Summary: Limitations of Native Mailbox Access Auditing Tools

Netwrix Auditor vs. Built-in Tools

Need	Netwrix Auditor	Native Mailbox Access Auditing
Reporting of non-owner mailbox access, who accessed what mailboxes	**Yes**	Yes, but difficult to analyze because event logs contain a lot of low-level information and noise.
Automatically delivered daily e-mail reports showing all changes made in the last day	**Yes**	No.
Ability to clearly distinguish between access to calendar and mailbox folders	**Yes**	No.
Consolidation of audit data	**Yes**	Ability to analyze events only on one file server at a time (no centralized audit data archive).
Detailed information on access to e-mail folders and specific messages (who accessed or changed what folders/messages and when)	**Yes**	No.
Ability to specify what mailboxes and users to monitor	**Yes**	No.
Prevention of audit data loss as a result of security log overwrites	**Yes**	No, defined by maximum log size and generally can hold no more than a week of audit records. Can enable automatic archiving of event logs when they are full, but need to clean them or otherwise they will fill up all available dsk space.
Long-term archiving capabilities	**Yes.** Saves required information on events to a compressed file-based storage that can support up to 7 years or more of audit data	No. Requires large amounts of disk space (no compression) to store logs. Logs require maintenance to avoid filling disk space. No retention rules.