Effective ICAM is Critical to Mission Success

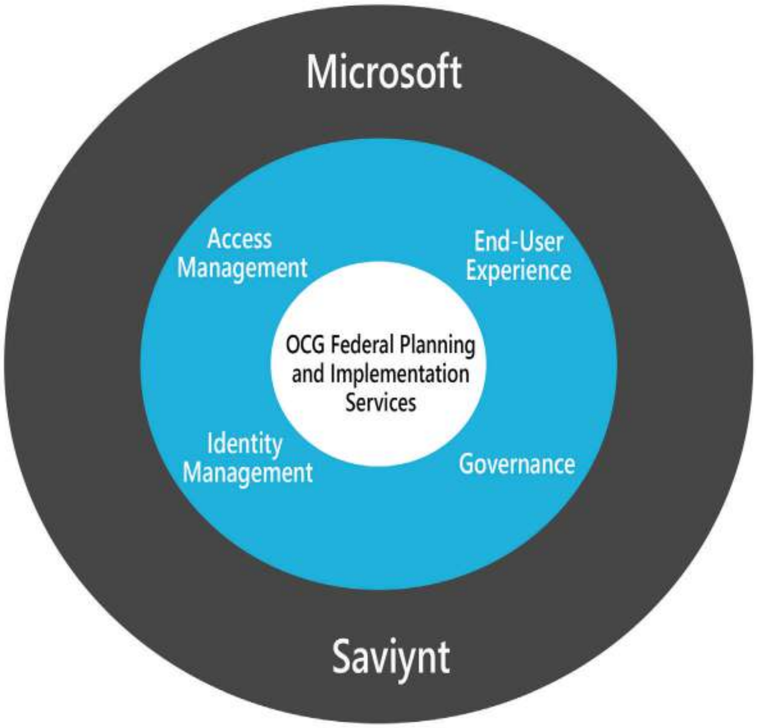
ICAM enables the ***right individual*** to access the ***right resource***, at the ***right time***, for the ***right reason***.

Adversaries, whether nation-states, criminal, or thrill-seekers, are aggressively targeting government agencies for cyber-attacks to exfiltrate data or to disrupt critical operations.

A primary target for these attackers is Federal Identity, Credentials, and Access Management (ICAM) systems. Compromising these systems enables attackers to assume the identity of federal users and can allow unfettered access to government data and systems.

At the same time, the federal government is undertaking a massive transformation from on-premises to a cloud-first infrastructure. This transformation requires a radical change in how we view ICAM as it becomes the foundation for how we secure both cloud and on-premises data and applications. This article intends to provide a roadmap to a widely accepted approach to a cloud-based identity model.

The perimeter security model no longer applies. Point solutions and multiple identity stores are no longer sufficient to properly secure identity data. Federal agencies must also comply with new requirements as they upgrade their ICAM requirements as they move to the cloud. NIST Special Publication 800-63 (Digital Identity Guidelines) outlines the technical identity requirements that agencies must follow.



Roadmap to an Effective ICAM Model

An effective ICAM program should be based on the following principles:

- Zero Trust mindset
- Single Identity Model
- Least Privilege Access
- Multi-Factor Authentication
- Risk-Based Identity Analytics
- Conditional Access

Federal Identity, Credentials, and Access Management (ICAM)

Zero Trust Mindset

Assume that you have already been breached and that all access requests are hostile. This requires continually evaluating access requests to ensure they are valid.

Single Identity Repository

Leverage a single, enterprise-wide identity repository for access across your on-premises and multi-vendor cloud environments. This enables a comprehensive set of access controls across all users and a single view of user entitlements and activities. Organizations that already have Microsoft 365 should leverage Azure Active Directory (Azure AD) as the single identity repository. All enterprises (including federal agencies) should embrace Microsoft's Hybrid approach leveraging Azure AD as the single identity repository in the cloud.

Microsoft Azure provides an easy path to move from on-premises to the cloud that allows Azure to connect to Active Directory, LDAP, SQL, or Web Services.

Least Privilege

Microsoft 365 and Saviynt provide the governance tools, including conditional access and Privileged Identity Management (PIM), to properly enforce and manage the principles of least privilege.

Multi-Factor Authentication (MFA)

Multi-Factor Authentication should be used by anyone with access to your applications or data. MFA doesn't always have to be via a phone or token, but could leverage Windows Hello to ensure a better user experience.

Risk-Based Analytics

Leveraging the single identity repository to perform risk-based identity analytics will enable organizations to focus security, compliance and management efforts on the identities that pose the most risk to the organization. Risk-based analytics will also allow for streamlining processes to improve the user experience and allow administrators to quickly identify security signals such as risky user sign-ins - all while reducing costs.

Conditional Access

Leverage Conditional Access policies based on risk-based analytics to limit access. For instance, users with a managed device would get access in accordance with their entitlements, but an unmanaged device may get read-only access. Users coming from abnormal locations may have their access limited or require an additional factor to authenticate.

Fully Integrated ICAM Solution

OCG Federal partnered with Microsoft and Saviynt to provide the solution for an effective ICAM program that meets the above criteria.

Microsoft via Azure AD provides the foundational Identity & Access Management (IAM) layer natively integrated with Azure Government Cloud to meet the appropriate compliance requirements. Saviynt natively integrates with AD to provide Identity Governance and Administration (IGA).

Why choose Oxford Computer Group and OCG Federal?

For over a decade, we have specialized in Microsoft identity, security, and governance solutions. We have an excellent track record, having won the Microsoft Partner of the Year award eight times. We were a finalist for Microsoft's Security System Integrator of the year in 2021.

We design and develop innovative solutions focused on delivering business value. We assess architectures and processes, and make recommendations designed to support strategic objectives. To accelerate deployment, we use our proven methodology, best practices, and a unique library of code developed during 900+ projects.

Get in touch!

877-862-1617
info@oxfordcomputergroup.com
www.oxfordcomputergroup.com

Microsoft OCG FEDERAL SAVIYNT