Desk Research | Internet2

Table of Contents:

The purpose of this document is to assess Internet2's competitors, products, services and sales tactics, and evaluate competitors' strengths and weaknesses relative to Internet2's IAM services.

This analysis will help SecondMuse see the unique advantage of Internet2's IAM system, as well as any potential barriers to growth. We want to use that information to make recommendations on how Internet2 may proactively strengthen its marketing, procurement and business strategies over the next 5 years. We want the recommendations we make to be rooted in the most real picture of the IAM landscape.

What is IAM?

Summary:

Identity and Access Management (IAM) is a cybersecurity framework that IT managers use to control how users access information within an organization.

It generally includes:

- SSO (single-sign on)
- 2-factor authentication
- Multi-factor authentication
- Privileged access management

The basic goal of IAM is to make sure that only the data that is necessary and relevant to a specific user is shared.

IAMs are generally provided by a third party vendor through a cloud-based subscription model, or deployed in a hybrid model or deployed on premises.

IAM frameworks perform the following:

- They determine how individuals in a system are identified
- They determine how roles are identified in a system and how they are assigned to individuals
- They add, remove and update individuals and their roles in a system
- They assign levels of access to individuals and groups
- They protect sensitive data within the system and secure the system itself.

A Deeper Dive on Global IAM Systems:

An Identity and Access Management (IAM) system is a framework for business processes that facilitates the management of electronic or digital identities. Its key components include:

1. Identity Provisioning:

- User Registration: The initial setup of a user's identity in the system.
- User Profile Management: Managing and updating user attributes and credentials.

2. Authentication:

- Single Sign-On (SSO): Allows users to access multiple applications with a single set of credentials.
- Multi-Factor Authentication (MFA): Enhances security by requiring multiple forms of verification.
- Biometrics: Uses unique physical or behavioral attributes for identification.
- Password Management: Tools and policies for secure password usage and resets.

3. Authorization:

- Access Control: Defines who or what can view or use resources in a computing environment.
- Role-Based Access Control (RBAC): Assigns access rights based on roles a user has within an organization.
- Attribute-Based Access Control (ABAC): Grants access based on a combination of attributes (user, resource, environment).

4. Directory Services:

- LDAP (Lightweight Directory Access Protocol): A protocol for organizing and finding data in a directory.
- Active Directory: A Microsoft product that manages users and computers in a network.

5. Identity Federation:

- Security Assertion Markup Language (SAML): An XML-based standard for exchanging authentication and authorization data.
- OAuth: An open standard for access delegation commonly used for token-based authentication.
- OpenID Connect: A layer on top of OAuth 2.0 that verifies the user's identity.

6. Identity Governance and Administration (IGA):

- Compliance and Auditing: Ensures that policies are followed and audits are conducted to check adherence.
- User Activity Monitoring: Monitors and logs user activities and access.
- Privileged Access Management (PAM): Manages and audits accounts and data access within an admin role.

7. Integration and API Security:

- API Gateways: Manages and secures API traffic.
- Service Providers: Third-party services that are integrated with the IAM system.

8. User Lifecycle Management:

- De-provisioning: The process of removing an identity from an ID repository and terminating access privileges.
- Identity Synchronization: Ensures that multiple systems maintain consistent identity data.

9. Security and Compliance Reporting:

- Audit Trails: Provides a record of system activity by system or application processes.
- Analytics and Reporting: Uses data analysis to detect and respond to security incidents.

10. Self-Service Capabilities:

- Password Reset: Allows users to reset their passwords without IT intervention.
- Profile Management: Enables users to manage their own profiles.

11. Scalability and Performance:

- High Availability: Ensures that the IAM system is accessible at all times.
- Load Balancing: Distributes incoming network traffic across multiple servers.

12. Standards and Protocols:

- XACML (eXtensible Access Control Markup Language): A declarative access control policy language.

13. Adaptive Access and Risk Analytics:

- Behavioral Biometrics: Analyzes patterns in user behavior to enhance security.
- Risk-Based Authentication: Adjusts authentication requirements based on the risk level of a request.

