SIGNAL AFCEA
More than a magazine: We're AFCEA.

## Turning Integration Bottlenecks into Mission Enablers:

# The Future-State Federated Identity Foundation for an Interoperable & Multi-Cloud ICAM Architecture

Identity drives everything across the federal space, from the PIV-CAC cards staffers carry to massive defense projects involving huge budgets and diverse players. The federal identity landscape has evolved rapidly in recent years, with the rise of public and private clouds, DevSecOps and zero trust. But underlying architectures have not kept pace with these advances. Established agencies are still grappling with aging investments made over successive waves of innovation, going from one authoritative directory behind a firewall to a growing collection of attributes scattered across diverse repositories.

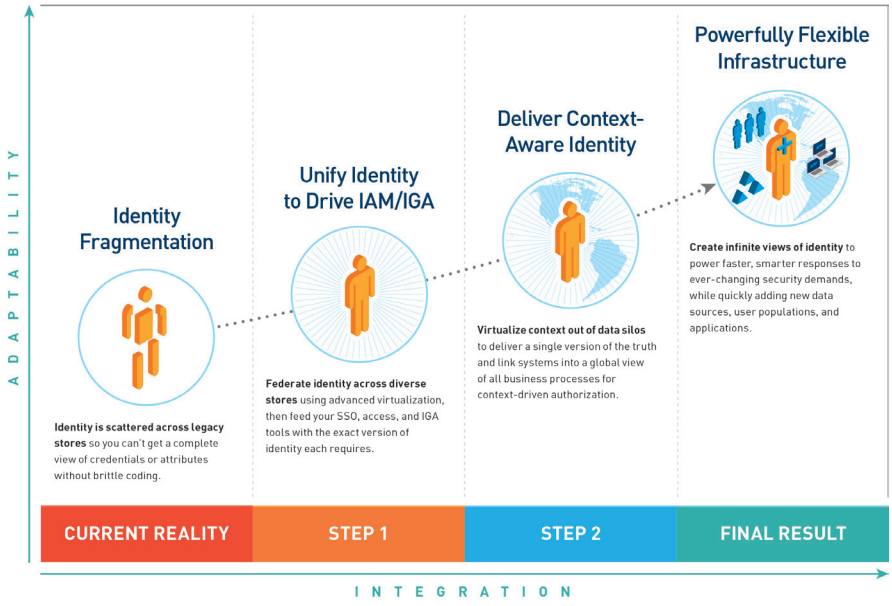
A global view of identity is difficult to achieve across so much fragmentation. But without an overarching understanding of identity, the underlying data can be manipulated, opening the door to data leaks. Federal IT teams must enable high level access and collaboration within—and often beyond—agencies, while keeping data safe at every level.

### Overcoming Identity Fragmentation for a Modern Identity Service

So how do agencies ensure their data is both authoritative and secure, delivering a single source of truth for accurate, immediate access and policy decisions? There is much talk about zero trust, which has updated the old slogan "trust, but verify" for a cloud-driven age. In today's increasingly perimeter-free world, the goal is to "never trust; always verify." Within this identity framework, access to agency resources is restricted until the user has proven their identity/access permissions in a series of progressive disclosures.

The overarching goal is a more adaptive infrastructure. However, many established organizations have

***Federated Identity (FID) Success Curve***




***RadiantOne FID is the unified identity foundation of the IAM landscape, allowing organizations to add flexibility to their infrastructures, enabling new capabilities and empowering new missions***

attributes scattered across diverse stores with no unified user directory. How can massive agencies overcome all this fragmentation to enable these newer identity solutions and lay the groundwork for zero trust identity?

