cloudficient

What Microsoft 365 activity history can reveal about matter scope

Retained and indexed audit records can give legal teams context on sources, relationships, and custodians during the case window.

A current list of custodians, repositories, owners, and permissions describes part of the environment. It does not necessarily show how people interacted with Microsoft 365 locations and files during the case window.

Available audit records may provide information about events associated with users, files, repositories, access, and sharing. Beyond the value of mapping what files and repositories a person of interest may have accessed during the relevant case window, the logs may help to identify the contemporaneous version of a linked file or the fact that said version no longer exists. The logs may also allow legal teams to more accurately and defensibly determine the scope of preservation and collection.

Build a matter-specific view of activity

Audit records are not organized around a matter. Selected activity must be considered alongside the custodian population, case window, organizational information, interviews, known sources, and other facts developed related to the matter.

This can help the legal team investigate:

- Which repositories were associated with activity during the case window
- Which custodians may have accessed matter-related repositories and/or files
- Whether custodians used shared or group-owned locations
- Whether access or sharing events point to additional people, files, or sources
- Whether observed relationships extend beyond individual ownership

The resulting data map is matter-specific. It may change as interviews identify additional participants, activity points to shared locations, or the case window is refined.

Permissions and activity answer different questions

Information	What it may help show
Repository ownership	Who owns or administers a location
Permissions	Who may have been able to access it
Recorded activity	Events associated with particular users, repositories, or files
Sharing activity	Recorded sharing events and associated changes to access, where available

Recorded activity does not independently establish relevance or legal scope. An access event does not prove what someone read, understood, or relied upon. An absence of recorded activity does not prove that no interaction occurred.

Activity should be considered alongside matter facts, custodian knowledge, organizational information, record availability, and legal judgment.

Can the available history support matter decisions?

When analyzing and evaluating the usefulness of audit history, consider four questions:

Availability
Will potentially useful records remain accessible when a matter arises?

Attribution
Can selected events be associated with identifiable people, repositories, or files?

Connection
Can the activity be considered alongside interviews, organizational information, known sources, and the case window?

Application
Can the resulting information support investigation of identification, preservation, and collection scope?

The team should also understand which periods, workloads, and event types the available records cover. Those boundaries affect what conclusions the activity can support.

Retention and indexing serve different purposes

Retention
Keeps Microsoft 365 activity history available beyond the period for which it might otherwise remain accessible.

Indexing
Makes selected activity searchable and usable within a matter.

Data mapping
Connects that activity to people, repositories, files, events, and the case window.

Legal judgment
Determines what the resulting information means for identification, preservation, and collection.

History that was not retained cannot be investigated later. Retained history that cannot be searched or connected to a matter may provide limited help when discovery decisions are being made.

NEXT STEP

Using Microsoft 365 Audit History for Matter-Driven Data Mapping

A practical guide to retaining Microsoft 365 audit history, indexing selected activity, building a matter-specific data map, and using available relationships to inform identification, preservation, and collection decisions.

Request the guide →