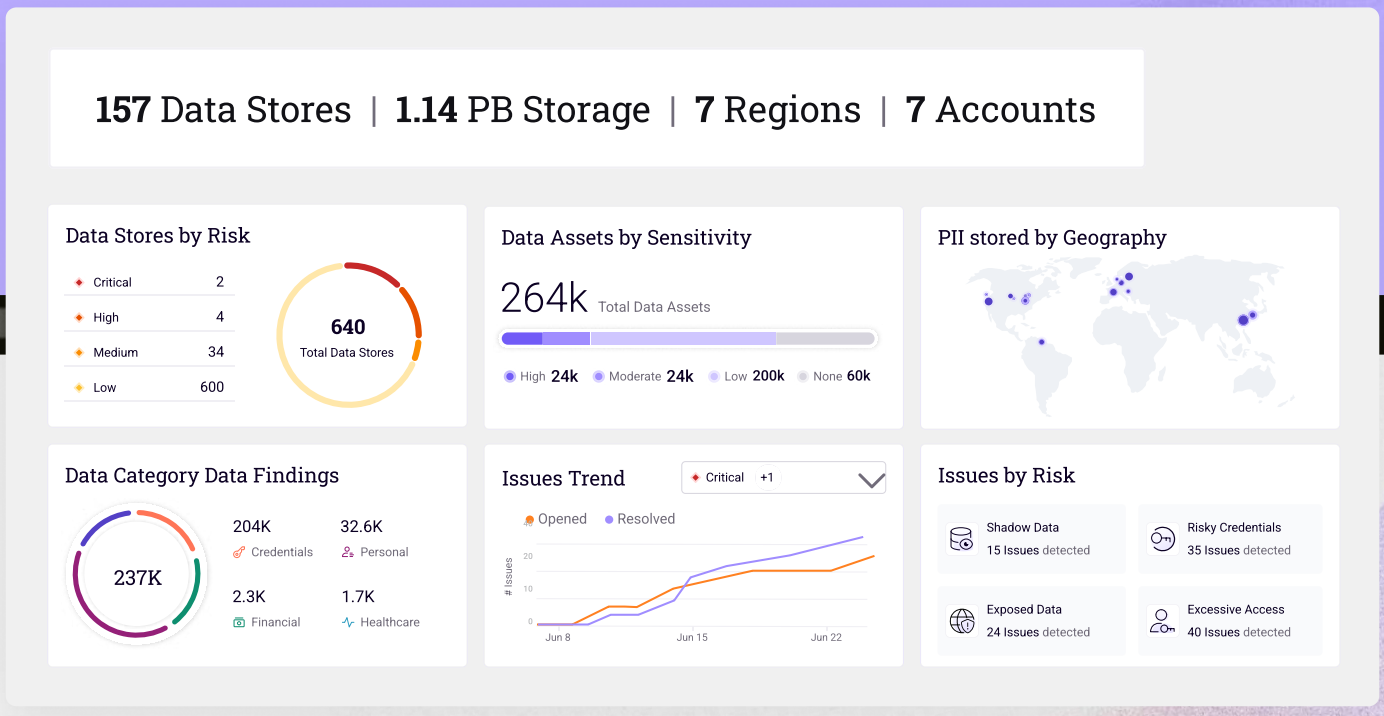
sentra

Technology Overview

How Sentra's Agentless Data Security Platform Works

Sentra's Data Security Posture Management (DSPM) platform gives you a clear and prioritized view of your sensitive cloud data at risk. We ensure that your most business critical data is always secure by determining the best security posture for each data file, store, and asset.

Sentra supports all self-hosted, unmanaged and managed databases, storage accounts, data warehouses, data lakes, data pipelines, and metadata catalogs across all major public cloud providers (AWS, Azure, GCP and Snowflake)



Here is how we do it in a nutshell:

Sentra's platform connects to your cloud infrastructure within minutes, supporting all major cloud providers. Our agentless setup simply provisions a few cloud resources in your cloud provider account, providing Sentra's SaaS with the necessary permissions.

