Cloud 9 Infosystems

Navnit Group prevents confidential data leakage using Azure Rights Management

Technology Specifications	• *Microsoft Azure Rights Management Service (Azure RMS)* • *Azure Active Directory (Azure AD)* • *Azure Directory Active Sync (AD Active Sync)*

The Navnit Group, a $100M plus integrated network of diverse companies, is a reputed and professionally managed Mumbai, India-based business and global brand. The company operates within sectors as diverse as automotive, infrastructure, marine, adventure sports, aviation and financial services. They provide a wide variety of products, services and support for dozens of franchises including but not limited to Rolls Royce, Ferrari, BMW, Hyundai, both Indian and global. They cater to the needs of their numerous upscale clients while providing a world class communications and customer experience for all.

Problem Statement

Due to the wide variety of business types, along with the strategic depth and cultural diversity of the group, they needed to ensure that they were poised for future growth, success and security. A major component for this mission critical initiative was the desire to improve upon their ability to create, share, manage and secure the documents produced in the course of their daily enterprise operations.

Navnit's communications and document ecosystem were not ideal and provided the perfect opportunity to build a state-of-the-art Document Management System that enabled the users to access, create, manage, share and protect business critical documents**.** At the top of Navnit's list of requirements was the ability to protect their enterprise assets and restrict access where needed and warranted based on company, user or document type. Data loss was also a major concern among different departments and franchisees and needed to be a part of the overall solution. There was also the need for improved accessibility tracking to identify suspicious activities from both within and outside of the organization.

Approach

Cloud 9 performed a full Enterprise assessment of the organization to understand all functional business areas and the unique document management requirements for each. Upon completion and after analysing all areas of the Enterprise, it was recommended that Navnit implement Microsoft's Azure RMS (Azure Rights Management Service). This cloud-based protection service uses encryption, identity, and authorization policies to help secure files and emails, and it works across multiple devices—phones, tablets, and PCs. Information could be protected both within and outside their organization because that protection remains with the data, even when it leaves their organizational boundaries. This enabled the customer to protect Office, pdf and image documents at the time of creation or modification and based on the source. It also enabled the customer to protect the documents based on document sensitivity and user rights.

Azure RMS ensures data is always protected – regardless of where it is stored or with whom it shared the files are encrypted for the entire lifecycle of the file. Navnit Group IT can track activities on shared

data and revoke access if necessary. IT can use powerful logging and reporting functionality to monitor, analyse, and resolve over shared data.

Navnit Group had an on-premise Active Directory Setup, and to minimize the user/group management operations for RMS, Azure AD Active Sync was setup enabling them to just manage their on-premise AD instance. Users/groups created on on-premise AD get auto-synced to Azure AD. Users need not have to maintain/remember separate passwords for Azure AD and On-premise AD, rather all on-premise user objects are synced with Azure AD, allowing them just to use one password which acts like a single sign-on.

Based on the AD Active sync configuration, Document Protection Rights could then be applied to the users on Azure AD. There were certain documents that needed to be shared only to the HOD with read-only rights, another set of documents for read-only across dealers/departments. Configurations were made to achieve this with an easy way of applying RMS protection to documents during creation or modification. By default, any document a user creates, is set to read-only for all the employees across the organization (as per the requirement.)

Users while creating their documents (based on its nature), would apply a label that would apply the configured protection rights for that document. Once the document is selected as confidential the Companies disclaimer and the watermark gets applied to the document automatically based on the configurations.

Tracking documents now enables the user/administrators to know whether the user viewed the document or not, whether the document was denied to a user who tried to access it along with the location from where the user tried to consume the document.

There were also a few labels configured based on department & dealers which enabled the document creators to select that scope while creating the document and read-only rights would be applied to a specific set of users for the appropriate department/dealers that were configured. Certain other documents were required to be shared on an ad-hoc basis with only authorized users based on the nature of the document. These documents were protected by the document owners with custom policies allowing them to send it to people within and outside the organization who had appropriate document rights.

When a user tries to open the protected document, he must first authenticate himself with his work credentials and thereafter it checks whether the user is authorized to view that document. If the user is authorized, then appropriate protections rights (assigned while creating the document) would be taken into consideration while the user is consuming the document.

Conclusion - Data Security the Navnit Way

The Navnit Group now has complete control over their most prized possession: Their Enterprise Data Assets. They are now able to provide best-in-class Global communications and Document Management practices to their employees, clients and franchises. The Navnit IT team is now able to know who accessed the file or attempted to access the file. Email notifications were set up for suspicious activity or unauthorized access. Azure RMS also allowed the team to revoke access to the file remotely if needed. They can share data safely within the organization as well as with clients and franchisees. RMS policies for auto disclaimer and watermark, when applied, allows the user to protect the confidential documents. The new policies get applied automatically and they are classified as the property of Navnit Group ensuring privacy and security.