Azure Application Registration Permissions for Collect

The Collect application in RelativityOne is a tool designed to streamline the data collection process for eDiscovery. Its primary purpose is to gather data from various sources, such as cloud-based applications and other data repositories, in a manner that is secure, defensible, and efficient. Collect aims to reduce the time and effort involved in data collection, ensuring that the data is accurate and complete, while maintaining chain of custody and compliance with legal and regulatory requirements.

Due to the architecture of the Collect application, Delegated permission can't be used and are not supported. The Collect application requires the use of Microsoft Graph API Azure Application permissions to facilitate the collection of data that occurs in processes running in the background.

The Collect application requires specific Graph API Application permissions be granted to an Azure Application Registration to facilitate efficient and comprehensive data collection for e-discovery and compliance purposes.

Following is an explanation of each Azure application Graph API permission required and why it is needed to support collections of M365 data:

1. **Calendars.Read:** This permission allows Relativity to access calendar events. For e-discovery, it's important to capture calendar data as it can provide crucial context, timelines, and evidence related to the case or investigation.
2. **Contacts.Read:** This permission allows access to contacts and is necessary to gather information about communications and relationships between individuals, which can be critical in understanding the full scope of interactions and connections in an investigation.
3. **Files.Read.All:** This permission enables Relativity to access all files in OneDrive and SharePoint. It is essential for collecting documents, spreadsheets, presentations, and other files that might contain relevant information for a legal matter or compliance review. This permission is also required to support collection of linked OneDrive and SharePoint files in Outlook emails and Teams chats.
4. **Mail.Read:** This permission allows access to emails, which is one of the core components of e-discovery. This permission allows Relativity to read email messages in users' mailboxes to identify, preserve, and analyze communications that are pertinent to the case.
5. **Sites.Read.All:** This permission allows Relativity to access all SharePoint sites, including content and metadata. It ensures that any relevant information stored in SharePoint sites can be collected and reviewed.
6. **User.Read.All:** This permission provides access to read the properties and membership of users. It is useful for identifying and understanding the roles, permissions, and activities of different users within the organization, which can be relevant for investigations and compliance checks.
7. **ChannelMessage.Read.All:** This permission provides access to all messages in Microsoft Teams channels. It allows Relativity to capture and review conversations and discussions that take place in Teams channels, which may contain pertinent information for legal or compliance purposes.
8. **Chat.Read.All:** This permission enables Relativity to read all chat messages in Microsoft Teams. This includes private chats between users. Access to these messages is essential for gathering complete communication records and ensuring that no relevant information is overlooked in an investigation.

9. **Group.Read.All:** This permission allows Relativity to read all groups in the directory, including their properties and memberships. It helps in understanding the structure and membership of various groups within the organization, which can be important for context in e-discovery and compliance scenarios.
10. **TeamsTab.Read.All:** This permission allows Relativity to read the properties of all tabs in Microsoft Teams. Tabs can contain important resources, documents, and tools that users interact with. Access to this information can provide additional context and insights into the work and communications of users.
11. **Team.ReadBasic.All:** This permission allows Relativity to read basic properties of all Teams. It helps in identifying and understanding the different Teams within the organization, their purposes, and their memberships, which can be relevant for investigations and compliance checks.
12. **ChannelMember.Read.All:** This permission provides access to the membership information of all Teams channels. It allows Relativity to see who is part of each channel, which can be important for understanding who had access to certain communications and information during an investigation.
13. **Full_access_as_app Permission:** The Microsoft Graph API doesn't support accessing Outlook Online Archives (Archived Mailboxes). We utilize Microsoft's Exchange Web Services (EWS) API to collect Archived Mailboxes.