Global Digital Forensics · Guide edition 2026-11-03 · evestigate.com/insights/cloud-tenant-first-source-map/

CLOUD COLLECTION PLANNING

Mapping Cloud Evidence Across Multi Tenant Environments and Acquired Businesses Before Collection Begins

Litigation, a regulator's inquiry or an incident that touches several business units will reach into tenants nobody at headquarters administers, each with its own retention clock already running. Inventory the tenants and their logs before collection starts, then call (800) 868-8189 at any hour.

Published September 5, 2026 · Updated October 30, 2026

By Joseph Caruso, Founder, CEO and CTO, Global Digital Forensics

The Complexity of Multi Tenant and Post Acquisition Cloud Environments

Enterprises that have grown through mergers, acquisitions or decentralized regional operations rarely house all of their digital evidence inside a single, uniform cloud tenant. A parent corporation may run an enterprise Microsoft 365 environment with ninety day audit retention, while a recently acquired subsidiary operates on an unintegrated Google Workspace domain, an independent AWS account or a basic Microsoft licensing tier where detailed mailbox auditing was never enabled. When litigation, regulatory scrutiny or a security incident strikes across business units, a tenant by tenant inventory reaches every custodian and record source across the units, well beyond what one central administrator sees.

How a Cloud Source Map Protects Counsel and Security Leaders

Working directly for retained counsel, internal audit and corporate security teams, Global Digital Forensics conducts rapid cloud evidence source mapping engagements at the outset of complex matters. We inventory every active and legacy tenant, identity federation boundary, administrative role owner, licensing tier and log retention clock across the organization and its subsidiaries. By documenting what each cloud provider records, how long those logs survive and what export rate limits apply before collection starts, we give trial attorneys and compliance officers a verified roadmap of the evidence position at the start of the matter.

© 2026 Global Digital Forensics, Inc. All rights reserved.

What a Source Map Records

A cloud source map is a verified inventory that comes before collection. For each business unit it records the identity provider and its federation boundaries, every Microsoft 365, Google Workspace, AWS, Azure or Google Cloud tenant and account, the license tier of each, the administrators who can export from it, the audit and sign in logs it generates, the retention period of each log, whether any log is forwarded to a SIEM or archive, and the export method and rate limit for each source. It also records which activities each source logs, so counsel knows on day one when a subsidiary on a basic license has mailbox auditing disabled and can plan around it.

The map works from the records within retention on the day it is built. For any log that aged out earlier, the gap register records the date and the secondary copies we look for, such as a SIEM, an archive or a prior export, so counsel addresses it directly. Services that were never connected to the identity provider, the shadow IT a regional office adopted on a corporate card, are traced through DNS, proxy and cloud access security broker logs. We ask about those logs because they often expose a source the enterprise did not know it had.

The value of the map for counsel is precision in the hold notice and the preservation letter. A hold that names every tenant, the specific logs to be preserved and the administrator responsible for each is a record of reasonable steps under Rule 37(e). Naming the sources turns a general instruction to preserve all relevant data into a specific plan IT can carry out, and that specificity is counsel's footing against a spoliation argument. Our cloud and SaaS forensics page describes the providers and record types this inventory covers. Precision in the hold is also what lets counsel answer a preservation challenge with a document rather than a narrative, and the map is that document.

Retention Schedules the Providers Publish

The urgency behind a source map comes from provider documentation rather than from us. Microsoft's audit log retention policies describe the Unified Audit Log as retained for 180 days on the standard tier, with one year and longer available through the appropriate licensing and configured retention policies. The Entra data retention reference lists sign in and audit log retention at seven days on the free tier and thirty days with Premium licensing. Google's data retention and lag times page lists retention per Workspace log type, with many retained for six months.

Those numbers vary tenant by tenant inside one enterprise. A parent on an E5 license with a one year audit retention policy and a SIEM may sit beside an acquired company on a Business Basic license with no retention policy and a Google Workspace domain that was never migrated. The map records the verified configuration of each, because headquarters settings often differ from those in the subsidiary where the custodians work. Where a subsidiary is a regulated financial services entity, its own obligations under 23 NYCRR Part 500 may have produced logs held at the subsidiary level.

Infrastructure accounts have their own clocks. AWS CloudTrail, Azure Activity Log and Google Cloud audit logs are retained for short default periods, and longer where the account owner configured export to storage, and the account owner in an acquired engineering team may be a departed founder. We identify those owners, confirm what has been exported, and recommend immediate retention changes under counsel's

© 2026 Global Digital Forensics, Inc. All rights reserved.

direction where a default period is about to close on something the matter needs. The map lists each such account with its owner and its clock, so every deadline is written down. Departed owners are escalated to counsel the same day.

