sentra

Protect Your Secret Sauce: Safeguard Critical IP in the Cloud

Power innovation across distributed R&D and production sites without exposing designs, formulas, and patents.

The Risk: Leveraging IP Creates Exposure

For manufacturers, intellectual property is everything. Formulas, patents, designs, and recipes are the secret sauce that fuel competitiveness. This critical data must flow through R&D teams, testing labs, and production lines to keep the business moving and thriving.

But in the cloud, this same accessibility that fuels innovation becomes a liability. Blueprints get duplicated in public OneDrives, recipes are stored in shared folders, and patents are over-permissioned to contractors or partners. A single accidental exposure can mean stolen IP, lost contracts, and potentially catastrophic business, financial, or reputational damage.

Security leaders need an accurate, efficient way to know exactly where intellectual property lives across their entire environment, who has access, and when and where it is copied or moved.

How Sentra Helps Security Teams Protect Critical IP

Sentra is built to transform how enterprises safeguard the data that matters most, at the speed and scale of modern cloud enterprises. The AI-powered platform automatically and continuously discovers, classifies, and protects both proprietary intellectual property and regulated customer data across multi-cloud and on-premises environments.

- **Automatically discovers and classifies critical data,** finding intellectual property everywhere it lives, including patents, designs, CAD files, formulas, communications, images, audio, and video files.
- **Alerts about over-exposed IP to enforce least-privilege access** so only the right teams and partners can access sensitive files.
- **Automatically apply DLP labels** for consistent controls across Microsoft 365 Purview, Google Drive, and AWS resource tagging.

- **Continuously monitor in real time** when files containing IP are overshared or moved and automatically detect similar sensitive data.
- **Securely adopt AI** while preventing privacy and compliance violations and sensitive corporate data leakage.
- **Reduce risk at scale** with agentless scanning that avoids outages, API throttling, or compute spikes.

With Sentra, organizations can embrace cloud and AI with confidence; securing their most valuable IP assets without slowing down innovation or production.

Why Security Teams Choose Sentra to Stop Insider Threats Faster

Detect and mitigate insider-driven data loss in real-time

Automate least-privilege access control for unstructured and sensitive data

Block risky sharing and apply encryption in SaaS tools like Google Drive and Microsoft 365

Prioritize threats using context-aware insights from identity, behavior, and sensitivity

Gain continuous visibility across multi-cloud and SaaS with a cloud-native architecture

Enhance DLP tools like Microsoft Purview to extend coverage and control

How an Aerospace Firm Secured Proprietary Designs

An aerospace manufacturer used Sentra to discover, classify and remediate exposure risk to proprietary data such as; patents, algorithms, and CAD designs across Microsoft 365 and Google Workspace. Sentra quickly discovered duplicate blueprints in employee OneDrives and flagged overshared design files that could have leaked via collaboration. They also used Sentra to enforce their policy of masking all data stored on Snowflake by accurately identifying data as masked or unmasked. Finally, they created a ticketing workflow to automate and streamline remediation of urgent issues. The company cut exposed IP by over 80% in the first month.

Deploying Sentra was simple and the scan quickly found exposed proprietary data, IP, and other critical data that if compromised or exfiltrated could cause catastrophic business, financial, or reputational damage.

Ready to Secure Your Most Valuable Assets?

Schedule A Demo

and Speak with a Data Security Expert

sentra