Case Study: National Healthcare Provider Secure Account Lifecycle Management

Background

National Healthcare Provider is the nation's premier home care provider for nuclear weapons and uranium workers. National Healthcare Provider provides in home care for workers suffering from chronic illnesses contracted in the course of their employment through an extensive nationwide network of nurses delivering quality care to enhance patient outcomes in the privacy and comfort of their own homes.

National Healthcare Provider's workforce is dynamic and primarily remote. New employees are hired daily, and existing employees often change roles within the National Healthcare Provider companies or are rehired by National Healthcare Provider after employment elsewhere. National Healthcare Provider nurses utilize mobile devices and cloud apps to provide medical services to patients, and to document patient information – which is uploaded to National Healthcare Provider's secure cloud service.

The Challenge

National Healthcare Provider uses Workday as its system of record for employee information, while Azure Active Directory (AAD) is used as their identity management platform. Management of the full user life cycle at National Healthcare Provider was a manual, time consuming and error prone process. With no integration in place between Workday and AAD employee data needed to be re-keyed into several systems. Temporary passwords were managed on a spreadsheet. Data entry mistakes and the lack of visibility between the systems created blocks to quickly and efficiently onboarding new users.

Human Resources and administrative staff were overwhelmed with user management issues, were unable to get information when they needed it, and were required to manually review system logs for errors in the user management process.

Solution

The application is centered around Workday, National Healthcare Provider's primary repository for employee information, and its integration with Azure AD enabling National Healthcare Provider to provide an automated employee life cycle management experience to its Human Resources and Information Technology staff.

When National Healthcare Provider's Human Resources staff creates a new user in Workday a new user is also created in AAD with an appropriate email address based on the new user's role at National Healthcare Provider. The new email address is written back to Workday. The new user's password is automatically re-set and emailed to the recruiters so they can inform the new user.

If a user is created in AAD in some other manner (e.g. through the Azure AAD UI or the Office Admin Center), the solution uses a custom function designed to automatically set the EmployeeID for that user when it computes a matching UPN from data it retrieves from Workday. The Workday ID gets attached

to the new employee in AAD attributes, then the user is created. AAD consumes a filtered set of attributes from Workday ensuring that an employee's personal information is protected and not consumed by AAD.

Dynamic groups in AAD are used to manage O365 licensing and security – attributes are scanned and users are added to dynamic groups where logic runs to provision licensing, security features and enable users.

Updated users are automated in a similar way. When the solution detects an updated user it automatically updates Workday or AAD regardless of where the update was performed.

The solution is designed to manage common scenarios such as multiple first/last names or UPNs by recognizing the duplicate and automatically sending an email to Human Resources alerting them to the issue and instructing them to choose a new name.

These automated actions for provisioning and updating new users in AAD are collected into an Azure Log Analytics workspace. An Alert is configured on the workspace to send emails to appropriate information technology staff when it finds errors among those actions.

Employees are allowed access to National Healthcare Provider applications and resources while they are employed. When employment is set to end and Workday has been updated accordingly, users are automatically disabled in AAD and removed from licensing groups. The user object still exists but is disabled with no licenses assigned. When an employee is rehired and Workday is updated, the user object in AAD is enabled and the appropriate licenses are assigned to the user.

Benefits

In using the Secure Account Lifecycle Management solution National Healthcare Provider gained the following benefits:

- Modernized application built on Microsoft Graph technology
- Automated management of the user account life cycle – a time consuming, error prone manual process
- Integrated with Workday
- Filtered data from Workday to provide only the data consuming applications require
    - Able to push different attributes to different applications as needed
- Automated provisioning of new accounts in Azure Active Directory (AAD) based on newly created workers in Workday
- Automated write-back of a new user's User Principle Name (UPN) into Workday as their work email address
- Automated Single Sign On (SSO) for users to log onto Workday with their AAD credentials
- Automated updating of account attributes based on values retrieved from Workday
- Automated setting of passwords on newly created accounts in AAD
- Automated notification of issues in provisioning and updating users