Building the Map, Phase by Phase

The first phase is discovery through people. We interview the identity team, the administrators of each known tenant, the corporate development group that handled acquisitions and the security team that runs the SIEM, and we review the identity provider's application and federation inventory. Every acquisition in the relevant period gets a line item: what the acquired company ran, what was migrated, what was left in place and who holds the credentials. This phase routinely surfaces tenants that the general counsel's office did not know existed, and it protects the client by converting assumption into inventory before anyone relies on it.

The second phase verifies each source against the provider's own admin console or API. We confirm the license tier, the audit configuration, the retention policies, the forwarding destinations and the administrator roster, and we test an export from each to learn its format, rate limits and completeness. Verification matters because the interview answer is often what the configuration was supposed to be, and the console shows what it is. Each verified source enters the map with a hash of the configuration export and the date verified, so the map itself can be defended as a record.

The third phase is the gap register and the preservation plan. Sources whose retention is about to expire are flagged for immediate export, sources with disabled logging are flagged for enablement under counsel's direction, and sources with no reachable owner are flagged for escalation. The deliverable is a map that names every source, every clock, every owner and every action, and it becomes the backbone of the hold notice and the collection plan. Our guide to reconciling Teams, Slack and email collections picks up where the map leaves off. The gap register is reviewed with counsel before any collection begins.

Using the Map in Due Diligence, Litigation and Incident Response

For counsel in litigation, the map is the exhibit that shows preservation was systematic. It supports the Rule 26(f) conference, where the parties address preservation and the form of production under Rule 26, and it lets counsel negotiate custodians and date ranges from a position of knowledge. When an opposing party asserts that a source must exist, the map is where counsel checks whether it does, what it retains and when it expires, and that answer is far stronger coming from a verified inventory than from an administrator's recollection at a deposition. It also narrows the negotiation to sources that actually exist.

For a security lead, the map is an incident response asset. The first hours of an incident are consumed by the question of which tenant holds the relevant logs and who can export them, and a map built in calm conditions answers it in minutes. Our forensic readiness planning service builds the map as a standing document, and our guide to preserving evidence during incident response describes how it is used when the clock is running and containment and preservation compete for the same administrators. A security team that already knows its clocks and owners spends those hours preserving rather than searching.

For a transaction team, the map is the diligence finding that reveals how an acquisition target actually logs and retains. A target with no audit retention and departed administrators holding root credentials is a different risk than its security questionnaire suggests, and the gap register becomes a list of integration tasks with a

© 2026 Global Digital Forensics, Inc. All rights reserved.

cost attached. Our cyber due diligence page and the guide to diligence before close describe that use in detail. Deal teams that run the map before signing learn what integration will cost, and those that run it afterward learn what the incident response plan should add, so the earlier the map is built the more it protects the client.

Preparing Your Tenant Inventory for Rapid Preservation

To accelerate a multi entity cloud examination, gather a list of all primary and secondary email domains, federated identity providers such as Okta or Entra ID, archive appliances and the designated Global Administrators for each business unit. Our guide to reconciling Teams, Slack and email collections covers the checks that follow once the map is built.

Whenever a high stakes dispute or cross entity incident arises, call Global Digital Forensics at (800) 868-8189 to lock down volatile multi tenant records while the rolling retention windows are open. The initial consultation is free.

Fields the Source Map Records for Every Tenant

A source map draws its value from the fields it verifies. This table lists what the map records for each tenant and infrastructure account, where that fact is confirmed and why counsel needs it in the hold notice or the collection plan. The verification column matters because the interview answer is usually the intended configuration and the console shows the real one. Read the last column as the sentence counsel can write into the preservation letter once the field is complete.

Fields verified for each cloud source, where each is confirmed and its use in the hold and collection plan.

Map field	Where it is verified	Why counsel needs it
Tenant identity and license tier	Admin console license summary	Sets the retention window and the export tools available
Administrator roster	Role assignments in the identity provider	Names the person the hold notice instructs and the deposition may call
Audit configuration	Audit settings and mailbox auditing status	Records whether item level access logging is enabled
Retention clock for each log	Provider documentation against tenant settings	Fixes the deadline for each export
Forwarding to SIEM or archive	Diagnostic settings and connector inventory	Reveals copies that outlive the tenant retention
Export method and rate limit	A test export from the source	Drives the collection schedule and its cost
Owner reachability	Corporate development and HR records	Flags departed founders holding root credentials
Gap register entry	Comparison of expected and verified sources	Records each source's status and the reason for it before anyone asks

© 2026 Global Digital Forensics, Inc. All rights reserved.