We evaluate your rule-based policies relative to the data sensitivity, security posture, access controls, and more. Sentra then generates prioritized alerts within the systems and productivity tools that you work with.

Sentra can run in a separate virtual network within each cloud account to analyze your data. Customers can choose a deployment model running in a dedicated cloud account.

We then automatically discover and classify data without introducing any privacy risks. Sentra's unique data classification leverages ML and AI to detect sensitive data proprietary to our customers.

Sentra's 3 Principles

1. Everything is read-only and API-based

It's effortless to connect to Sentra, and you can rest assured that nothing gets created or deleted by Sentra outside of the isolated environment set up by Sentra.

2. Sentra is non-intrusive, never interfering with your current network or data flows

Sentra only scans copies of your data while preserving the integrity of your production environment. For instance, in the case of database or disk scanning, Sentra captures snapshots and performs scans within a secure, isolated environment.

Similarly, when examining an object storage account, Sentra leverages cloud APIs to scan local replicas of objects without affecting your live data.

3. Your data never leaves your environment

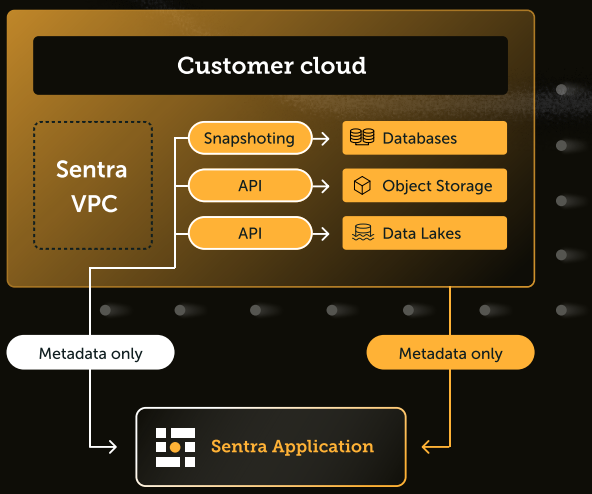
Sentra's SaaS servers only have access to the metadata extracted from your cloud environment. The scanned data never leaves your environment at any time.

Sentra's Technology

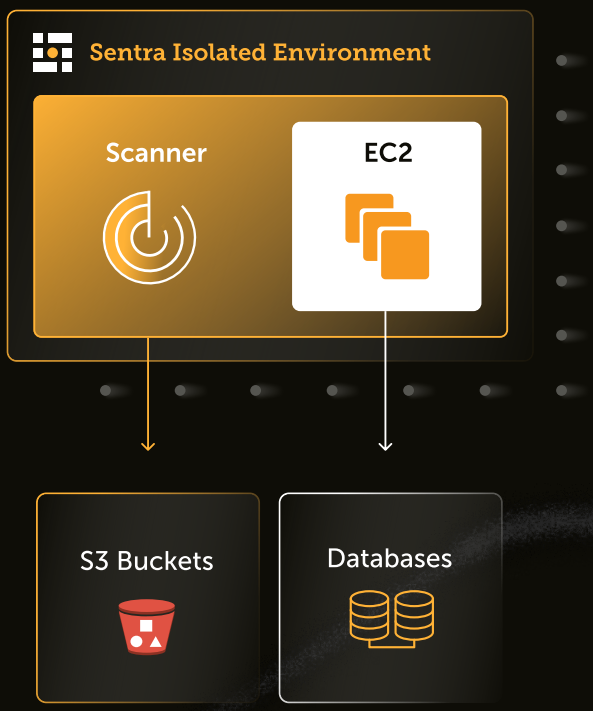
Discovery & Scanning

Sentra's unique intelligent sampling approach enables us to scan your cloud environment at the speed of data creation by understanding the different types of data assets your environment contains and selecting the correct data to scan. Users can quickly track data appearing anywhere to ensure no sensitive data findings are missed.

