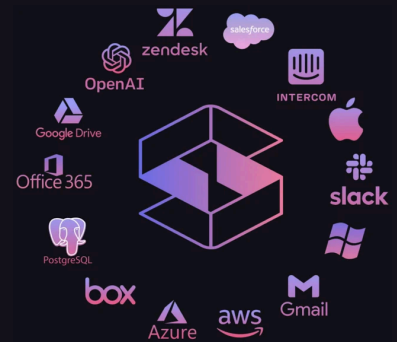


AI-NATIVE DATA SECURITY PLATFORM

Find, protect, and govern sensitive data **everywhere** it moves — SaaS, cloud, endpoints, browsers, and AI.

Strac discovers PII, PHI, PCI, secrets, source code, and IP wherever it lives, then **fixes the problem automatically**: redact, mask, block, quarantine, delete, revoke sharing, or label. One console, one policy engine, one set of ML detectors, applied across five product lines.


01 · ENDPOINT
Endpoint DLP

Mac · Windows
(Linux available)

02 · AI AGENTS
MCP DLP

Any MCP server, via
reverse proxy

03 · BROWSER
Browser DLP

Chrome · Firefox ·
Edge · Safari

04 · SAAS
SaaS DLP

Slack, Google, M365,
Salesforce, Zendesk
...

05 · DATA AT REST
DSPM

Know what AI can
reach before you
connect it

WHERE IS IT?

Scan and classify sensitive data at rest across SaaS apps, cloud storage, databases, and endpoints — unstructured documents and structured tables alike, including text inside PDFs, images, and screenshots via OCR.

WHERE IS IT GOING?

Watch data in motion: messages, tickets, emails, uploads, downloads, USB, AirDrop, pastes, GenAI prompts on the desktop and in the browser, AI-agent tool calls over MCP, and AI browser agents reading SaaS apps in the user's session.

WHAT DO WE DO ABOUT IT?

Policies choose the action per surface — audit, warn the user, block, redact, delete, revoke access, or apply a label — with a full audit trail for compliance.

100+

ML & OCR detectors for PII, PHI, PCI, secrets, code, IP

60+

SaaS, cloud, email, and database integrations

50+

MCP connectors, plus a reverse proxy for any MCP server

15 min

Typical time from connect to first protected app

COMPLIANCE, EVERY SURFACE

Every product line — DLP, DSPM, and the AI controls (desktop agents, browser GenAI, MCP) — enforces the same policies and produces audit evidence mapped to:

PCI DSS

HIPAA

SOC 2

ISO 27001

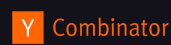
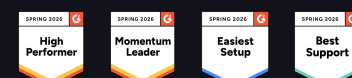
GDPR

CCPA / CPRA

ISO 42001

NIST CSF

TRUSTED BY

BACKED BY

ON G2


Four enforcement points, one policy engine

Endpoint DLP

Agent · macOS & Windows

A lightweight agent for everything that happens on the device itself: local files, removable media, peer-to-peer sharing, and the AI tools that run outside the browser.

- **AI on the desktop:** prompt monitoring and file-upload control for Claude Code, Claude Cowork, Codex, Cursor, and other local AI agents and IDE copilots
- **Shadow AI & shadow MCP discovery:** find AI apps and MCP servers running on endpoints that nobody approved
- File uploads & downloads, **USB, AirDrop, Bluetooth**, clipboard, print
- Deploys silently via **Jamf, Intune, NinjaOne** or any MDM
- **Data discovery & classification at rest:** where sensitive files live on the device and who touched them
- **Data lineage:** files from Drive, Box, OneDrive, or SharePoint stay tagged as corporate after rename, copy, or edit — exfiltration is blocked by origin, not just content

Audit

Warn / nudge

Block

Discover & classify

MCP DLP

Reverse proxy · any MCP server

AI agents (Claude, ChatGPT, Cursor, Copilot, custom) reach into SaaS, databases, and warehouses through MCP tool calls. Strac sits inline on every call and protects the data inside it, not just who called what.

