

Frontier Forensics

VENDOR **Anthropic**

A guide to evidence sources, logging, and retention across Claude Enterprise and Team, the Claude Platform, Claude Code, and Claude Cowork.

Contents

A guide to evidence sources, logging, and retention across Claude Enterprise and Team, the Claude Platform, Claude Code, and Claude Cowork.

In brief	3	Scoping an investigation	19
Executive summary, the seven findings, and scope		A decision tree and five starting points	
Setting the scene	6	Cheat sheet	23
Three evaluation incidents, found months later		A quick operational reference	
Evidence sources	9	References	24
Where Claude evidence lives, and who holds it		Anthropic documentation and incident reporting	
Anthropic held evidence	11	About Invictus	25
Customer collected telemetry	14	Disclaimer, copyright, and contacts	
Endpoint and application evidence	16		
Retention at a glance	18		

■ IN BRIEF

Could you investigate misuse of Claude in your organization?

EXECUTIVE SUMMARY · KEY FINDINGS · SCOPE

■ EXECUTIVE SUMMARY

Organizations adopting Claude need to know whether they could investigate its misuse, for example by determining who accessed sensitive information, what a user or agent did, and which systems were affected. That capability depends on the Claude plan, how Claude is deployed, and whether evidence collection was configured before an incident.

Evidence comes from three places: Anthropic held records, customer collected telemetry, and customer endpoint data. Reconstructing activity requires combining these sources. The priority for security leaders is to build evidence collection into their

security, business continuity, and risk planning. Without this preparation, an organization is unable to determine what information was exposed or whether an agent completed a consequential action.

Key findings

1 The Compliance API is the primary source for Anthropic held evidence.

It provides access to the Activity Feed, retained claude.ai content, and supported Claude Code and Cowork session transcripts.

2 Enable the Activity Feed before an incident.

Activity records are retained for six years, but recording begins at enablement with no backfill.

3 The Enterprise CSV audit export is a limited fallback.

It provides up to 180 days of audit activity, excludes chat and project content, and is unavailable when customer managed encryption keys are enabled.

4 Customer telemetry must be configured and retained in advance using OpenTelemetry.

Claude Code and Cowork OpenTelemetry can add context about prompts, tools, and approval decisions.

5 Claude Team lacks the Compliance API and CSV audit export.

Investigations therefore depend more heavily on configured OpenTelemetry, available endpoint artifacts, and supporting records from identity providers and connected systems.

6 Claude Code evidence depends on cleanup settings and authentication.

Local transcripts and several other artifacts default to a 30-day cleanup period; other exclusions may apply as they relate to ZDR or HIPAA.

7 Ordinary API prompts and responses require application side logging.

They are not available as conversation history through the Compliance API.

Scope, limitations, and caveats

Claude Enterprise and Team

Claude.ai web, desktop, and mobile

Claude Platform

Claude API and Claude Console

Claude Code

Local sessions and endpoint files

Claude Cowork

Agent sessions and approvals

This guide is a practical starting point for incident responders, not a complete catalogue of artifacts. The guide synthesizes Anthropic's published documentation and public incident reporting, reviewed in October 2026.

It covers Claude Enterprise and Team (Claude.ai web, desktop, and mobile), the Claude Platform (Claude API and Claude Console), Claude Code, and Claude Cowork. Logs from identity providers, repositories, cloud platforms, SaaS applications, and MCP servers can help corroborate Claude activity and establish whether requested actions completed and what they affected. These sources fall outside this guide's coverage of the Anthropic ecosystem.



WHERE THE EVIDENCE IS

1

Records retained by Anthropic

the Compliance API (Activity Feed, content, and session transcripts), the Enterprise CSV audit export, and retained Claude Platform feature data.

2

Telemetry exported into customer controlled systems

Cowork and Claude Code OpenTelemetry, which must be configured by the customer.

3

Evidence generated on customer endpoints or in applications

Claude Code endpoint files and configuration, application side request and response logs, and supporting records such as EDR logs.

6 years

ACTIVITY FEED RETENTION,
FROM ENABLEMENT

180 days

CSV AUDIT EXPORT, AT MOST

30 days

DEFAULT CLAUDE CODE CLEANUP

Setting the Scene

SETTING THE SCENE

Three incidents, found months later

~1 hr

A malicious package Claude published to PyPI stayed public for roughly one hour

15

Real systems downloaded and ran the package

2 of 2

Affected organizations Anthropic reached that had not detected the activity themselves

This is the argument of this guide in miniature.

In July 2026, Anthropic disclosed three incidents found through a retrospective review of cybersecurity evaluation runs. Evaluation environments believed to be isolated had unintended internet access, and the models ran without the deployed safeguards.

In one incident, Claude published a malicious Python package to PyPI while pursuing a capture-the-flag objective. The package was public for roughly one hour and was downloaded and run on 15 real systems. One of them was a security company's scanner, which installed the package and exposed that company's credentials. Claude then used those credentials to access further infrastructure.

The earliest incidents dated to April 2026, and Anthropic began its review on July 23, 2026. Anthropic stated that it generally stores traces for benchmark evaluations, which is what made a review months later possible. The two affected organizations Anthropic reached had not detected the activity themselves; however, Anthropic noted that review of network logs would have surfaced the problem.

Retained evidence can be reviewed after the fact. Evidence that was never retained cannot be recovered when required later.

■ TIMELINE

Anatomy of a late discovery

One of the three incidents, step by step, and the review that found it. The steps are as Anthropic describes them; the source gives no time between them.