How to Begin and What Happens on the First Call

Bring a list of business units and acquisitions in the relevant period, the identity providers in use, the known tenants and their administrators, any SIEM or archive the security team operates and the matter's date range. The examiner asks what question the matter will need to answer, which custodians and units are implicated, whether a hold has issued, what retention settings are known and where the gaps are suspected. The conversation produces a written proposal that names the sources to be verified, the preservation exports to be made immediately, the interviews required and the form of the map and gap register, with timing driven by the number of tenants and the availability of their administrators. The initial consultation is free. Call (800) 868-8189 at any hour.

Technical References and Further Reading

Primary sources and provider documentation behind this guide: Microsoft Purview Audit and Google Workspace audit tools.

Authorities cited in this guide: Microsoft Purview audit log retention policies. Establishes the 180 day standard retention of the Unified Audit Log and the licensing needed for longer retention, as published by Microsoft and consulted October 2026. Microsoft Entra data retention reference. Establishes the seven and thirty day retention of Entra sign in and audit logs by license tier, as published by Microsoft and consulted October 2026. Google Workspace data retention and lag times. Establishes per log retention periods for Google Workspace audit data, as published by Google and consulted October 2026. Federal Rule of Civil Procedure 26. Governs the discovery conference at which preservation and the form of production are addressed, current text at Cornell LII.

FREQUENTLY ASKED

Questions Counsel and Security Leaders Ask About Cloud Collection Planning

What is a cloud evidence source map?

A verified inventory of every cloud tenant, identity provider and infrastructure account across an enterprise and its subsidiaries, recording for each the license tier, the logs it generates, how long each log is retained, who can export it, how the export works and which records fall outside retention. It is built before collection so counsel and the security team know what exists, what is about to expire and who must act, and it becomes the basis for a precise hold notice and a scoped collection plan.

© 2026 Global Digital Forensics, Inc. All rights reserved.

Do we need a map before issuing a litigation hold?

A hold can and should issue immediately when litigation is anticipated, and the map should follow quickly so the hold can be made specific. A general hold notice tells people to preserve, and the retention policy in a subsidiary's tenant and the clock on an infrastructure log are changed by administrators acting on specific instructions. The map identifies the policies and clocks that need action and the administrators who must take it, and the supplemental hold then names them.

Can you recover audit logs that already expired?

Once the provider's retention period has passed, we look for copies elsewhere: a SIEM or log analytics workspace, a storage account or bucket configured for export, a backup appliance, a managed service provider's archive or a prior export made for a compliance audit. The map records those secondary locations, and the gap register records the result plainly so counsel can address it from the start.

How is a recently acquired subsidiary handled?

As its own entry with its own clocks. We identify what the subsidiary ran before the acquisition, what was migrated, what still runs in its original tenant and who holds administrative credentials, including departed founders or former IT contractors. We verify its license tier and audit configuration directly, because a subsidiary's settings usually differ from the parent's, and we flag any source whose administrator has moved on for counsel to escalate.

What drives the cost of building a source map?

The number of business units and acquisitions in scope, how many distinct providers and tenants exist, how well the identity provider documents federation, whether administrators are available for interviews and console verification, and whether the engagement includes immediate preservation exports or only the inventory. A single tenant enterprise is a short engagement. A holding company with a dozen acquisitions and departed administrators is a longer one. The initial consultation is free and produces a written proposal.

Web Addresses for the Sources Cited

1. Rule 37(e): https://www.law.cornell.edu/rules/frcp/rule_37
2. audit log retention policies: https://learn.microsoft.com/en-us/purview/audit-log-retention-policies
3. Entra data retention reference: https://learn.microsoft.com/en-us/entra/identity/monitoring-health/reference-reports-data-retention
4. data retention and lag times: https://support.google.com/a/answer/7061566
5. 23 NYCRR Part 500: https://www.dfs.ny.gov/cybersecurity/23-NYCRR-Part-500
6. Rule 26: https://www.law.cornell.edu/rules/frcp/rule_26
7. Microsoft Purview Audit: https://learn.microsoft.com/en-us/purview/audit-solutions-overview
8. Google Workspace audit tools: https://support.google.com/a/answer/9725452

Reviewed by Joseph Caruso, Founder, CEO and CTO, CISSP. Last reviewed October 31, 2026.

© 2026 Global Digital Forensics, Inc. All rights reserved.

Start With a Free Consultation

The initial consultation is free, and requests are handled in confidence. On the first call a senior member of our team listens to the question you need answered, identifies the records and systems involved, and recommends the next step.

Call (800) 868-8189, answered 24/7, request a consultation at evestigate.com/contact, or email info@evestigate.com.

© 2026 Global Digital Forensics, Inc. All rights reserved.