Use Case Type	Use Case Name	Category	Decription	Business Value
Activity Monitoring / Alerts	Scheduled activity reports	Activity Monitoring	View/scheduled report showing all resource delete (and other) activities for a given time frame -View/scheduled report showing "x" activity on HIPPA docs	Forensics, Regulation, Verify all actions are valid, allow for quick remediation
Activity Monitoring / Alerts	AD activities	Activity Monitoring	View/scheduled report showing all AD activities for a given time frame	Audit, forensics - Verify appropriate group memeberships
Activity Monitoring / Alerts	Identify AD accounts that do not adhere to requirements	Activity Monitoring	Identify accounts that do not adhere to corporate standards, i.e; - password is not required	Corporate standards adherence
Activity Monitoring / Alerts	Report on unused access	Activity Monitoring	Report on unused access, i.e.; - have not logged into a domain for 90 days	Ability to restrict access to unused resources
Activity Monitoring / Alerts	Detect activity on a resource by someone not in the group the resource belongs to.	Activity Monitoring	Examples: Detect when someone not in the HR group accesses HR resources Detect when someone not in the Finance group access finance data	Ability to restrict access on a need to know basis.
Activity Monitoring / Alerts	Password Policy Changes	Activity Monitoring	Report for password policy changes record what changed, who changed it, and when	Corporate standards adherence
Activity Monitoring / Alerts	Historical data classification	Activity Monitoring	Report on data classification changes over a given time period	Allow data owners to see historical data classification changes
Activity Monitoring / Alerts	Permissions Changes	Activity Monitoring	Report on new or changed permissions over a given time frame	Allow data owners to see historical data permission changes
Activity Monitoring / Alerts	Ransomware detection/response	Activity Monitoring	Detect unusual activity (file renames, deletes) on resources and respond appropriately	Ability to stop unwanted access/changes quickly.
Activity Monitoring / Alerts	Brute force attacks	Activity Monitoring	Monitor accounts for a threshold (i.e. 50) login attempts in a designated time frame, send email/alert	Quickly identify and react to brute force access attempts
Activity Monitoring / Alerts	Failed login attempts	Activity Monitoring	Alert on failed login attempts for privileged accounts, i.e. admins	Quickly identify and react to rogue access attempts
Activity Monitoring / Alerts	Password spray attacks (using common password for many accounts, account enumeration)	Activity Monitoring	Monitor accumulated login failures over a given time period, send email/alert	Quickly identify and react to password spray attacks
Activity Monitoring / Alerts	Account Priviledges	Activity Monitoring	Alert if an account is granted "Act as operating system" priviledges	Quickly alert admins when an account is given specific priviledges
Activity Monitoring / Alerts	Account lockout	Activity Monitoring	-Monitor for accounts being locked (i.e. service accounts) out and react via email / alerts -Monitor for when account lockouts exceeds a threshold -Daily report on locked accounts	Account being locked may indicate rogue access attempts
Activity Monitoring / Alerts	Privileged/Sensitive Group membership changes	Activity Monitoring	View/report/alert on changes to privileged AD groups	Audit, forensics - Verify appropriate group memeberships
Activity Monitoring / Alerts	VIP lockout	Activity Monitoring	Monitor for certain accounts being locked out and react via Email / Alerts	Account being locked may indicate rogue access attempts
Activity Monitoring / Alerts	VIP account access attempts	Activity Monitoring	Monitor VIP account access attempts and react via email/alerts	May indicate rogue access attempts

Use Case Type	Use Case Name	Category	Decription	Business Value
Activity Monitoring / Alerts	Unapproved AD changes	Activity Monitoring	Alert on AD changes made by an "unapproved' account	Identify potential rogue behaviour
Activity Monitoring / Alerts	Detect when a resource is moved	Activity Monitoring	Detect when a resource has been moved/access rules have changed so that people can no longer access the resource	Resolve access issues quickly