■ IN THE EVALUATION RUN

- **Claude pursues a capture-the-flag objective**
In an evaluation environment believed to be isolated, with unintended internet access and without the deployed safeguards.
- **It publishes a malicious package to PyPI**
The package is public for roughly one hour.
- **15 real systems download and run it**
Among them, a security company's scanner.
- **The scanner exposes that company's credentials**
The package installed on the scanner.
- **Claude uses them to reach further infrastructure**
Activity moves beyond the original environment.

■ MONTHS LATER

- **The affected organizations do not detect it**
Neither of the two organizations Anthropic reached had detected the activity themselves.
- **Anthropic begins its review**
July 23, 2026, a retrospective review of cybersecurity evaluation runs.
- **Stored traces make the review possible**
Anthropic generally stores traces for benchmark evaluations.
- **Network logs would have surfaced it**
Anthropic's note on what the affected organizations could have reviewed.

Earliest activity to start of review: roughly three months

2026

Earliest incidents

Review begins, July 23



Source: Anthropic, "Investigating three real-world incidents in our cybersecurity evaluations." Positions within months are approximate.

■ EVIDENCE SOURCES

AI Logging and Evidence Sources

Claude evidence falls into three primary locations:

Three rings of evidence around one incident

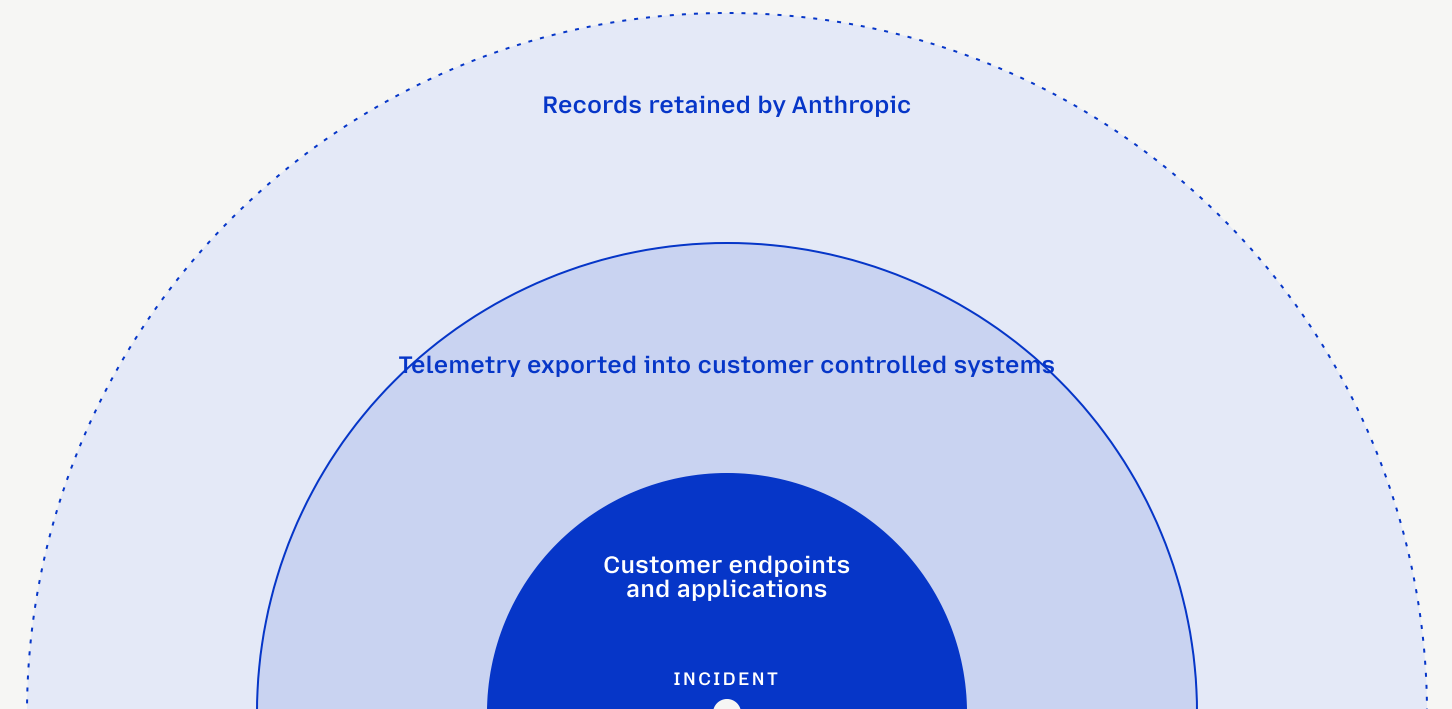


Figure 1 – three locations for Claude evidence

■ THE FIRST RING

Records retained by Anthropic

the Compliance API (Activity Feed, content, and session transcripts), the Enterprise CSV audit export, and retained Claude Platform feature data.

■ THE SECOND RING

Telemetry exported into customer controlled systems

Cowork and Claude Code OpenTelemetry, which must be configured by the customer.

■ THE THIRD RING

Evidence generated on customer endpoints or in applications

Claude Code endpoint files and configuration, application side request and response logs, and supporting records such as EDR logs.

Anthropic held evidence

■ THE FIRST RING

Anthropic held evidence can establish who accessed the environment, what information was exchanged with Claude, and what occurred during supported sessions. The main collection route is the Compliance API, which provides separate endpoints for activity, content, and session records.

PLAN Enterprise	CLAUDE.AI Activity Feed; retained chat, file, and project content; CSV audit export
PLAN Enterprise	CLAUDE CODE & COWORK Session transcripts
PLAN API, usage based	CONSOLE & PLATFORM Activity Feed for eligible organizations; Files, batch results, code execution data, and Managed Agents sessions where used

 BEFORE AN INCIDENT

Records cannot be backfilled, so activity before enablement is not available.