Other components of IAM systems:

SAML: Security Assertion Markup Language is an open standard for exchanging authentication and authorization data between parties, in particular, between an identity provider and a service provider.

OAuth2.0: a protocol that allows applications to obtain limited access to user accounts on an HTTP service. It is widely used for token-based authentication and plays a crucial role in Identity and Access Management (IAM) system architecture. It enhances IAM systems by providing a robust and standardized mechanism for authorization, delegation, and token-based authentication. In an IAM system, OAuth 2.0 typically integrates with components like:

- Identity Providers (IdP): Services that authenticate user identities and may issue OAuth tokens.
- API Gateway: Manages and secures API traffic, potentially performing OAuth token validation.
- Identity Store: A database or directory service where user credentials and attributes are stored.
- Applications: Web or mobile applications that rely on OAuth 2.0 to access user resources securely.

Here's how OAuth 2.0 fits into the overall IAM landscape:

1. Authorization and Delegation:

- OAuth 2.0 enables users to grant third-party applications access to their resources without sharing credentials.
- It is commonly used for delegation, where a user allows an application to act on their behalf to access data hosted by another service.

2. Token-Based Authentication:
    - Instead of using credentials, OAuth 2.0 uses access tokens to authenticate and authorize API requests.
    - This token-based approach reduces the risk associated with handling and storing user credentials.
3. Single Sign-On (SSO):
    - OAuth 2.0 can be used to enable SSO, allowing users to log in once and access multiple applications without needing to log in again.
    - OpenID Connect (OIDC), an extension of OAuth 2.0, provides authentication capabilities in addition to authorization, making it suitable for SSO.
4. Third-Party Integrations:
    - OAuth 2.0 allows easy integration with third-party applications and services.
    - Users can use their credentials from one service (like Google or Facebook) to log into another, improving the user experience.
5. Scalable and Modular Security:
    - OAuth 2.0 is designed to be extensible and supports different types of applications (web, mobile, server-side, etc.).
    - It defines various "grant types" for different use cases, such as Authorization Code Grant, Implicit Grant, and Client Credentials Grant.
6. Fine-Grained Access Control:
    - OAuth 2.0 allows users to specify the scope of access that third-party applications have to their data.
    - For example, a user might grant an application read-only access to their calendar but not to their email.
7. User Consent and Privacy:
    - OAuth 2.0 ensures that users have control over which applications can access their data and what level of access is permitted.
    - This aligns with privacy regulations and user consent requirements.
8. Risk Mitigation:
    - By using short-lived access tokens and optional longer-lived refresh tokens, OAuth 2.0 minimizes the risk of token compromise.
    - Revocation of access is also straightforward without the need for password changes.

OpenID Connect (OIDC): an authentication protocol that is built on top of the OAuth 2.0 authorization framework. It provides a secure and efficient way for applications to manage user authentication while respecting privacy and consent by allowing third-party applications to verify the identity of the user and to obtain basic profile information about the user in an interoperable and REST-like manner. OIDC is commonly used to facilitate Single Sign-On (SSO) across various applications and services.

Key aspects:

1. Components:
    - Relying Party (RP): The client application that wants to authenticate the user.
    - OpenID Provider (OP): The server that authenticates the user and issues ID tokens.
    - End-User: The individual whose identity needs to be verified.
2. Tokens:
    - ID Token: A JSON Web Token (JWT) that contains claims about the authentication event and the user. It is issued by the OpenID Provider and consumed by the Relying Party.
    - Access Token: Used by the client to access the user's protected resources.
    - Refresh Token: Used to obtain new access tokens.

3. Flows:
    - OIDC supports different flows (e.g., Authorization Code Flow, Implicit Flow) which dictate how tokens are issued and exchanged between the parties.
4. Claims:
    - Claims are pieces of information about a user (like username, email, etc.) that are encoded in the ID Token.
5. Scopes:
    - Scopes define the access level that the application is requesting from the user. Common scopes include openID, profile, email, etc.
6. Discovery:
    - OIDC providers publish their configuration in a well-known discovery document, which includes endpoints and supported features.
7. Standards Compliance:
    - OIDC is a widely-adopted standard and is compatible with a wide range of platforms and libraries.

