Modernizing Identity and Access Management Through Identity Integration at the Department of the Navy

How the Department of the Navy Used a Federated Identity and Directory Service to Enable a Unified Network Initiative and Centrally Manage their IdAM Infrastructure

Integrating, Normalizing, and Modernizing Identity and Access Management

Over time the systems built by the Department of the Navy (DON) no longer supported the demands and mandates associated with modern identity protocols. Their systems and networks operate using 20-year-old design patterns for identity. They are stove-piped around application and network boundaries, preventing network, application, and data interoperability. Current solutions do not provide the type and level of control, monitoring, automation, and reporting needed to ensure security and operational flexibility in the modern hybrid operating environment.

The On-Shore, Off-Shore Challenge: Integrating and Synchronizing Identities in a Distributed Environment with Intermittent Connectivity

The DON requires identity information to ensure security and operational flexibility in a hybrid operating environment—however, connectivity proved to be a challenge as ships would be in low connectivity environments for lengths of time.

The Program Executive Office for Enterprise Information Systems (PEO EIS) was seeking an integrated identity solution providing at least an 80% increase in modern IdAM capabilities. There were two pressing problems that demanded attention:

1. **Multiple persona integration:** As service members change roles within the DON, they accumulate different personas in the identity system based on their stationed location. This led to challenges in authentication, authorization, and other IAM processes.

2. **Low-connectivity environments:** Navy has two networks—the on-shore network (NMCI), and ship network (CANES). The two networks were not syncing, making off-loading and on-boarding a significant challenge.

These technical limitations created a roadblock to allowing better security, interoperability, and cloud migration, and prevented the adoption of industry standard IdAM capabilities.

The DON needed to create a universal view of identities to integrate identities across roles, simplify access, and synchronize across the two networks.

The Opportunity: Building a Foundational Identity Infrastructure

When addressing these challenges, the DON had a unique opportunity to lay a foundational identity infrastructure to pursue several long-term strategic initiatives. They had two primary goals:

1. **Build a global view of identity across all groups** in the Navy by creating a unique repository linking all personas to a single individual, making it easier to flexibly manage groups.
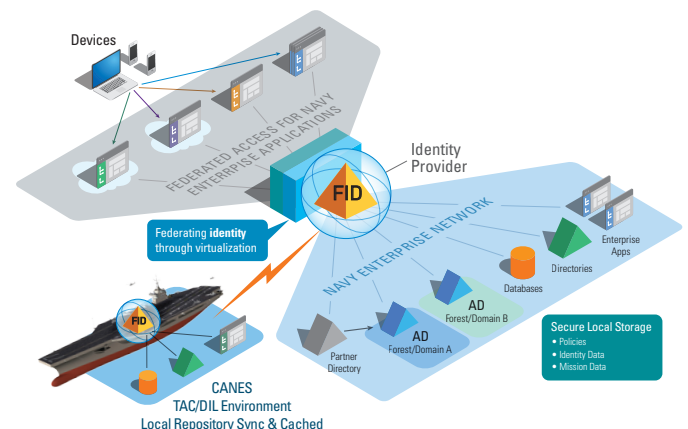

Figure 1. The DON had the objective of creating a "One Navy" unified network

2. Build a "One Navy" unified network, connecting the on-shore and off-shore networks, modernizing identity operations across Disconnected, Intermittent, and Low-bandwidth (DIL) environments. Because the ships on the CANES network were only available for a short time, it was essential that the two could quickly exchange information and updates. This would enable the DON to centrally manage and implement the Navy IdAM infrastructure, and support real-time operations across TAC/DIL and hybrid cloud environments.

The DON needed to streamline and automate IdAM processes, and improve their cyber risk posture.

Solution: An Integrated Identity Platform

To address these challenges, the Department of the Navy built a comprehensive identity services platform, designed to be loosely coupled to operate across boundaries.
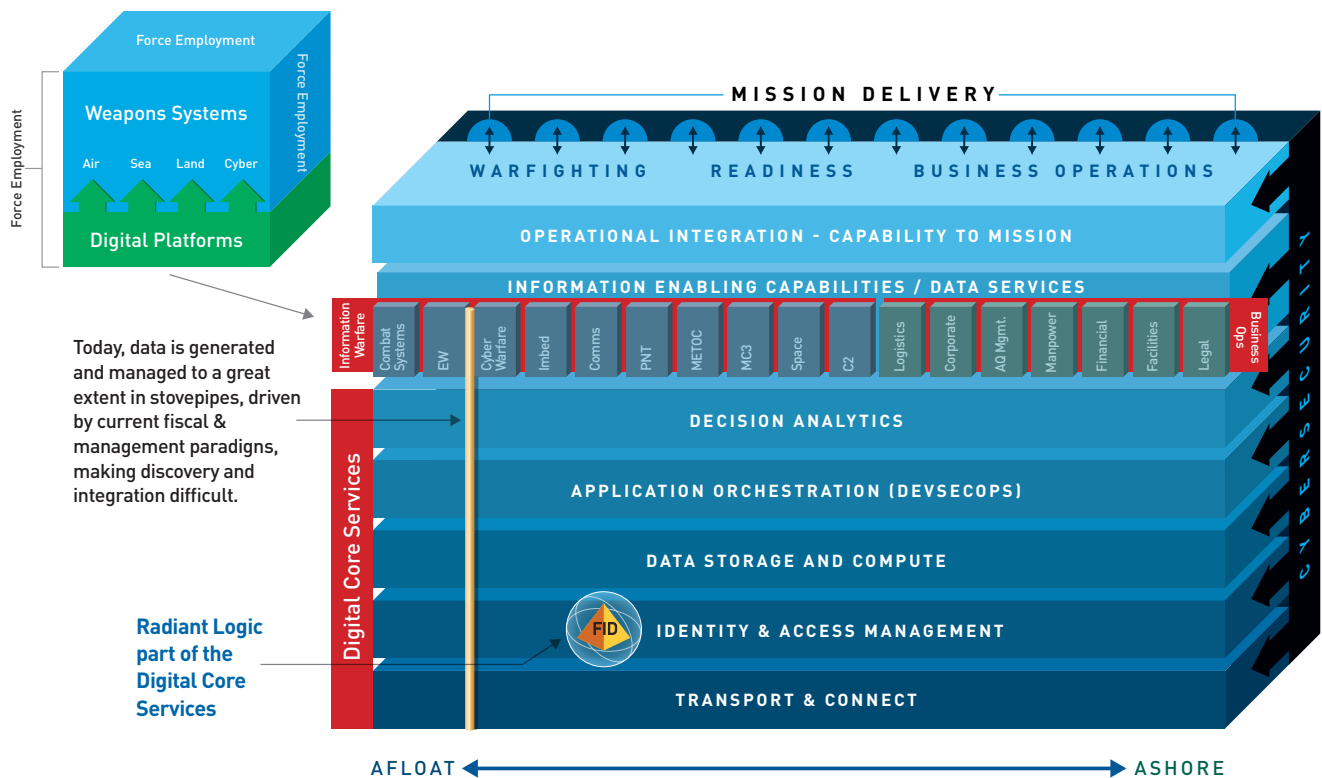