- 50+ connectors: Slack, Google Workspace, M365, Salesforce, GitHub, Snowflake, Databricks, Postgres, MongoDB, Stripe, Workday ...
- Works as a reverse proxy, so **any existing MCP server** can be governed without rebuilding it
- Per-agent access control, shadow MCP server discovery, prompt-injection detection
- Every tool call logged as audit evidence mapped to SOC 2, HIPAA, PCI, GDPR

Audit

Redact before the model sees it

Block / approve

Revoke

Browser DLP

Extension · Chrome, Firefox, Edge, Safari

Lightweight, agentless control over everything employees type, paste, upload, or download in a web app — including GenAI tools like ChatGPT, Claude, Gemini, and Copilot.

- **GenAI & prompt monitoring:** inspect prompts, file attachments, and model responses in real time
- **Shadow AI discovery:** see which AI tools are in use, by whom, and what data goes in
- **AI browser-agent control:** discover agent extensions (Claude in Chrome, Comet, Atlas, Gemini in Chrome, Copilot), log which SaaS apps they read in the user's logged-in session, and allow or block per agent and per domain
- File uploads, downloads, and form submissions to any site; shadow IT and unapproved SaaS
- Deployed centrally via Chrome/Edge enterprise policy or MDM

Audit

Warn / nudge

Block

SaaS DLP

API integrations · no agent needed

Where Strac started and where it leads. Connect in minutes and remediate sensitive data inside the app itself — messages, tickets, docs, records, attachments.

- **AI can't read what isn't there:** redact at the source so AI browser agents, MCP connectors, and any future agent reading the app get sensitive_data links, not data — the one control that holds no matter how AI reaches it
- **Native AI governance:** keep regulated data out of Microsoft Copilot, Gemini for Workspace, Slack AI, Zendesk and Salesforce AI — redaction removes it from what they index; labels in Google and SharePoint/Purview govern what they can summarize
- Slack, Teams, Gmail, M365, Google Drive, OneDrive, SharePoint, Box, Dropbox, Salesforce, HubSpot, Jira, Confluence, Notion, Zendesk, Intercom, ServiceNow, Zoom ... (see /integrations)
- **Redaction and delayed redaction** of messages and attachments; blocking; deletion on cloud drives
- **Posture fixes:** revoke public links, remove external members, strip risky permissions, quarantine files; alert on anomalous sharing and access
- **Labeling** in Google Drive and SharePoint/Purview so native controls kick in

Audit

Warn user

Block

Redact

Quarantine

Delete

Revoke sharing

Label

DATA AT REST

DSPM: **historical scanning** for everything you already have

The same connectors and detectors used for real-time DLP run as deep historical scans across months or years of legacy data — without data leaving your cloud. Find sensitive files and records, see who can access them, and fix exposure automatically.

- **AI-readiness before you connect:** before Copilot, Gemini, or an MCP agent is pointed at a drive, site, or warehouse, know exactly what sensitive data is in it — then redact, label, or revoke so the AI inherits a clean corpus, not years of PII
- **AI access graph:** see which AI agents, connectors, and copilots can reach which stores that hold sensitive data, and cut the ones that shouldn't

SCANS

Slack Google Drive Gmail OneDrive SharePoint
M365 Email Box Dropbox Salesforce Zendesk
Notion Confluence AWS S3 Azure Blob
Google Cloud Storage DynamoDB CloudWatch
Snowflake Postgres SQL / Oracle
Windows file shares & NAS Endpoints

REMEDIATES

Revoke public / external sharing
Apply classification labels Redact or mask fields
Delete Alert to Slack, Teams, SIEM

REPORTS

Data map and access graph: what sensitive data exists, where, who owns it, and who can reach it. Compliance evidence for HIPAA, PCI, SOC 2, ISO 27001, GDPR audits.

See it on your own data

Integrations: strac.io/integrations · MCP connectors: strac.io/mcp-integrations
Partners: strac.io/mssp-partner-program · hello@strac.io

[Book a demo](#)