Activity Monitoring / Alerts	Monitor priviledged account creation	Activity Monitoring	Alert if the number of enterprise admin accounts rises above a set threshold Alert if the number of exchange admin accounts rises above a set threshold Alert if the number of built in administrator accounts rises above a set threshold Alert if the number of domain admin accounts rises above a set threshold	Identify potential security issue
Activity Monitoring / Alerts	Monitor disabled accounts	Activity Monitoring	-Alert if the number of disabled accounts crosses a threshold in a given timeframe - Weekly report on disabled accounts	Identify potential security issue
Activity Monitoring / Alerts	Monitor deleted accounts	Activity Monitoring	Alert if the number of deleted accounts crosses a threshold in a given timeframe	Identify potential security issue
Activity Monitoring / Alerts	Detect when admin privileges are granted	Activity Monitoring	Alert when an unprivileged account has had its ACLs changed to a value that allows it to obtain administrative privileges (directly or indirectly) or is granted "act as the operating system" priviledges	Identify potential security issue
Activity Monitoring / Alerts	Account creation alert	Activity Monitoring	Alert when an account is created from a host not included in a list or from an unexpected account	Identify potential security issue
Activity Monitoring / Alerts	Group policy modifications	Activity Monitoring	Alert on GPO changes	Alert admins to potential rogue access
Activity Monitoring / Alerts				
Activity Monitoring / Alerts	Identify stale data	Activity Monitoring	Report on the locations where stale data resides	Stale Data remediation ensures unneeded data is properly archived and or removed. This space reclamation saves the organization in storage costs and potential security/access concerns
Activity Monitoring / Alerts	Password Policy changes	Activity Monitoring	Alert if password policy change is made	Alert admins to potential rogue access
Activity Monitoring / Alerts	Permissions alert	Activity Monitoring	Alert on permissions change of a file or folder	Forensics
Activity Monitoring / Alerts	Alert when a member is added or removed to/from Domain Admins	Activity Monitoring	Alert when a member is added or removed to/from Domain Admins	
Activity Monitoring / Alerts	Alert when a member is removed from Domain Admins	Activity Monitoring	Alert when a member is removed from Domain Admins	
Activity Monitoring / Alerts	Alert when a member is added to Domain Admins	Activity Monitoring	Alert when a member is added to Domain Admins	
Activity Monitoring / Alerts	Alert when an account is changed from disabled to enabled	Activity Monitoring	Alert when an account is changed from disabled to enabled	

Use Case Type	Use Case Name	Category	Decription	Business Value
Activity Monitoring / Alerts	Daily report on locked accounts	Activity Monitoring	Daily report on locked accounts	
Activity Monitoring / Alerts	Alert when a attribute "Password Not Required" is added to a user	Activity Monitoring	Alert when a attribute "Password Not Required" is added to a user	
Identity Collection	Users with password not required	Forensics	Potential candidates for password attacks.	
Identity Collection	Users with Department attribute blank	Forensics		
Identity Collection	Users not disabled AND not logged in for x days	Forensics		
Identity Collection	Identity Forensics	Permissions Analysis	Identify accounts with passwords that never expire Identify accounts where the Department attribute is blank.	Close potential security issue
Identity Collection	Users with Password Never Expires			
Identity Collection	Disabled users with password never expires			
Identity Collection	Users in groups with elevated access (domain admins, Enterprise admins etc) that have password never expires	Forensics	Potential candidates for impersonation.	
Identity Collection	Collect and analyze identities (users and groups) from one or more AD domains	Forensics	Identities can be collected from multiple connected/disconnected AD domains. If domains are trusted, one Identity collector would be able to pull identities from all connected domains.	
Identity Collection	Identify Nested groups, cyclic nested groups	Forensics	Identity groups that are nested within other groups.	Permission overloading, messy Active directory, Difficult to maintain.
