

SPOTLIGHT ON

Claude Enterprise Coverage

How to achieve complete visibility, enforce governance, and manage risk across Claude's full enterprise deployment surface.

Problems

Incomplete Visibility

Endpoint monitoring covers Claude Desktop, Cowork, and Claude Code. The conversation and project content within Claude Enterprise sits outside the reach of existing security tooling.

Compliance Blind Spots

Security and compliance teams lack programmatic access to Claude conversation data, creating gaps in audit trails, data governance, and regulatory reporting.

Governance Drift

As usage expands across chats and projects, risk surfaces multiply without corresponding controls or oversight.

Business Outcomes



Complete Coverage

Full visibility across Claude's enterprise deployment surface, from developer endpoints to enterprise conversation and project content, in a single governance view.



Unified Audit Trail

Conversation content, files, project data, and audit log events consolidated into a single compliance record, mapped to organisational policy and reporting requirements.



Proactive Remediation

Geordie's remediation suite, Beam, applies proactive protection across all Claude surfaces for controls that scale with Claude Enterprise deployment.

Claude Coverage: Existing and Extended

EXISTING VIA ENDPOINT		NEW VIA COMPLIANCE API	
● Claude Desktop	Endpoint	● Claude Enterprise Chats	Compliance API
● Cowork	Endpoint	● Claude Enterprise Projects	Compliance API
● Claude Code	Endpoint	● Claude Platform activity logs	Compliance API

How Georgie Works

Using agentic fingerprinting, Georgie meets agent data where it is across Claude Desktop, Cowork, and Claude Code, capturing activity across developer workstations, tool invocations, and code repositories wherever agents operate.

Via the **Claude Compliance API**, Georgie ingests conversation content, files, project data, and audit log events directly from Claude Enterprise, normalised alongside endpoint telemetry into a unified behavioural picture.

Beam, Georgie's proactive context governance tool, applies in-line guardrails across all Claude surfaces in real time. Beam operates at the endpoint layer to prevent data exfiltration and route alerts into existing security workflows.

Full Claude coverage, as of May 2026:

● Claude Desktop

● Cowork

● Claude Code

● Claude Chats

● Projects

● Activity logs

● Existing endpoint coverage ● New via Compliance API