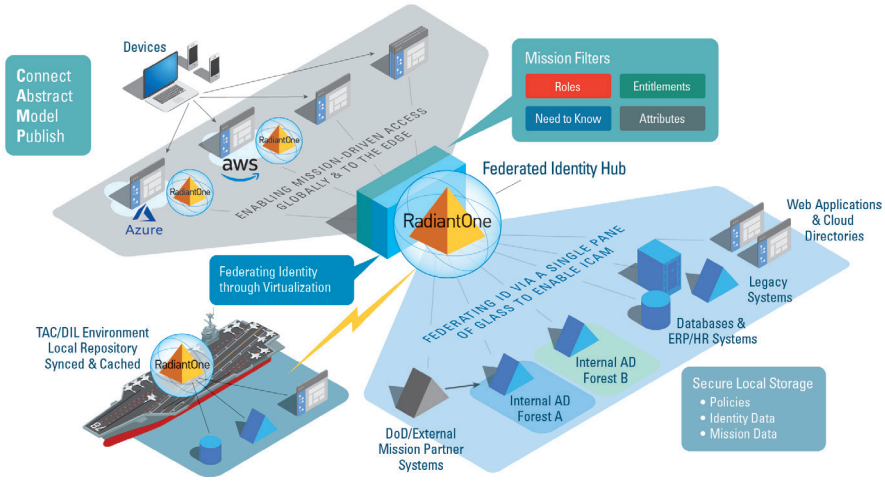
A key factor in building this "always verify" architecture is the ability to create a normalized view of diverse systems, rationalizing identity to enable single sign-on, while tapping into an array of attributes for context-driven authorization. As TechVision Research says in *The Future of Identity Management (2020-2025):* "Pulling together this scattered identity information and creating this organizational version of the truth is critical to limiting attack points and driving strong security programs. Make no mistake, zero trust relies on these and related IAM capabilities to an enormous extent."

Overcoming the diversity of different stores, each with its own protocol, requires a special solution, one that unifies identity across diverse stores, creating "a single version of the truth," with a global list where every user is represented once, as well as a global profile for each user containing every attribute across all systems for finer-grained policies. Enter RadiantOne FID, the unified identity foundation that is a necessary springboard for achieving a context-driven zero trust future.

## Laying the Groundwork for a Flexible, Future-First Identity

Agencies used to be protected by the traditional network firewall, but now, identity is the new perimeter. RadiantOne FID provides a single "pane of glass" to deliver idealized identity data for every mission requirement. Based on virtualization, this federated identity and directory service makes it easy to integrate and rationalize identity from diverse data stores. The result? An infinitely reusable central identity hub featuring complete user profiles. RadiantOne drives initiatives from tactical to strategic, making it easier to orchestrate identity across diverse sources and endpoints, delivering attributes all the way to the edge.

***Future-State & Multi-Cloud ICAM Integration Layer***




***Acting as an abstraction layer between applications and the underlying identity silos, virtualization isolates applications from the complexity of backends***

Federal agencies have long turned to RadiantOne to unify identity infrastructures, fortify the perimeter and enable new mission requirements. RadiantOne accelerates interoperability and eliminates integration as the key bottleneck to mission success while enabling modern identity-as-a-service across a multitude of mission-critical use cases, like these:

### 1. Delivering Multidomain Interoperability Based on Security Level

While "domain" often conjures up Active Directory, for the US military, domains are areas of authority within the different branches of service. So, a captain in the Navy would be a colonel in the Air Force; however, linking the two across disparate identity systems requires aggregating and correlating the identities. Such identity data usually resides in secure islands within agencies, each with its own unique identity infrastructure, so sharing across agencies and other organizations becomes quite complex.

In today's federal landscape, securely sharing identity attributes across well-vetted entities is essential for enabling collaboration across partner organizations. This can be seen when the military engages in multinational joint forces coalition exercises. Each underlying security system requires a thoughtful "translator" to smooth communications while keeping each organization's individual data secure.

RadiantOne FID acts as an abstraction layer, translating across protocols and integrating selected data across all the diverse entities, to facilitate attribute-based access based on security levels, without recreating entire infrastructures or sharing any sensitive data. With RadiantOne FID, it's easy to quickly spin up a federated identity service to drive access and collaboration during exercises, then decommission it once they are over.

Managing multiple personas is another essential capability. Someone may be an intelligence officer with access to classified materials most of the time, but aboard ship during training exercises, they act as a signals officer with very different classification access. Each role has different groups, attributes and functions; the key is knowing which persona is in play at any given time so the appropriate access can be granted for that role or context.

RadiantOne FID can associate multiple personas with a single person, offering contextual access for the persona in use. It also associates dependents with a single person,

such as an Army Major whose children get treated at a Military Treatment Facility (MTF), where they are attached to their active-duty parent's record. Without RadiantOne FID, this takes months of inflexible coding to map and correlate data for each specific role or relationship.