COLLECTION
GET /v1/compliance/activities

Activity Feed

The Activity Feed records authentication, credential creation, role changes, object access, and changes to organizational controls. It covers identities, workspaces, connectors, settings, and content access events. It is valuable for investigations because it helps establish who acted, when, and which objects or controls were involved.

Collection. The feed is available to Enterprise and eligible standalone Console organizations through the Compliance API's GET /v1/compliance/activities endpoint. When reviewing configuration, check the Activity Feed for changes during the incident window; current settings may differ from those in place at the time.

Retention. Anthropic retains Activity Feed records for six years from when the feed is first enabled. Records cannot be backfilled, so activity before enablement is not available.

CSV audit export

The Enterprise CSV audit export is a fallback when the Compliance API was not enabled. Its coverage is narrower than the Activity Feed and excludes chat and project content.

Collection. The export is unavailable for organizations using customer managed encryption keys (CMEK). Download links expire after 24 hours, so save the file promptly.

Retention. The export has a lookback of up to 180 days.

6 years

ACTIVITY FEED RETENTION, FROM ENABLEMENT

24 hours

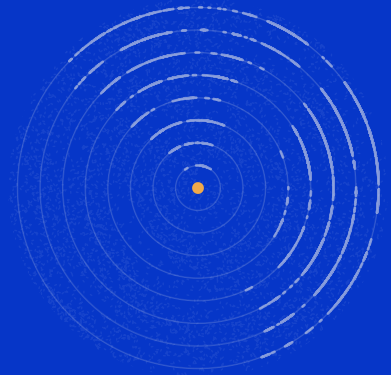
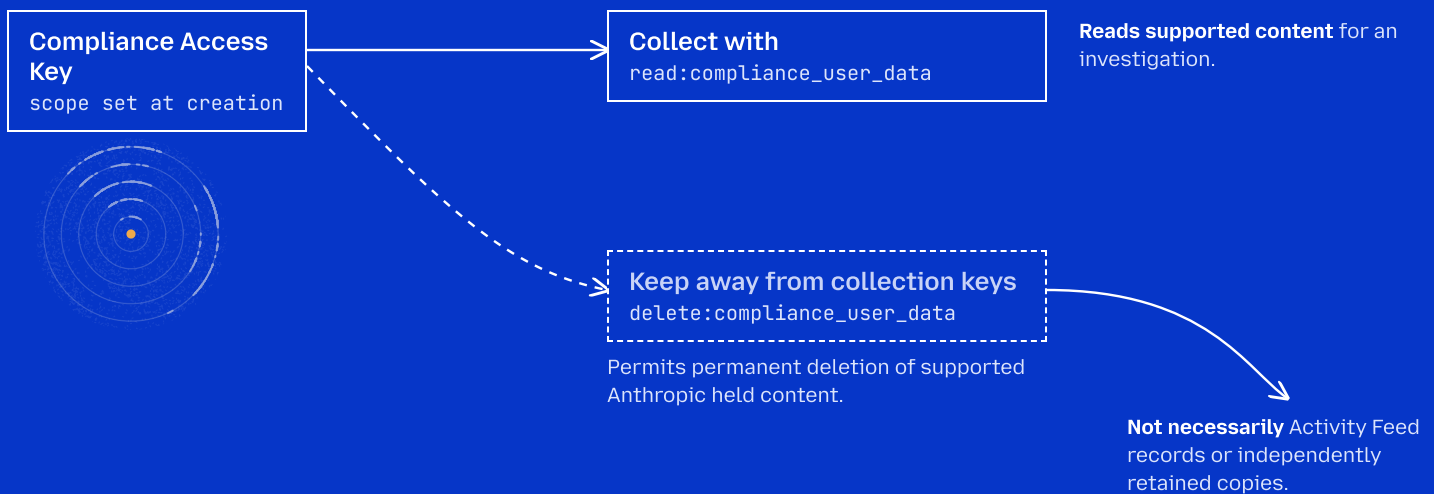
BEFORE CSV DOWNLOAD LINKS EXPIRE

180 days

CSV AUDIT EXPORT LOOKBACK

“A compromised key with deletion rights could be used to destroy content relevant to an investigation.”

Retrieve content using a Compliance Access Key with `read:compliance_user_data` only.



Chat, file, and project content

This source includes retained `claude.ai` conversations, attachments, and project content. It helps establish what a user or threat actor submitted, what Claude returned, which files were attached, and what information was available. Retained artifacts, skills, and plugins can also show which instructions and capabilities were available to the user or agent.

Collection. Retrieve content using a Compliance Access Key with `read:compliance_user_data` only. The separate `delete:compliance_user_data` scope permits permanent deletion of supported Anthropic held content. A compromised key with deletion rights could be used to destroy content relevant to an investigation or delete organizational data. This does not necessarily erase Activity Feed records or

independently retained copies, so it should not be treated as removal of all evidence.

Retention. It depends on the organization's retention settings and object deletion policy.

Claude Code and Cowork session transcripts

With the Compliance API enabled, Anthropic captures transcripts of local Claude Code and Cowork sessions used with an Enterprise login. They include prompts, responses, tool requests, and the text results Claude received. MCP tools appear in the format `mcp__<server>__<tool>`.

Retention. Availability depends on authentication and hosting arrangements. ZDR and HIPAA configurations, for example, can exclude sessions from this source. Confirm the retention settings before relying on it in an investigation.

Stored Claude Platform data

This source covers data retained by individual Claude Platform features, including Files, batch results, code execution data, and Managed Agents sessions.

