

Detect Insider Threats and Prevent Data Exposure

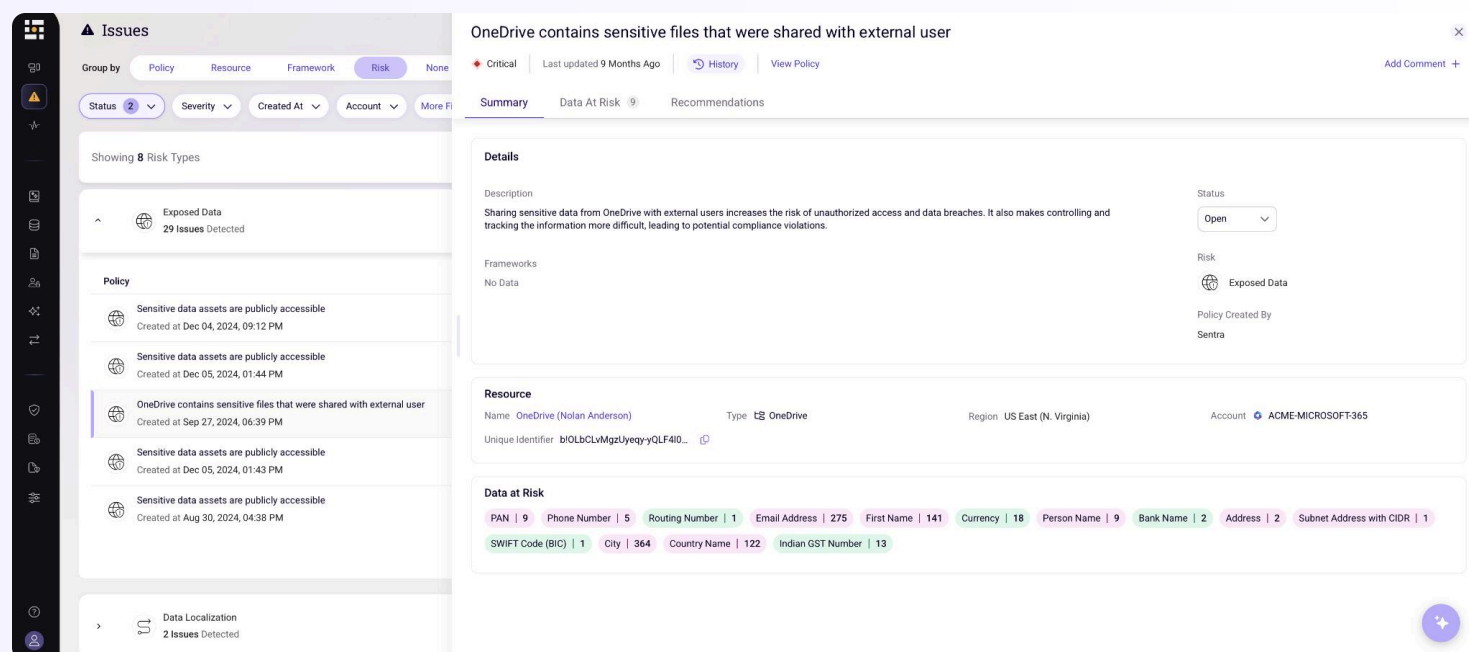
Boost cloud DLP with real-time visibility, smart prioritization, and automated response.



Legacy DLP Can't Keep Up with Insider Risk in the Cloud

Legacy DLP tools were built for static, on-premises environments—and they fall short in today's fast-moving, cloud-native world. They rely on predefined patterns and lack the context to understand where data lives, who's accessing it, and how it's being used. As a result, legacy DLPs generate false positives, miss real threats, and can't keep up with dynamic insider risk. Sentra bridges this gap with AI-powered, context-aware classification and real-time monitoring that understands both the data content and the environment around it. With smart risk prioritization and automated response, Sentra enables precise, proactive protection across SaaS, cloud, and unstructured data—before damage occurs.