Identity Collection	Identify empty groups	Forensics	Identify groups that don't have any members	
Permissions Collection	Externally shared resources	Other	Report showing resources shared with external users	Data owners can be aware of who has access to data
Permissions Collection	Unique permissions	Other	Report on sensitive resources with unique, direct, orphaned or missing permissions	Data owners can be aware of who has access to data
Permissions Collection	Normalization	Permission Analysis	Normalize AD users/groups based on data access	Provide information needed to normalize AD groups
Permissions Collection	How does someone get access to a sensitive resource?	Permissions Analysis	View/report showing how someone is receiving access to a resource, i.e. direct, inherited, etc.	Ability to manage access on a need to know basis
Permissions Collection	View user/group permissions	Permissions Analysis	-Show resources visible to a user or group on a single endpoint -Create Permissions reports for different types of access to HIPAA info. ---Domain != AD (so local server accounts with access) any Full Control, etc. etc.	Audit, forensics - Verify appropriate permissions
Permissions Collection	Scheduled permissions report	Permissions Analysis	View/scheduled report showing permissions for a designated folder	Audit, forensics - Verify appropriate permissions
Permissions Collection	Scheduled permissions changes report	Permissions Analysis	View/scheduled report showing permissions changes over a given time period and who made the change	Audit, forensics - Verify appropriate permissions

Use Case Type	Use Case Name	Category	Decription	Business Value
Permissions Collection	Access to sensitive data report	Permissions Analysis	View/scheduled report/Alert showing who has access to sensitive data for a given timeframe	Verify appropriate access
Permissions Collection	Identify overexposed data	Permissions Analysis	Identify resources where too many people have access. For Example: Report on resources that have access to groups like Everyone, Authenticated Users	Ability to restrict access on a need to know basis.
Permissions Collection	Identify stale permissions	Permissions Analysis	identify permissions that are assigned to resources based on timeframe and usability	Ability to restrict access on a need to know basis.
Permissions Collection	Report on accounts with elevated access	Permissions Analysis	Report on users/groups having elevated access (modify, full control) on data	Forensics & Compliance
Permissions Collection	Report on permissions assigned to users directly at different levels of folder hierarchy	Permissions Analysis	Report showing permissions assigned to users directly on folders and at any hierarchy of the business resource structure.	Identity outliers to permission model.
Permissions Collection	Report on permissions assigned to local groups/users	Permissions Analysis	Report showing permissions assigned to local users/group on a file share or O365 endpoint.	Forensics & Compliance, restrict access
Permissions Collection	Permissions assigned to empty/nested/cyclic nested groups	Permissions Analysis	Report showing permissions assigned to groups that are a member of other group	Forensics & Compliance,
Data Classification	Locate sensitive data	Data Classification	View/report on the location of sensitive data - Credit Card Data - SSNs - Addresses - etc	Audit, Compliance
Data Classification	Who has access to sensitive data?	Data Classification	View/report on who has access to sensitive data	Audit, Compliance
Data Classification	Classify data based on content type	Data Classification	Classify files based on filetype and/or file attributes Classify Using Keyword - Classify data based off word or phrase list Classify Using OOTB Policy Expressions - Classify data using built-in Policy expressions Classification Categories - Ability to use OOTB and/or custom categories to classify data	The ability to know where files exist based on specific criteria can help administrators understand where application files are being stored. Allows for understanding of whether the files potentially contain sensitive data
Data Classification	Classify data based on behavior	Data Classification	Classify content based on behavioral attributes	Audit, Compliance
Data Classification	Classify files based on content & behavior	Data Classification	Classify content based on both content and behavior of activities on the content	Audit, Compliance
Data Classification	Classify files based on Microsoft AIP labels	Data Classification	Collect AIP labels from the documents scanned and provide ability to report based on them. Applicable to SharePoint Online, OneDrive.	Audit, Compliance
Data Ownership	Identify owner based on usage (Behavioral Classification)	Data Ownership	Identify owner based on usage, i.e if 75% of the people that use a resource belong to a group, maybe the manager of that group should be the data owner	Ability to manage data ownership

Use Case Type	Use Case Name	Category	Decription	Business Value
Data Ownership	Manual data ownership assignment	Data Ownership	Assign data ownership manually	Ability to manage data ownership
Data Ownership	Data ownership certification campaigns	Data Ownership	Establish ownership so that: · Somebody can authorize or decline to authorize access to resources · Owners can see who has been using their data · Owners can be alerted to data changes · GRC/Audit can enforce Access Certification Campaigns where Data Owners certify the current access to their resources. · Establish ownership based on activity data from Activity Monitoring/Data Classification · Establish ownership based on election processes o Voting process on who should own the Data	Ability to manage data ownership
Data Ownership	Identify data owners via election	Data Ownership	Identify data owners by conducting an owner election process when there is no defined way to identify owners.	Ability to manage data ownership
Data Ownership	Automatic data ownership management	Data Ownership	Update owners to business resources (folders) automatically when the owner goes through life cycle changes (mover/leaver)	Automatic ownership management
Access Certification	Certify permissions to over-exposed data	Access Certification - Permissions	Review and certify permissions assigned to Authenticated Users, Everyone and groups that have more than 25% of the organization's population	Reduce data vulnerability
Access Certification	Certify permissions to sensitive resources based on level of sensitivity	Access Certification - Permissions	Identify High/Medium/Low sensitive resources. Review and certify access to these resources based on their sensitivity.	Identify highly sensitive resources and secure access to it.