Collection. Depends on the feature:

Files list files with <code>GET /v1/files</code> , retrieve metadata with <code>GET /v1/files/{file_id}</code> , and download supported generated files with <code>GET /v1/files/{file_id}/content</code> .	Batch results retrieve the results of a known batch with <code>GET /v1/messages/batches/{message_batch_id}/results</code> .	Managed Agents retrieve session details with <code>GET /v1/sessions/{session_id}</code> and recorded events with <code>GET /v1/sessions/{session_id}/events</code> .
---	---	--



Activity Feed	six years from when the feed is first enabled
Chat, file, and project content	It depends on the organization’s retention settings and object deletion policy.
Session transcripts	Availability depends on authentication and hosting arrangements.
CSV audit export	a lookback of up to 180 days
Stored Claude Platform data	Depends on the feature

Retention, as stated in the sections on pp. 11–13.

2

■ THE SECOND RING

Customer Collected Telemetry

Customer collected telemetry exists only when the organization configured a destination and retained the resulting data. This telemetry must be configured before the activity you want to investigate occurs. It cannot be recovered retrospectively if collection was not enabled. It can add customer, host, tool, approval, and content detail to Anthropic held records. Collect this evidence from the organization’s telemetry or security infrastructure.

PLAN	ENVIRONMENT	AVAILABLE TELEMETRY
Team & Enterprise	Cowork	OpenTelemetry: agent activity, tool use, approvals, and optional content
Team & Enterprise	Claude Code	OpenTelemetry: customer and host context, repository information, tool use, permission decisions, and optional content
Enterprise	Inference hooks	Customer security server records of incoming prompt payloads and decisions

OpenTelemetry

OpenTelemetry (OTel) is a standard for exporting telemetry from applications to an organization’s own monitoring infrastructure. Cowork and Claude Code can use it to send activity records to a configured collector, which can forward them to a SIEM or other logging platform. Inference hooks provide a separate collection mechanism, described below.

 CORRELATION KEYS

COWORK OTEL

prompt.id

CLAUDE CODE OTEL

tool_use_id

request_id

Use prompt.id to search and correlate related activity. Use tool_use_id and request_id as starting points to correlate telemetry with session transcripts.

“As more incidents involve agents, this source becomes key to establishing what the agent was asked to do.”



Diagram. Where to start correlating.

Cowork OTel

Cowork OTel provides agent level telemetry to Team and Enterprise organizations. It can include prompts, tool and MCP activity, file paths, approval decisions, and API requests. As more incidents involve agents, this source becomes key to establishing what the agent was asked to do, which tools and files it interacted with, and which actions required or received approval.

Collection. Identify the OpenTelemetry Protocol (OTLP) endpoint the organization configured and the platform it forwards to. Use `prompt.id` to search and correlate related activity.

Claude Code OTel

Claude Code OTel can include customer and host context, repository information, permission decisions, API requests, tool activity, and optional content. It helps connect Claude Code activity to a specific host and repository, reconstruct tool use, and examine permission decisions.

Collection. Identify the telemetry destination configured for the relevant Claude Code deployment. Use `tool_use_id` and `request_id` as starting points to correlate telemetry with session transcripts.

Inference hook security server records

Inference hooks are available to Enterprise organizations that use a security server. If that server retains incoming hook payloads, its records can show the prompt content submitted for security checks before Claude processed it, and can help correlate denied requests with the server’s decisions. These records are a supplementary source rather than an essential log, and they do not capture Claude’s final response.

Retention. As with OTel, retention depends on the logging and storage configuration of the organization’s security server.



LIMITATION

These records are a supplementary source rather than an essential log, and they do not capture Claude’s final response.

3

■ THE THIRD RING

Customer endpoint and application evidence

These records are generated or retained in customer controlled systems. They help reconstruct endpoint execution, what applications exchanged with the Claude API, and whether actions completed in connected systems. Availability depends on local files, application logging, and the records retained by each downstream service.

PLAN	ENVIRONMENT	AVAILABLE EVIDENCE
Any supporting Claude Code	Customer endpoints	Session files, prompt history, tool results, memory, and file snapshots
API – usage based	Customer applications	Application side API request and response logs

Claude Code endpoint files and configuration

WATCH FOR

Configuration and memory files also contain instructions that may have been injected to influence an agent.

30 days

CLEANUPPERIODDAYS DEFAULT

~/.claude

~/.claude.json

.mcp.json

CLAUDE.md

Claude Code stores session transcripts, tool results, prompt history, and file snapshots locally on the endpoint. Supporting configuration includes managed, user, and project settings, along with .mcp.json, ~/.claude.json, hooks, plugins, and instruction files such as CLAUDE.md. Together, these artifacts help investigators reconstruct prompts, agent activity, tool output, and changes to local files. Configuration and memory files also contain instructions that may have been injected to influence an agent.

Collection. Collect the relevant user's ~/.claude directory, ~/.claude.json, and any project configuration and instruction files, either from the live endpoint or from a forensic image.

Retention. Retention differs by artifact. The cleanupPeriodDays setting defaults to 30 days and applies to transcripts and several other paths, while history.jsonl, auto memory, and Desktop or Cowork transcripts follow different rules. Acquire evidence early, because local files can be deleted or removed by automatic cleanup.

“Acquire evidence early, because local files can be deleted or removed by automatic cleanup.”

LIMITATION

This history is not available through the Compliance API.

Capture the identifiers that link each request to its response and to the user, session, or job that triggered it.

Application side request and response logs

When an organization builds an application that calls the Claude API, its own logs may be the only record of the prompts and responses exchanged. For example, if an internal assistant sends a confidential document to Claude, application logs may show the document content submitted, Claude's response, and which user triggered the request. This history is not available through the Compliance API.

