NTFS (New Technology File System) is the default file system of modern Windows, including Windows 10. It provides several security features (Microsoft, 2021a). Privileging, determining which users or groups can access or modify files or folders. Auditing, which logs access and changes to files or folders. Security Descriptors, consisting of user access identifiers for Access Control Lists, and control lists for accessing and auditing policies. Additionally, Security Descriptors allow file permissions to be defined. Files within the NTFS file system are also individually encrypted using the Encrypted File System, or EFS (Microsoft, 2023b).

Privileging is used in conjunction with the User Right’s found within Access Control Lists (Microsoft, 2023c). Privileges are held by a caller (Microsoft, 2023d). Privileges dictate system-level permissions of users and groups, such as the ability to modify any file even in cases where File Permissions may not permit such. Consequently, they are closely tied to the File System and provide an additional layer of security. Privileging was introduced alongside Access Control Lists in Windows NT 3.1 with NTFS. Earlier file systems, such as FAT (File Allocation Table) did not include privileging (Microsoft, 2008).

Auditing works in conjunction with security descriptors. If auditing is enabled for an object or event, then the security descriptor for the file will include an SACL (System Access Control List) (Microsoft, 2009). This informs which actions should be audited. When an action that should be audited occurs, then a record is created in the Security-category of Window’s Event Viewer. This record includes information about the user, action preformed, and time occurred. Administrators may specify which objects are audited, including by whom and which user-class, as well recording of the permissions that led to that to that event being generated (Microsoft, 2022). Auditing was introduced apart of Windows NT 3.1 which released in 1993. The capabilities were enhanced in subsequent releases, with Windows NT 3.5 and Windows NT 4.0.

Security Descriptors are a critical component of security in the NTFS. They enforce access controls and file permissions.