# Cloud-based Identity Management Systems

A cloud based identity management system can be used to delegate responsibility for user registration, authentication and verification on an online platform. Cloud based identity management should reduce complexity of creating, configuring and deploying a portion of a system that handles user authentication and authorisation flows. For the purposes of this comparison, I’ve selected two cloud based providers: Microsoft Entra ID and Okta. Both platforms provide solutions that would suit use cases in an educational context.

## Features

Okta and Microsoft Entra ID provide the following features, at least which would be applicable in an educational context with emphasis on security and ease of access:

**Multifactor authentication** – where user access requires a second mode of authentication to prove who they actually are

**Single sign-on** – users sign onto a single page, and have access to the range of resources to which they have been granted

**Privileged access** – access to certain resources can be sectioned off, permitting access only based on groups and user roles

Okta provides a user friendly way to interact with their workforce identity platform via an access gateway. The access gateway provides a convenient landing page, or dashboard from where users can access a plethora of external applications via Oktas integrations (Okta, n.d.).

Microsoft Entra ID is an identity management platform that allows users to access internal and external resources, including Microsoft 365 and has integrations with a large number of SaaS applications (Microsoft, 2024).

## Security Features

Okta boast their workplace identity platform utilises zero trust when it comes to securing access to their platform (Okta). Zero trust is a security framework that essentially trusts nobody and no device on a network. With the level of traffic across an organisations cloud, and the potential for devices to move between or be connected to several clouds at a time, it’s critical for a platform to prioritise protecting its own resources, with the mindset that trust should never be presumed and should be actively monitored (Dhiman, et al., 2024).

Microsoft do facilitate zero trust as a paradigm and guide users on how to configure their tenant to employ zero trust policies (Microsoft, 2024). Both platforms have ways of configuring monitoring and alerting should trust events arise, with Okta utilising their own logging and monitoring tools, and Microsoft provide monitoring tools via Entra monitoring and health.

## Data residency

Depending on the platform, and because both solutions from Okta and Microsoft exist on the public cloud, it is possible for data to be transported between, and stored at different geographic locations, depending on the users location. Typically user data would be stored on a node as close to their location as possible to ensure fast interaction when authenticating. Prior to choosing a solution, understanding data residency of the providers platform is of importance, and this should be transparently communicated to end users of the cloud system to ensure they agree to allow their data to be stored in processed in the manners defined by each system.

With Microsoft Entra ID, data is stored at the same location as the tenant, and the customer chooses where this will be upon creation of the tenant (Microsoft, 2024).

Within Okta, it is a similar scenario where the customer selects where user data will be stored. They have customer data stores in the USA, Japan, Australia and the EMEA region. They state that customer data protection is their top priority, where they meet industry standards and are certified to comply with FedRAMP, GDPR and HIPAA to name a few requirements (Okta).

It is vital to understand exactly where and how data will be processed and stored when it comes to end user data on a public cloud. It is also of importance to gain consent from, and inform individuals when their data might have been compromised. User data is unfortunately a commodity and should be treated as such.