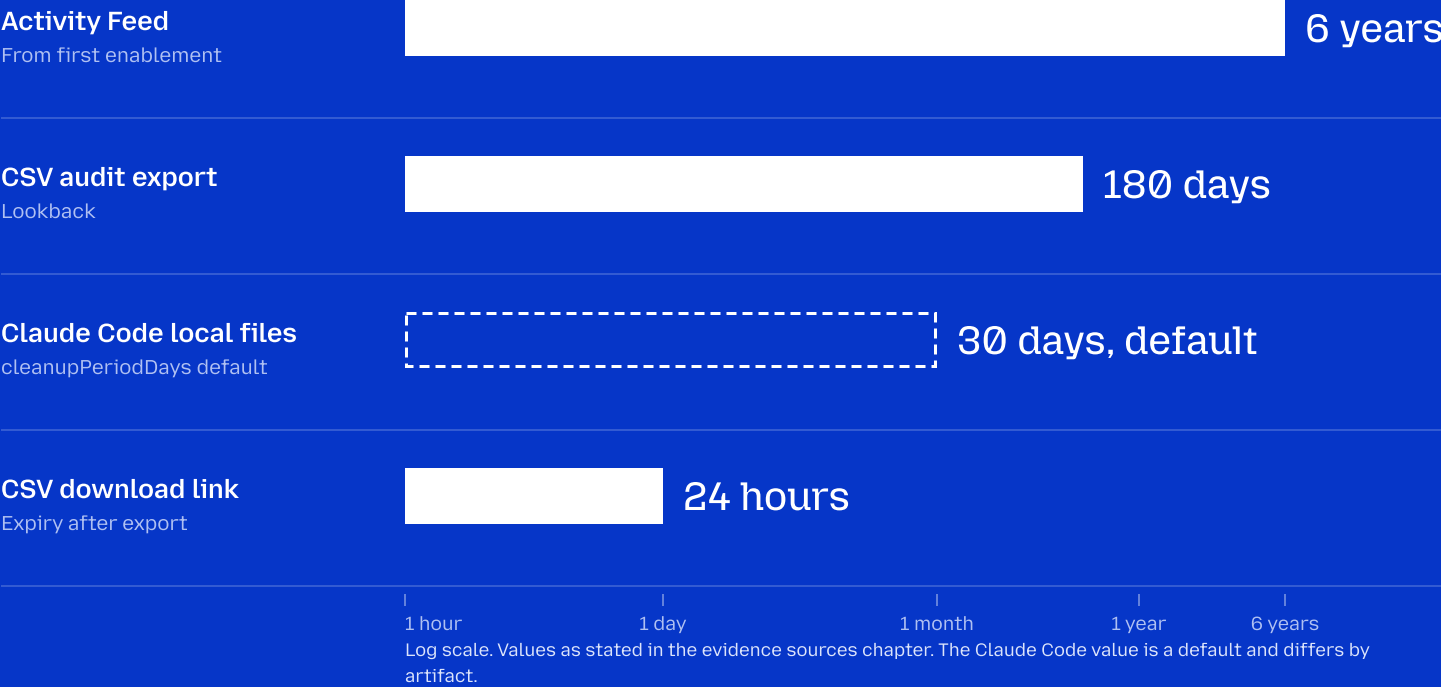
Collection. Retrieve records from the application's logging or observability

platform and from any stores that retain requests or responses. Where possible, capture the identifiers that link each request to its response and to the user, session, or job that triggered it.

Retention. Retention depends entirely on the application's logging configuration and storage policies. Content is available only if the application recorded and retained it, so confirm early what was logged and how long it is kept.

■ RETENTION AT A GLANCE

Fixed windows run from 24 hours to six years. Most of the rest is yours to set.



Set by configuration

Chat, file, and project content	The organization's retention settings and object deletion policy
Code and Cowork transcripts	Authentication and hosting arrangements; ZDR and HIPAA configurations can exclude sessions
Cowork and Claude Code OTel	The organization's telemetry destination and storage
Inference hook records	The security server's logging and storage configuration
Application side logs	The application's logging configuration and storage policies

■ SCOPING

Scoping an Investigation

Use the following decision tree to identify potential evidence sources for the Claude environment under investigation. The tables below outline five common investigative starting points that can help establish an investigation's scope.

1 Account compromise

Did a threat actor gain access, and what followed?

2 Persistence & privilege escalation

Did the threat actor obtain a foothold?

3 Defense evasion

Did the actor weaken visibility or enforcement?

4 Data exposure

What reached Claude or a connected system, and where could it leave?