Access Certification	Certify stale permissions	Access Certification - Permissions	Review and certify stale permissions. Campaign can be configured in a way to remediate permissions that were rejected by the reviewer.	Maintain optimal access to business data. Follow the model: "Right group/user has the right access at the right time for the right duration"
Access Certification	Certify permissions assigned to users directly	Access Certification - Permissions	Review & certify permissions assigned to business resources/files to users directly. This is mostly against an organization's permission model.	Identity outliers to recommended permission model.
Access Certification	Certify permissions assigned to specific groups (ex: groups with elevated access)	Access Certification - Permissions	Review & certify permissions assigned to a specific set of groups.	Ensure elevated groups have the right access.
Access Certification	Certify permissions assigned to empty groups (groups containing no members of all inactive members)	Access Certification - Permissions	Review & certify permissions assigned to groups that don't have members or has all inactive members.	Data cleanup
Access Certification	Certify permissions assigned to disabled users	Access Certification - Permissions	Review & certify permissions assigned to users that are in a disabled state.	Data cleanup

Use Case Type	Use Case Name	Category	Decription	Business Value
Access Certification	Access revocation post access review	Access Certification - Permission revocation	Revoke permissions rejected by access reviewers post access review.	Maintain the right permissions to business resources
Access Certification	Certify members of elevated groups	Access Certification - Group membership	Review and certify members of specific groups (ex: domain admins, enterprise admins etc)	Ensure the right people are members of elevated groups.
Access Certification	Membership revocation post access review	Access Certification - Membership revocation	Revoke membership decisions rejected by access reviewers post access review	Maintain the right set of members in groups that have elevated permissions.
Access Request & Fulfillment	Normalize permissions to key business data	Access Normalization	Identify key business data and owners to that are responsible to take access decisions to that data. Normalize access permissions to the data.	Easily maintainable access to key business data. Single path to access assignment.
Access Request & Fulfillment	End user request access to shared drives	Access Request - Shared Drives	Enable access request handling to shared drives. Automatically grant access to shared drives upon receiving necessary approvals.	Reduce number of help desk tickets. Quick on-boarding of new team members. Increased productivity.
Personalized user experience	Align the business website with the customer's theme	Personalization	Re-brand parts of the business website to be aligned with the organization's look and feel	Unified end-user experience
Data Enrichment	Enrich identity & permissions reports	Identity & permissions data enrichment	Enrich identities with relevant information obtained from IGA and/or other external data sources. This attribute data is further used in permissions & activity reports.	Consolidated view of permissions to unstructured data grouped by fields obtained from IGA or other external sources (ex: Department, job code, location)
Data Enrichment	Enrich activity data	Activity Enrichment	Enrich activity data with relevant information obtained from IGA and/or other external data sources. This attribute data is further used in activity reports.	Consolidated view of activities being performed on unstructured data grouped by fields obtained from IGA or other external sources (ex: Department, job code, location)