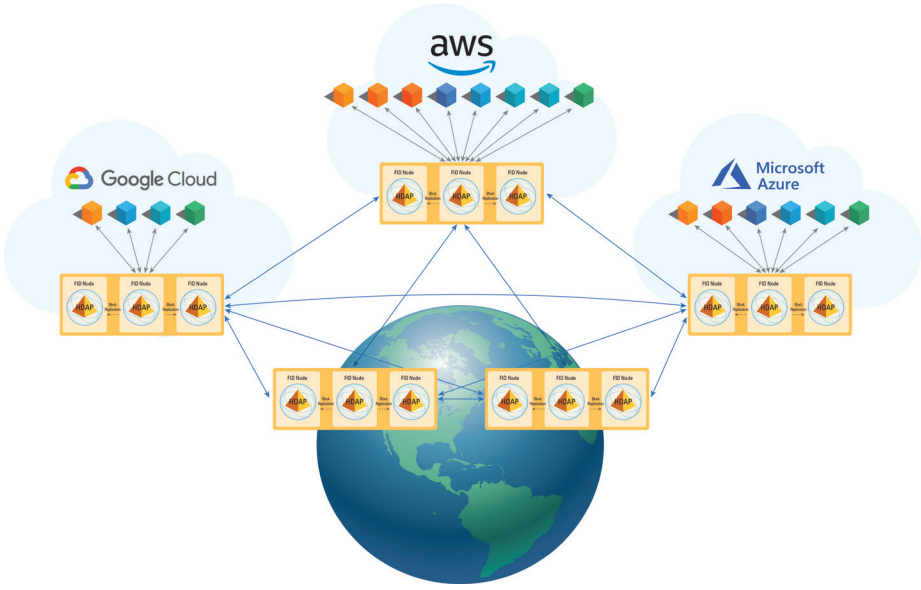
## 2. Building an Agnostic Directory Firewall for Syncing to Multi-Cloud Environments

Cloud directories are the repository of choice for critical data across public and private organizations, reducing infrastructure costs while enabling secure sharing. RadiantOne FID offers deep visibility into the current identity landscape while modeling idealized ecosystems to better meet new demands.

Acting as a master user record, RadiantOne FID allows agencies to identify the authoritative source for each data point and assign attributes to provision to the cloud directory, ensuring they are accurate, secure and normalized. All this is done in real time since cloud deployments need to match authoritative sources and be split-second accurate for secure log-ins/access.

Acting as a directory firewall, RadiantOne FID protects legacy internal systems from the cloud, allowing the identity team to decide what data each application receives and where to store credentials for swift, secure SSO and policy enforcement. When provisioning identity from cloud directories into different SaaS apps, RadiantOne transforms the data from the master user record to match exactly what each application requires, regardless of protocol or format.

RadiantOne FID is cloud-agnostic, giving users the freedom to quickly move between cloud directories and reshape their infrastructures at will. Because each cloud directory deployment refers to a common identity set, it is easy to move from cloud to cloud, whether the team is expanding its reach or leveraging better tools on another platform.




*It's easy to replicate identity data between multiple clouds to expand capabilities or target new goals*

Because they are globally available neutral spaces, cloud directories are also excellent environments for securely sharing data with foreign mission partners who have different data privacy regulations and security standards. If a foreign attribute is not allowed beyond its borders, RadiantOne can proxy to confirm that data without touching or moving it. It presents a tailored view of identity to an application, which can call that view and successively query the attributes that allow it to sign in users, authorize access or check group memberships.

## 3. Securing Remote-Access Telework in a Time of Global Crisis

The last several months have been a time of rapid learning as the world navigates a growing global pandemic. Remote work has become the norm, forcing a steep learning curve for IT departments—especially government agencies, where the security of classified data is essential for the safety of the nation. Suddenly, what used to happen within an extremely secure infrastructure has been scattered across individual homes, where government users now access work assets using personal networks.

The usual protocols were not in play, so IT teams ramped up the zero trust model, where access is granted gradually over several attribute-driven decision points. With RadiantOne, systems can access a rich global profile for each user containing a complete array of attributes from across every data source, giving a larger set of identifying factors to ensure appropriate access.

By integrating identity data into one unified identity data store, it is easy to provide Identity Providers with needed identity information in the exact format required—while giving organizations an integrated, highly scalable infrastructure that is ready to navigate challenges. In times of disruption, such as the COVID-19 pandemic, it was key to helping several federal agencies support this new demand for remote work quickly and effectively.

RADIANT LOGIC™

*Learn more about RadiantOne FID in the federal space at www.radiantlogic.com/government.*