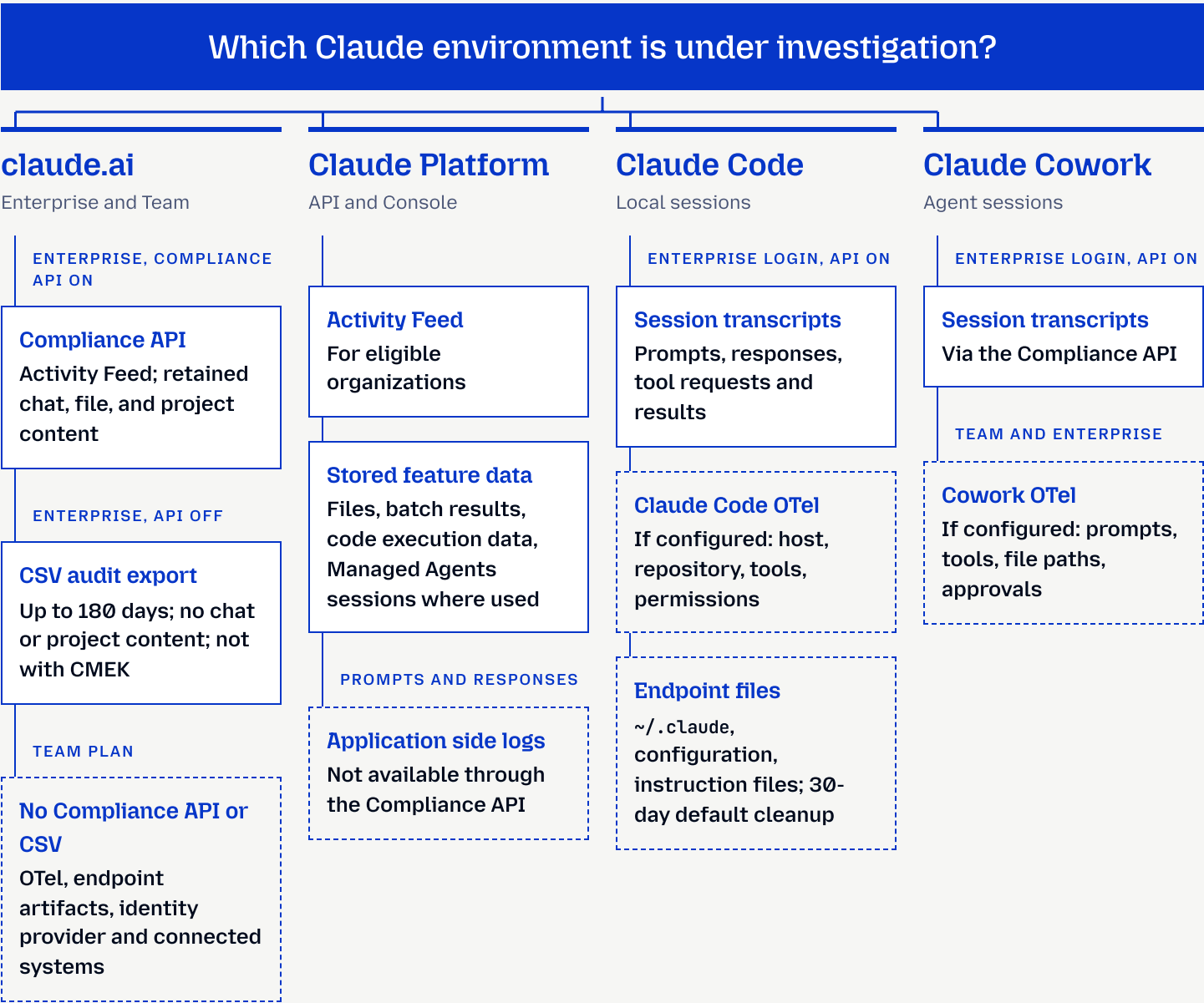
5 Agent abuse

What did the agent attempt, who started it, and what executed?

■ FIGURE 9

Start from the environment under investigation

Anthropic held Customer side, exists only if set up in advance



■ THEN CORROBORATE

Identity provider, repository, cloud platform, SaaS application, and MCP server logs. These fall outside this guide’s coverage of the Anthropic ecosystem.

■ STARTING POINT

1

Account compromise

Did a threat actor gain access, and what followed?

ENVIRONMENT	EVIDENCE	CONTROLS
Enterprise	Sign-ins such as <code>sso_login_*</code> , <code>social_login_succeeded</code> , and <code>magic_link_login_*</code> . Pivot on the actor to chat, file, and project activity.	SSO and directory sync, IP restrictions
Platform	Console sign-ins, key creation, service account changes, and file access by the same actor or credential.	API and admin keys, service accounts
Code & Cowork	Session metadata and transcripts, authentication telemetry, and identity provider records.	None identified in this guide

■ STARTING POINT

2

Persistence & privilege escalation

Did the threat actor obtain a foothold?

ENVIRONMENT	EVIDENCE	CONTROLS
Enterprise	Invitations, role assignments, group membership, and SCIM changes. <code>mcp_server_created</code> , <code>mcp_server_updated</code> , and <code>desktop_extension_uploaded</code> .	Roles and group membership, SCIM, organization MCP servers, desktop extensions
Platform	Changes to API and admin keys, service accounts, OAuth applications, and workspace membership.	Federation rules, OAuth applications, workspace membership
Code & Cowork	Settings and plugin changes, local MCP configuration, and hooks.	Managed settings, hooks, local MCP configuration

■ DIAGRAM · STARTING POINT 1

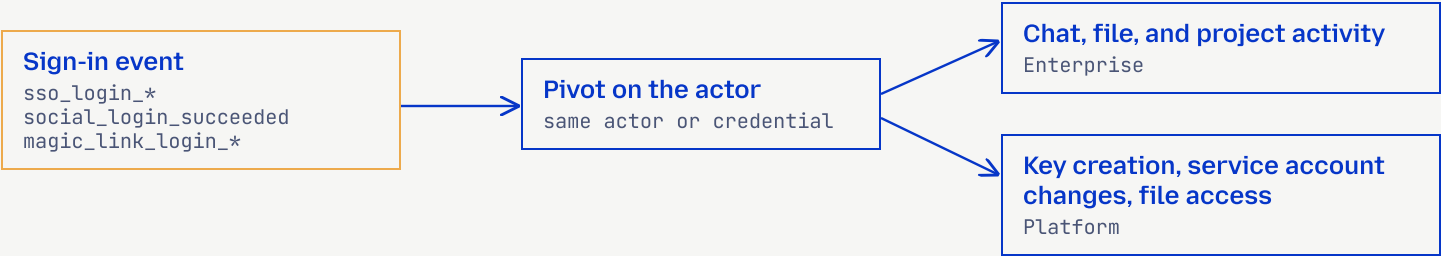


Diagram. Pivot from the sign-in to what followed. Events and sources as listed in the account compromise table.