Figure 2. The digital core services stack requires identity integration to enable mission delivery

The RadiantOne federated identity and directory (FID) service is a key element in the DON's digital platform. Through advanced virtualization, it abstracts and integrates identity information from across both the on-shore and off-shore networks, effectively building a universal identity repository that can be queried by mission-critical applications.

This integrated identity platform will enable several mission-critical initiatives:

- Create a universal directory, linking in and correlating all personas to a single individual across networks

- Enable syncing across on-shore and off-shore networks, transferring information with real-time updates

- Facilitate finer grained identity management decisions and supplied real-time information and grouping to streamline authorization

- Build a foundation for a best-in-breed ICAM solution suite, including access management, identity governance and administration, and privileged access management.

Thanks to the federated identity and directory service, the DON can now:

- Deploy an integrated IdAM stack to address all aspects of a modern IAM platform, including SSO and governance

- Manage centrally but consume identities across the Navy network

- Extend IdAM to ships and submarines across the low-connectivity environments

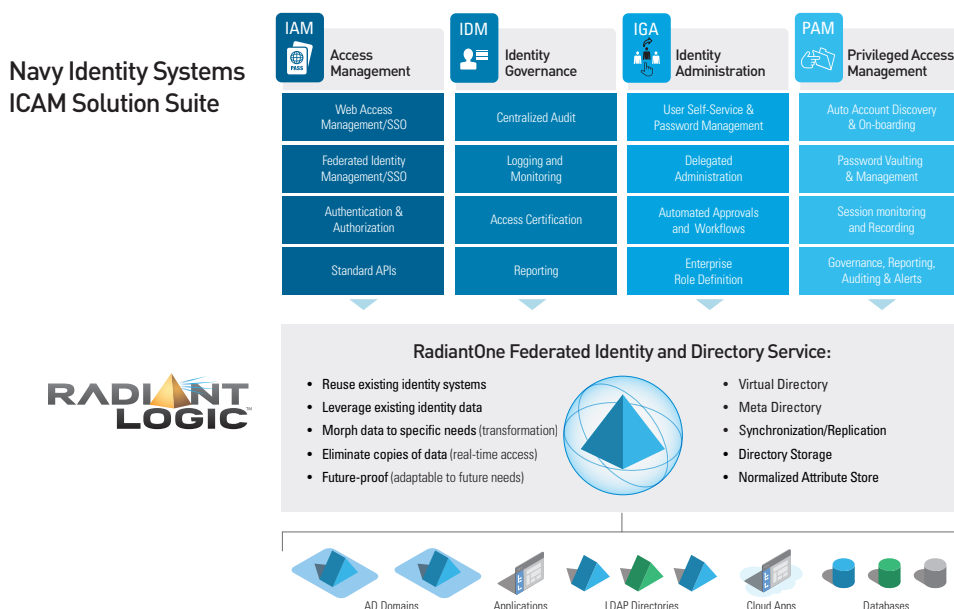- Create a foundation to make the migration to the cloud secure and easy to deploy.

Figure 3. The Federated Identity and Directory Service forms a foundation for an integrated IdAM stack, including SSO and governance

About Radiant Logic

As the market-leading provider of federated identity services based on virtualization, Radiant Logic delivers simple, logical, and standards-based access to all identity within an organization. RadiantOne FID, our federated identity and directory service, enables customizable identity views built from disparate data silos, driving critical authentication and authorization decisions for WAM, federation, and cloud deployments. Fortune 1000 companies rely on RadiantOne to deliver quick ROI by reducing administrative effort, simplifying integration, and building a flexible infrastructure to meet changing business demands. For more information, visit www.radiantlogic.com.

Contact Us

To find out more about Radiant Logic, please call us at **877.727.6442**, email us at info@radiantlogic.com, or visit www.radiantlogic.com.