Example of OIDC in Action:

- Request: A user tries to log in to an application (Relying Party).
- Redirection: The application redirects the user to an OpenID Provider (e.g., Google).
- Authentication: The user logs in with the OpenID Provider.
- Token Issuance: The OpenID Provider issues an ID Token and possibly an Access Token to the application.
- Verification: The application verifies the user's identity from the ID Token and logs the user in.

Why are IAM systems important?

There is increasing regulatory and organizational pressure to protect access to corporate resources.

Business leaders and IT departments bear the burden of this work.

IAMs automate what were once manual tasks and enables swift, scalable, granular access controls, as well as the ability to audit corporate access and premises in the cloud. **In short, the security landscape is complex and covers a variety of features. IAM is the scalable solution to securing these features.**

Good IAM demonstrates that its processes and technologies are actually providing a more secure environment. You do this by providing privilege tiers to your users. This gives the sense that sensitive information is being protected.

Identity and access management has become fundamental to many companies' cybersecurity strategies. IAM tools and frameworks can help with:

Regulatory compliance: Standards like GDPR and PCI-DSS require strict policies around who can access data and for what purposes. IAM systems allow companies to set and enforce formal access control policies that meet those standards. Companies can also track user activity to prove compliance during an audit.

Data security: According to IBM's *Cost of a Data Breach* report, credential theft is the leading cause of data breaches. IAM systems can add extra authentication layers, so hackers need more than just a password to reach sensitive data. RBAC policies can limit the lateral movement of malicious actors, including insider threats.

Digital transformation: With the rise of multi-cloud environments, IoT devices, remote work, and BYOD, companies need to facilitate secure access for more types of users to more types of resources. IAM systems can centralize access management for all users and resources in a network, maintaining network security without disrupting the user experience.

What is InCommon’s current IAM service offering?

- Link to all products and services
- InCommon Federation is the biggest force-multiplier and attractor to these other service components.
    - Federation
    - TAP
    - Academy
    - Catalysts
    - eduroam - InCommon runs this on behalf of Internet2. It’s an authentication service (acts like air traffic control), not a network. It runs on the network that is provided by a service provider. Someone could run it in their own home.
    - Certificates - a paid, completely standalone service. It has some connectivity to Federation. Generates revenue that fuels other components.

Internet2’s Top Competitors

Note: Internet2 has no direct competitors. Below are the top secondary/indirect competitors. These are the businesses that offer products and services that target any administrator seeking an IAM system, but are in Internet2’s general category with regard to IAM services.

Microsoft Active Directory (Azure)

- Comprehensive IAM system that is known to simplify the user authentication and access control process
  - SSO functionality, eliminating the need for remembering multiple usernames and passwords for different apps
  - Centralized location for managing user identities across resources, which allows administrators to create and manage user accounts, groups and permissions, and enforce policies and security controls quickly and seamlessly
  - MFA capabilities, which add an extra layer of security to user logins, preventing unauthorized access to sensitive data and applications
- Provides application and device management tools, allowing users to access cloud applications and enforce policies for corporate-owned and personal devices
- Good B2B and B2C collaboration features, allowing for seamless and secure collaboration between external users
- Downsides:
  - Complex to implement and the learning curve is steep
  - Cost-prohibitive:
    - Free with a 365 subscription
    - Can run up to $3.5k for enterprise and $14k for premium
  - Limited in terms of support for legacy apps
- Azure AD is a solution provider for many InCommon participants, but doesn't support SAML for federated login to their services.

AWS Cloud for Higher Ed

- Colleges and universities are digitally transforming with cost-effective, scalable, secure, and flexible Amazon Web Services (AWS) Cloud infrastructure.
- With AWS, you can support teaching and learning, connect the campus community to systems and tools, store data efficiently, make data-driven decisions to save money and resources, and accelerate research efforts.

