Strac

Data Security Across SaaS, Cloud, Gen AI, Browsers

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 and Browsers**.

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 · snap finance

Key Features

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

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

Cloud Native Infrastructure Protection

1. Cover cloud infrastructure via agentless integrations (e.g., IAM roles, RDS, S3) within customer's AWS, Azure or GCP account
2. Detect misconfigurations, excessive permissions, data-movement risks, and integrate with DSPM (cloud-data risk posture)
3. Blend DLP + DSPM: see both data and how it's accessed/used/exposed

Alerting, Workflow & SIEM Integration

1. Send alerts to Slack, Teams, email, or SIEM/SOAR platforms
2. Embedded case-management, investigation workflows and remediation tasks
3. Leverage built-in policies or customise rules based on your organisation's compliance/regulatory regime