Strac

Data Security For SaaS, Cloud, Gen AI, Endpoints, MCP

Strac is the pioneering cybersecurity company providing state-of-the-art solutions for **Data Discovery**, **Data Security Posture Management (DSPM)**, and **Data Loss Prevention (DLP)**, ensuring end-to-end protection for sensitive data across **SaaS**, **Cloud**, **Gen AI, Browsers, Endpoints and MCP**.

1. DISCOVER	2. CLASSIFY	3. REMEDIATE
Scan Unstructured Documents, Unstructured Text and Structured Databases/Tables **(Real-Time + Historical Scanning)**	Classify via Machine Learning & OCR Models	**a.** Redaction b. Labeling c. Deletion d. Blocking e. Revoke Access (Public/External Members)

Trusted By Enterprises & ScaleUps

UiPath · crypto.com · Rho · THREDUP · rightway · UNDERDOG FANTASY · meridianlink · HONEYBOOK · VOLTAS

Key Features

Data Discovery & Classification

1. Automatically discover sensitive and regulated data across SaaS apps (e.g., Google Workspace, Microsoft 365, Slack, Salesforce) and cloud stores (e.g., S3, Azure Blob, Google Bucket)
2. Apply machine learning & OCR for PII, PHI, IP, credentials, secrets, financial data, and adversarial prompt content
3. Visualize data maps, access graphs and “who has access” across SaaS + cloud

Real-time Monitoring & Remediation

1. Real time scanning of sensitive file uploads or chat messages or email or gen ai prompt
2. Incorporate remediation such as redaction, masking, labeling, blocking, remove external access, quarantine file

Strac © 2026

https://strac.io

HIPAA · PCI-DSS · ISO 27001 · SOC 2 · CCPA · GDPR

3. Detect anomalous uploads/downloads, unauthorized sharing, mass downloads, context-aware risk signals

Historical Scanning & Remediation

1. Dive into historical data for retrospective scanning of at-rest content, previously shared files, old chat logs, archive repositories
2. Bulk remediation actions: remove external members, remove public access, change permissions, enforce labels/policies, redaction, masking
3. Built-in workflows for investigation, triage, remediation with audit-trail for compliance

Gen AI Prompt & Output Protection

1. Monitor Gen AI prompt submissions and model responses for leakage of sensitive data or risky content
2. Apply real-time blocking or coaching when a user attempts to upload sensitive file content into a Gen AI chat interface
3. Ensure safe Gen AI usage while enforcing enterprise data protection policies

Endpoint DLP

1. Deploy lightweight agent on Mac and Windows endpoints
2. Monitor sensitive data movement via USB, Bluetooth, AirDrop.
3. Browser extension for upload, paste, and download controls on web apps
4. Integrates with MDM like Jamf, Intune, Ninja One for zero-touch deployment

MCP DLP

1. Protect enterprise data flowing through AI agent tool calls (Claude Desktop, Cursor, any MCP client)Inline redaction before sensitive data reaches the LLM — zero storage, zero exposure
2. Covers Microsoft 365, SharePoint, OneDrive accessed via MCP servers
3. Redacts SSN, credit cards, PHI, API keys, and custom patterns in real time
4. Agentless — works as an MCP middleware, no proxy, no TLS interception