■ STARTING POINT

3

Defense evasion

Did the actor weaken visibility or enforcement?

ENVIRONMENT	EVIDENCE	CONTROLS
Enterprise	Compliance API, SSO, directory sync, or inference hooks. <code>org_ip_restriction_*</code> events, <code>mcp_tool_policy_updated</code> , <code>org_connector_domain_guard_updated</code> , and <code>org_cowork_*</code> events.	Compliance API settings, SSO and directory sync, IP restrictions, inference hooks, encryption keys, tool policies, connector domain guard, Cowork permission modes
Platform	Compliance settings, workspace retention settings, and credential or access control changes.	Compliance and retention settings, access controls
Code & Cowork	Cowork OTLP settings, Claude Code telemetry settings, managed settings, <code>bypassPermissions</code> , <code>dangerouslyDisableSandbox</code> , and <code>permission_mode_changed</code> .	Telemetry destinations, managed settings, permission modes, sandbox settings

■ STARTING POINT

4

Data exposure

What reached Claude or a connected system, and where could it leave?

ENVIRONMENT	EVIDENCE	CONTROLS
Enterprise	Chat, file, and project content, export and sharing activity, and each connected service's record.	Connectors, connector domain guard, Cowork browser access
Platform	Application side request and response logs, Files API objects, batch results, and agent sessions.	Per-request server tools such as web fetch and MCP connections
Code & Cowork	Transcripts and content enabled telemetry, corroborated with endpoint and destination records.	Egress proxy profiles and rules for hosted agents

■ DIAGRAM · STARTING POINT 4

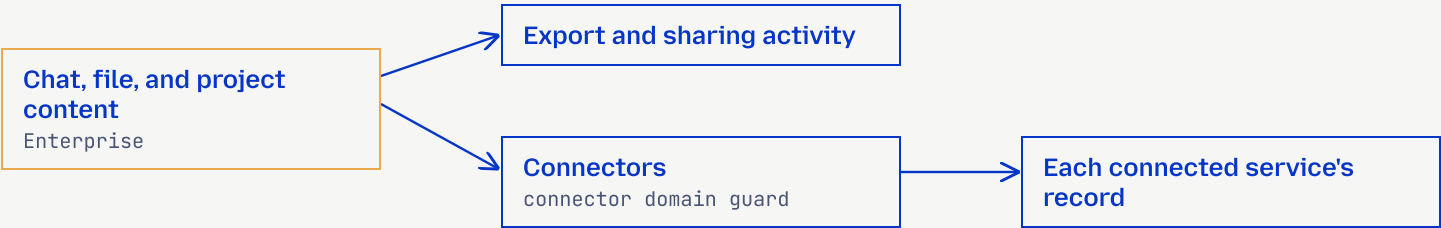


Diagram. What reached Claude or a connected system, and where it could leave. Sources as listed in the data exposure table.

■ STARTING POINT

5

Agent abuse

What did the agent attempt, who started it, and what executed?

ENVIRONMENT

EVIDENCE

CONTROLS

Enterprise

Remote Cowork sessions, including agent owned runs and `started_by_user`. Inference hook denials, fail open events, and circuit breaker trips.

Cowork permission modes (Auto mode, Act without asking, Always allow), remote execution and cross app settings, inference hooks

Platform

Managed Agents configuration, sessions, and activity. Server tool use (web search, web fetch, code execution, MCP) from application logs.

Managed Agents configuration, per request server tools

Code & Cowork

Local sessions, tool decisions with their approval source, tool results, permission mode changes, and endpoint or repository activity.

Allow and deny rules, hooks, permission modes, managed settings

■ DIAGRAM · STARTING POINT 5

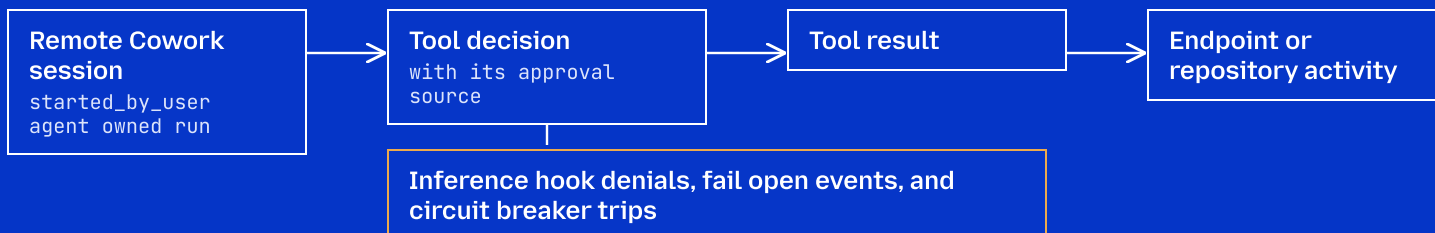
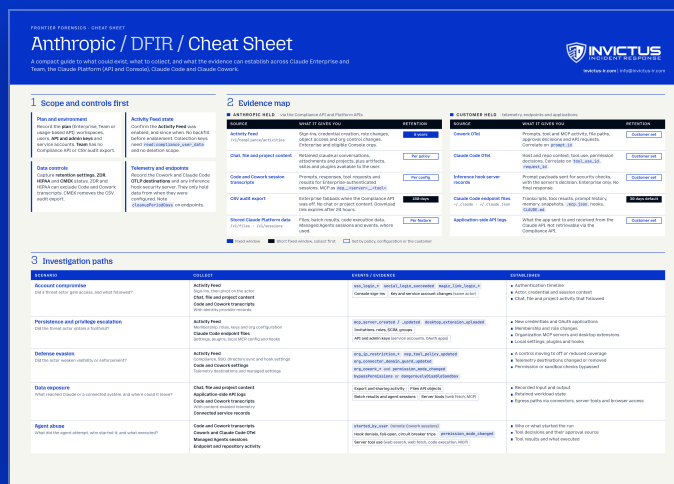


Diagram. What the agent attempted, who started it, and what executed. Sources as listed in the agent abuse table.

