we get Zero Trust right, not only will we have a lot of tools in our toolboxes to deal with any trust level, but it will also allow us to dial in our tolerance the way we need to, and improve collaboration with our partners while reducing friction between us and our customers to a level that's acceptable."

Roundtable Participant

As modernization to the cloud and Zero Trust progresses, roundtable participants anticipate that the paradigm of identity proofing is going to shift. If there is proof of strong user authentication, agencies can easily validate a user based on the specific device someone is using, and the location the request is coming from. Using Zero Trust attributes, agencies can quickly establish high confidence in a user's identity.

Contact us today to learn more and get involved in ATARC's Cloud Working Groups and other ATARC events!