sentra

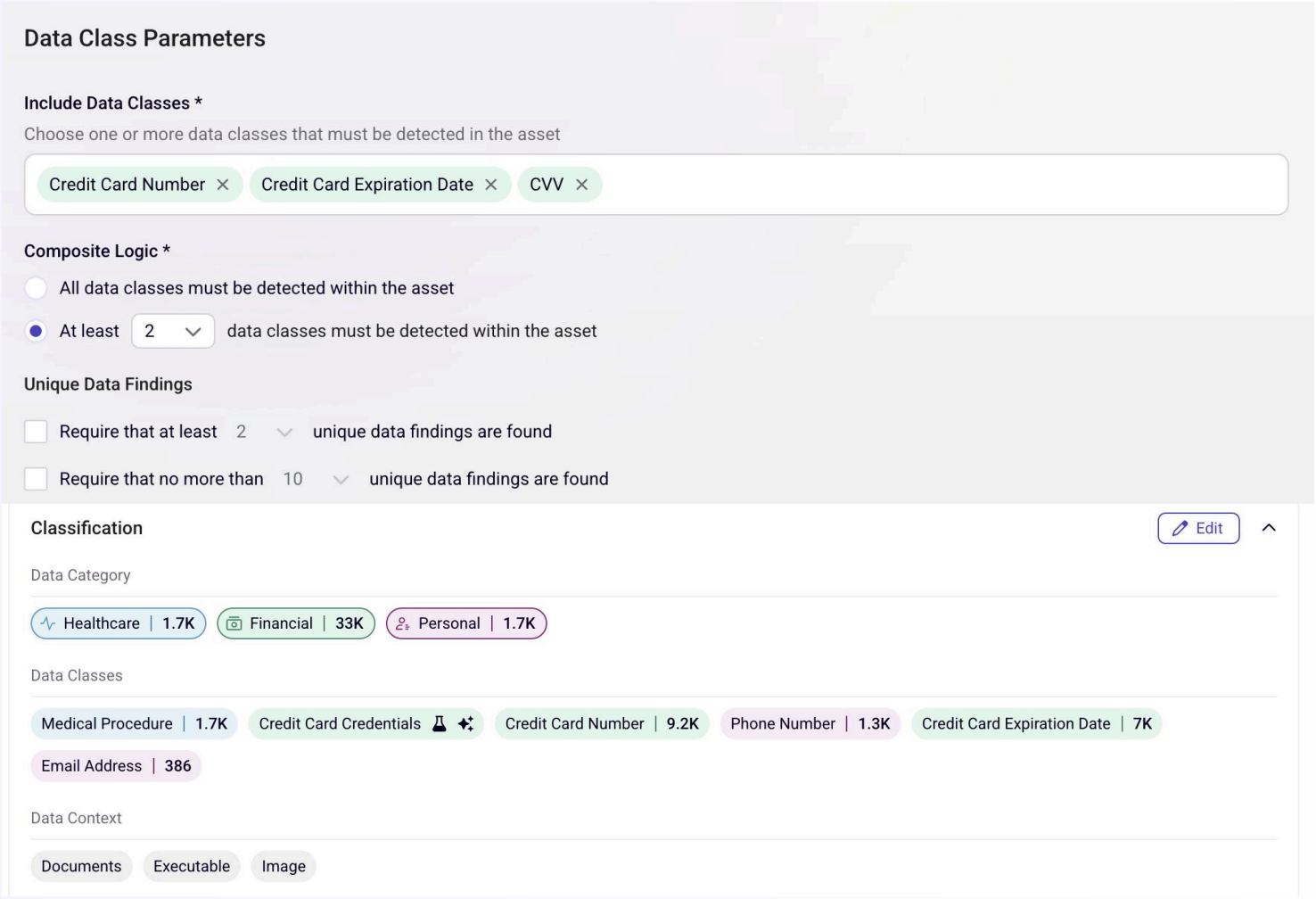
Minimize Sensitive Data Exposure in Cloud Drives

Stop oversharing and overpermissioning from putting critical data at risk.

Cloud File Sharing is a Silent Risk—Here's How to Regain Control

Sensitive data in employee cloud drives is often overshared, overexposed, and overlooked, especially when buried in unstructured formats like documents, spreadsheets, and emails, which make up over 90% of enterprise data. Native tools in Google Workspace and Microsoft 365 often miss these risks. Sentra uses AI-driven discovery, contextual classification, and monitoring to help prevent sensitive data exposure without disrupting collaboration.

Define and Find Unique Toxic Combinations



Sensitive Data Is Overshared, Underprotected, and Hard to See

Overpermissioned access to cloud drives often leads to undetected exposure of sensitive data. Business documents, customer information, and other critical files can spread across employee-managed storage and be shared publicly, internally, or with third parties, often without visibility. This challenge is compounded by the fact that most organizations lack the ability to detect when sensitive files are shared externally or via public links. Manual reviews and fragmented policies delay response, while native tools in Google Workspace and Microsoft 365 struggle to classify unstructured content like contracts and PII. Without centralized visibility and automated controls, risk continues to grow.

Make Invisible Risks Visible

Sentra gives organizations the tools to uncover and control data exposure risks across employee cloud drives like Microsoft 365 OneDrive and Google Drive. It continuously discovers sensitive unstructured data, such as PII, contracts, and customer files, and detects when that data is shared publicly, across the organization, or with untrusted third parties. Sentra's cloud-native platform goes beyond basic metadata scanning, using advanced AI models, including zero-shot and LLM-based techniques, to classify unstructured data with over 95% precision. It identifies dangerous groupings of sensitive data and risky access permissions known as toxic data combinations, uncovers shadow data, and dissolves visibility silos by providing unified control over data across major data platforms. With real-time alerts, file-level access mapping, and policy-based enforcement, Sentra enables teams to reduce exposure, enforce least privilege, and secure data sharing without disrupting productivity.

Why Security Teams Choose Sentra to Reduce Sprawl and Optimize Storage

Discover and classify sensitive unstructured data across Microsoft 365, Google Workspace, and other cloud drives using AI-driven context

Enforce policy-based controls and respond to exposure events with real-time alerts and automated remediation

Detect risky sharing behaviors such as public links, org-wide access, and third-party exposure

Monitor file-level access to uncover overpermissioned data and reduce excessive access

SaaS Company: Regained Control of Google Drive Sharing

A global SaaS company turned to Sentra to assess data exposure risks across more than 20,000 employee Google Drive accounts. The security team quickly uncovered thousands of sensitive files, including contracts and customer PII, that had been shared externally or made accessible through public links, often without anyone's knowledge. With Sentra's real-time alerts and automated policy enforcement, they were able to identify and remediate the most critical risks. This improved their visibility, strengthened data governance, and helped bring cloud file sharing back under control.

Ready to Reduce Data Exposure and Take Control of Cloud File Access?

Get A Demo

or learn more about
Powerful Data Access Governance for a Robust Zero Trust Strategy.

sentra