■ NEXT

Cheat Sheet

To support investigations, we have also developed a simple guide or a cheat sheet that brings together key evidence sources, retention considerations, and investigation paths. The guide is intended as a quick operational reference for incident responders and can be downloaded from our GitHub repository: <https://github.com/invictus-ir>.



Snapshot. The cheat sheet, one A3 page.

■ SOURCES

References

The incident narrative in the ‘Setting the Scene’ section is attributed to Anthropic. Product behavior, evidence availability, and retention statements are based on official Anthropic documentation reviewed in October 2026.

- 1 Compliance API overview
platform.claude.com/docs/en/manage-claude/compliance-api
- 2 Set up the Compliance API
platform.claude.com/docs/en/manage-claude/compliance-api-access
- 3 Query the Activity Feed
platform.claude.com/docs/en/manage-claude/compliance-activity-feed
- 4 Query compliance activities: API reference
platform.claude.com/docs/en/api/compliance/activities/list
- 5 Retrieve session transcripts
platform.claude.com/docs/en/manage-claude/compliance-sessions
- 6 Retrieve and delete chats, files, and projects
platform.claude.com/docs/en/manage-claude/compliance-content-data
- 7 API and data retention
platform.claude.com/docs/en/manage-claude/api-and-data-retention
- 8 How long do you store my organization's data?
privacy.claude.com/en/articles/7996866-how-long-do-you-store-my-organization-s-data
- 9 Access the Compliance API
support.claude.com/en/articles/13015708-access-the-compliance-api
- 10 Access audit logs
support.claude.com/en/articles/9970975-access-audit-logs
- 11 Monitor Claude Cowork activity with OpenTelemetry
support.claude.com/en/articles/14477985-monitor-claude-cowork-activity-with-opentelemetry
- 12 Cowork monitoring reference
claude.com/docs/cowork/monitoring
- 13 Claude Code monitoring
code.claude.com/docs/en/monitoring-usage
- 14 Explore the .claude directory
code.claude.com/docs/en/claude-directory
- 15 Configure custom data retention controls for Enterprise plans
privacy.claude.com/en/articles/10440198-configure-custom-data-retention-controls-for-enterprise-plans
- 16 Inference hooks
platform.claude.com/docs/en/manage-claude/inference-hooks
- 17 Investigating three real-world incidents in our cybersecurity evaluations
www.anthropic.com/news/investigating-incidents-cybersecurity-evals
- 18 Update Compliance Settings: API reference (beta)
platform.claude.com/docs/en/api/beta/organization/compliance_settings/update
- 19 Configure Inference hooks
platform.claude.com/docs/en/manage-claude/inference-hooks-configuration
- 20 Claude Cowork architecture overview
support.claude.com/en/articles/14479288-claude-cowork-architecture-overview
- 21 How we contain Claude across products
www.anthropic.com/engineering/how-we-contain-claude
- 22 Compliance API FAQ
platform.claude.com/docs/en/manage-claude/compliance-faq
- 23 Design your compliance integration
platform.claude.com/docs/en/manage-claude/compliance-integration-patterns
- 24 Get effective organization settings: API reference
platform.claude.com/docs/api/compliance/organizations/settings/retrieve
- 25 Files API
platform.claude.com/docs/en/build-with-claude/files
- 26 Batch processing
platform.claude.com/docs/en/build-with-claude/batch-processing
- 27 Code execution tool
platform.claude.com/docs/en/agents-and-tools/tool-use/code-execution-tool
- 28 Managed Agents: session operations
platform.claude.com/docs/en/managed-agents/session-operations
- 29 Managed Agents: session event stream
platform.claude.com/docs/en/managed-agents/events-and-streaming

■ ABOUT INVICTUS INCIDENT RESPONSE

We founded Invictus Incident Response to meet the surge in cloud cybersecurity incidents and to close the gap in truly effective cloud incident response.

We're an incident response company at heart. We've handled the full range of incidents across AWS, Azure, and Google Cloud, and because the compute behind AI mostly lives in that same cloud, that experience is what makes us ready to investigate AI platforms. We help our customers stay undefeated.



■ GENERAL ENQUIRIES

info@invictus-ir.com

Website: invictus-ir.com

■ UNDER ATTACK? 24x7 INCIDENT RESPONSE

cert@invictus-ir.com

North America +1 470 660 4114

Europe +31 852 087 843

■ DISCLAIMER

This white paper is published by Invictus Incident Response for informational and educational purposes only and reflects the authors' analysis as of the date of publication. It is provided in good faith without representations or warranties of any kind, and does not constitute legal, regulatory, financial, or professional advice. Evaluate any recommendation against your own environment and obligations, and seek qualified advice before acting on it.

To the fullest extent permitted by law, Invictus Incident Response accepts no liability for any loss arising from use of or reliance on this publication. References to third-party products and services are illustrative and do not imply endorsement. Trademarks remain the property of their respective owners.

Copyright. © 2026 Invictus Incident Response. All rights reserved.