Sentra's scanning technology analyzes, classifies, and extracts data stores and assets from your cloud resources. A scanner is created per scan in the isolated virtual network, with a dedicated security group, which is terminated once the scan is complete.



Client Environment



- As part of Sentra's installation, Sentra creates two storage buckets: an inputs bucket for passing scan configuration to the scanner and a results bucket for saving metadata results and showing them in Sentra's SaaS.
- When scanning your resources, Sentra creates a virtual machine (Sentra Scanner) in Sentra's isolated virtual network (residing in your cloud account) and runs the scanning and classification engines that extract metadata from your data.
- To scan unmanaged databases, Sentra creates snapshots of the unmanaged VM's disks and creates new disks from these snapshots, which are later attached to the Scanner instance for scanning and classification.
- To scan cloud-native databases, Sentra uses API calls to scan your data.
- Once the analysis is complete, Sentra's resources are deleted.

Automated Structured & Unstructured Data Classification

Sentra's classification engine is built out of a combination of proprietary and open-source tools. We analyze files and databases and extract unstructured data e.g. text, images, and structured (tabular) data.

Structured and unstructured data are classified using different classification methods, relying on various statistical methods. For example, structured data uses all of the samples in a specific column to infer the data class of the column and may not even allow two data classes to appear in the same column.

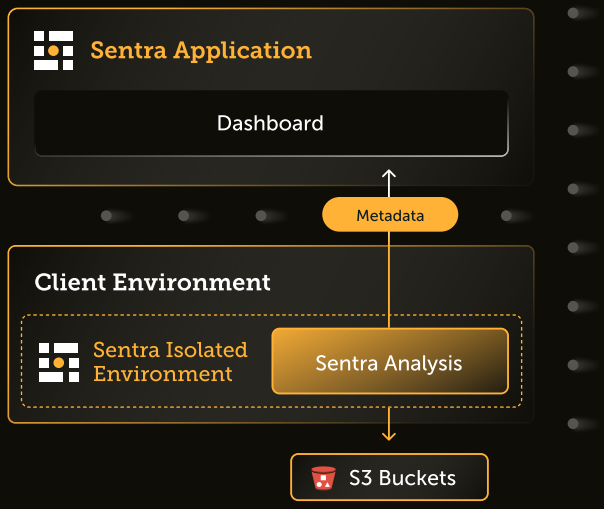
The classification engine collects metadata such as:

- Scanned file and column names
- Number of rows in which a classification was found
- Number of rows scanned
- Classification probability

Once all classification results are collected, they are returned to Sentra via the results bucket. The results bucket is periodically analyzed and loaded into Sentra's application.

After completing the loading process, Sentra deploys the compound classification engine, aggregating the scanning results alongside other metadata and user configurations.

Note: All scanning is done on your cloud account - no data ever leaves your environment.