Google IdP or Google Workspace

- A collection of cloud computing, productivity and collaboration tools, software and products developed and marketed by Google
- Consists of:
  - Gmail, Contacts, Calendar, Meet and Chat for communication
  - Currents for employee engagement
  - Drive for storage
  - Google Docs Editors suite for content creation
- An Admin Panel is provided for managing users and services
- It’s expensive. To give you a sense, BU would have had to pay $900k for 6.5 petabytes of storage for 195k user accounts (they negotiated it down to $171k for 4 petabytes, thanks to Internet2 services). Read more here.

Okta

- An enterprise-grade IAM service
- Provides cloud software that helps companies manage and secure user authentication into applications
- Helps developers build identity controls into applications, website web services and devices

- Includes Provisioning, Single Sign-On (SSO), Active Directory (AD) and LDAP integration, the centralized deprovisioning of users, multi factor authentication (MFA), mobile identity management, and flexible policies for organization security and control
    - Plays very nicely with the above competitors mentioned

Complete list of competitors:

1. Okta:
    - Overview: Okta is a cloud-based IAM solution that provides Single Sign-On (SSO), Multi-Factor Authentication (MFA), and identity lifecycle management.
    - Features: Okta supports integration with a wide range of applications, adaptive MFA, and automated user provisioning.
2. Microsoft Azure Active Directory (Azure AD):
    - Overview: Azure AD is Microsoft's cloud-based identity and access management service.
    - Features: It offers features like SSO, MFA, and integration with Microsoft 365, Office 365, and thousands of other SaaS applications.
3. OneLogin:
    - Overview: OneLogin is a cloud-based IAM solution designed to simplify identity management with secure, one-click access to applications.
    - Features: It provides SSO, MFA, and real-time Active Directory synchronization.
4. Ping Identity:
    - Overview: Ping Identity offers a suite of identity management solutions, including SSO, MFA, and access security.
    - Features: It emphasizes security for mobile and API-based applications and supports identity federation standards such as SAML and OAuth.
5. ForgeRock:
    - Overview: ForgeRock provides a comprehensive identity management solution designed to cater to a variety of businesses.
    - Features: It includes features such as user provisioning, SSO, and contextual and risk-based authentication.
6. IBM Security Identity and Access Management:
    - Overview: IBM offers a suite of IAM solutions including IBM Security Verify and IBM Cloud Identity.
    - Features: These solutions provide SSO, MFA, identity governance, and user lifecycle management.
7. Auth0:
    - Overview: Auth0 provides a platform for authentication and authorization, focusing on a seamless developer experience.
    - Features: It offers customizable login pages, social login, and support for multiple programming languages and frameworks.
8. Duo Security (now part of Cisco):
    - Overview: Duo Security provides a user-centric zero-trust security platform for all users, devices, and applications.
    - Features: Duo offers MFA, secure SSO, and endpoint security.
9. SailPoint:
    - Overview: SailPoint provides enterprise identity governance solutions with on-premises and cloud-based identity management.

- Features: SailPoint offers identity governance, password management, compliance reporting, and AI-driven recommendations.

10. LastPass (by LogMeIn):
    - Overview: LastPass is known for its password management, but also offers identity and access management solutions.
    - Features: LastPass provides password management, MFA, and biometric access on mobile devices.

General cost structures look like:

- Per User Pricing: Many IAM providers charge on a per-user basis, with costs increasing as more users are added.
- Tiered Plans: Some services offer tiered plans, where the cost per user decreases as you move to higher tiers with more features.
- Custom Pricing: For large enterprises or specific needs, providers might offer custom pricing based on negotiations and requirements.
- Free Tiers: Some providers might offer free tiers with limited features for a small number of users.

What other services are regional networks, libraries, schools, community colleges using?

Some IAM solutions now incorporate AI and ML to enable a more dynamic approach to authentication and authorization. AI can look for indicators of suspicious behavior (many failed login attempts in a short period of time, a remote user not using the company's VPN) and automatically take action like asking for more authentication factors or terminating access.

IDaaS (identity as a service) solutions are third party that deliver cloud-based identity and access management services and tools. They're gaining popularity right now.