View Sensitive Data Shared Externally



The screenshot displays the Sentra interface. On the left, a sidebar shows a list of issues under the 'Issues' section. The main panel shows a detailed view of a specific issue titled 'OneDrive contains sensitive files that were shared with external user'. The issue is marked as 'Critical' and 'Last updated 9 Months Ago'. The 'Details' section provides a description of the issue, stating that sharing sensitive data from OneDrive with external users increases the risk of unauthorized access and data breaches. The 'Resource' section identifies the resource as 'OneDrive (Nolan Anderson)' with a unique identifier 'bi0LbCLvMgzUyey-yQLF40...'. The 'Data at Risk' section lists various data types at risk, including PAN, Phone Number, Routing Number, Email Address, First Name, Currency, Person Name, Bank Name, Address, Subnet Address with CIDR, SWIFT Code (BIC), City, Country Name, and Indian GST Number.

Issues

Group by: Policy Resource Framework Risk None

Status: 2 Severity Created At Account More Filter

Showing 8 Risk Types

- Exposed Data
29 Issues Detected
- Policy
 - Sensitive data assets are publicly accessible
Created at Dec 04, 2024, 09:12 PM
 - Sensitive data assets are publicly accessible
Created at Dec 05, 2024, 01:44 PM
 - OneDrive contains sensitive files that were shared with external user
Created at Sep 27, 2024, 06:39 PM
 - Sensitive data assets are publicly accessible
Created at Dec 05, 2024, 01:43 PM
 - Sensitive data assets are publicly accessible
Created at Aug 30, 2024, 04:38 PM
- Data Localization
2 Issues Detected

OneDrive contains sensitive files that were shared with external user

Critical Last updated 9 Months Ago History View Policy Add Comment

Summary Data At Risk Recommendations

Details

Description: Sharing sensitive data from OneDrive with external users increases the risk of unauthorized access and data breaches. It also makes controlling and tracking the information more difficult, leading to potential compliance violations.

Status: Open

Risk: Exposed Data

Policy Created By: Sentra

Resource

Name: OneDrive (Nolan Anderson) Type: OneDrive Region: US East (N. Virginia) Account: ACME-MICROSOFT365

Unique Identifier: bi0LbCLvMgzUyey-yQLF40...

Data at Risk

PAN | 9 Phone Number | 5 Routing Number | 1 Email Address | 275 First Name | 141 Currency | 18 Person Name | 9 Bank Name | 2 Address | 2 Subnet Address with CIDR | 1

SWIFT Code (BIC) | 1 City | 364 Country Name | 122 Indian GST Number | 13

You Can't Stop What You Can't See (especially when it's internal)

Insider threats demand more than surface-level visibility. In modern cloud and SaaS environments, preventing insider-driven data loss requires real-time detection and automated control. False positives and alert fatigue make it hard to identify true threats. Unrestricted sharing in tools like Google Drive and Microsoft 365 increases the risk of accidental exposure. Manual access control over sensitive, unstructured data delays least privilege enforcement. Without automated response to changes in data classification or posture, exposure can persist. Insider risk requires accurate classification, context-aware detection, and responsive, policy-based enforcement.

Automate Threat Detection and Response at Cloud Scale

Sentra gives enterprises the visibility and control they need to stop insider threats before sensitive data is exposed. Built to address the realities of modern cloud and SaaS ecosystems, Sentra continuously monitors access activity, classifies sensitive data in real-time, and enforces policy automatically based on context and risk. Security teams can detect insider threats as they happen, block risky sharing, apply encryption, and restrict access as data sensitivity or posture changes. Native integrations with platforms like Google Drive, Microsoft 365, and Microsoft Purview increase the effectiveness of existing DLP investments. By combining deep context with automated enforcement, Sentra delivers intelligent, scalable protection for sensitive data wherever it lives or moves.

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

Heathcare Company: Reduced Insider Risk and Secured PHI'

A leading healthcare provider partnered with Sentra to reduce insider risk, enhance data loss prevention (DLP), and strengthen protection of Protected Health Information (PHI) across its multi-cloud environment. With limited visibility into how PHI was being shared across platforms like Google Drive, Microsoft 365, Salesforce, and Snowflake, the organization deployed Sentra's agentless data discovery and classification to identify and monitor over 230 TB of sensitive data. With Sentra continuously monitoring data access it flagged high-risk sharing events in real-time, automated least-privilege access enforcement, and blocked potential exfiltration attempts. These capabilities not only reduced insider threats and response times but also helped maintain HIPAA compliance while enabling staff to continue agile collaboration across clinical, administrative, and research environments.

Ready to Detect Insider Threats and Prevent Data Exposure?

[Get A Demo](#)

or download the
[Complete Guide to Data Security Posture Management \(DSPM\)](#)