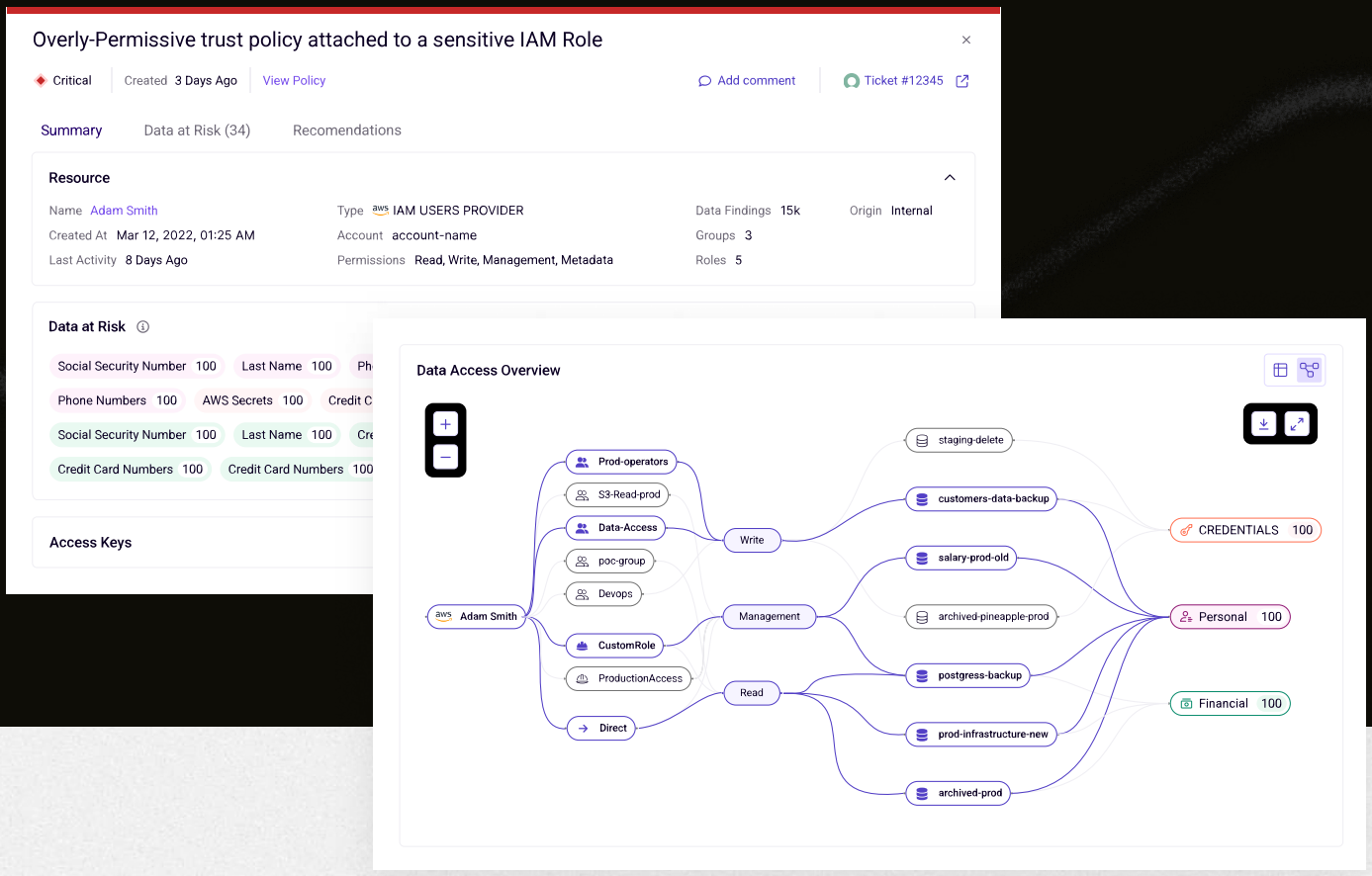
Deep Analysis of Data Sensitivity and Security Posture

Our policy engine enables you to configure the relevant out-of-the-box policies aligned to the key compliance regulations, or you can create your custom policies with an intuitive rules builder.
Now that you have defined your policies and the data scanning and classification are complete, the metadata is analyzed within your environment.

Our analysis looks for sensitive data that doesn't have the proper security posture, including PII, PCI, and company IP. The analyzed metadata is then sent to Sentra's SaaS. Sentra's scanner and anything else created in your environment are tagged by Sentra. This enables you to measure Sentra's resource use easily and helps us to quickly remove all of our instances from your cloud whenever needed.

Results and Remediation

Sentra automatically generates triggered alerts based on policies and is prioritized according to the criticality of the data risk score assigned to your sensitive data assets. You can easily drill down into each alert to better understand the root causes behind the weakened security posture. You can also easily access all the information required for quick investigation and remediation to fix each prioritized issue before it becomes an incident.



Sentra integrates with many of the security and productivity tools you already use. For example, you can notify your team's Slack channel of newly created alerts, or automatically generate a ticket in JIRA for every new critical alert.

For more information, please contact us at info@sentra.io