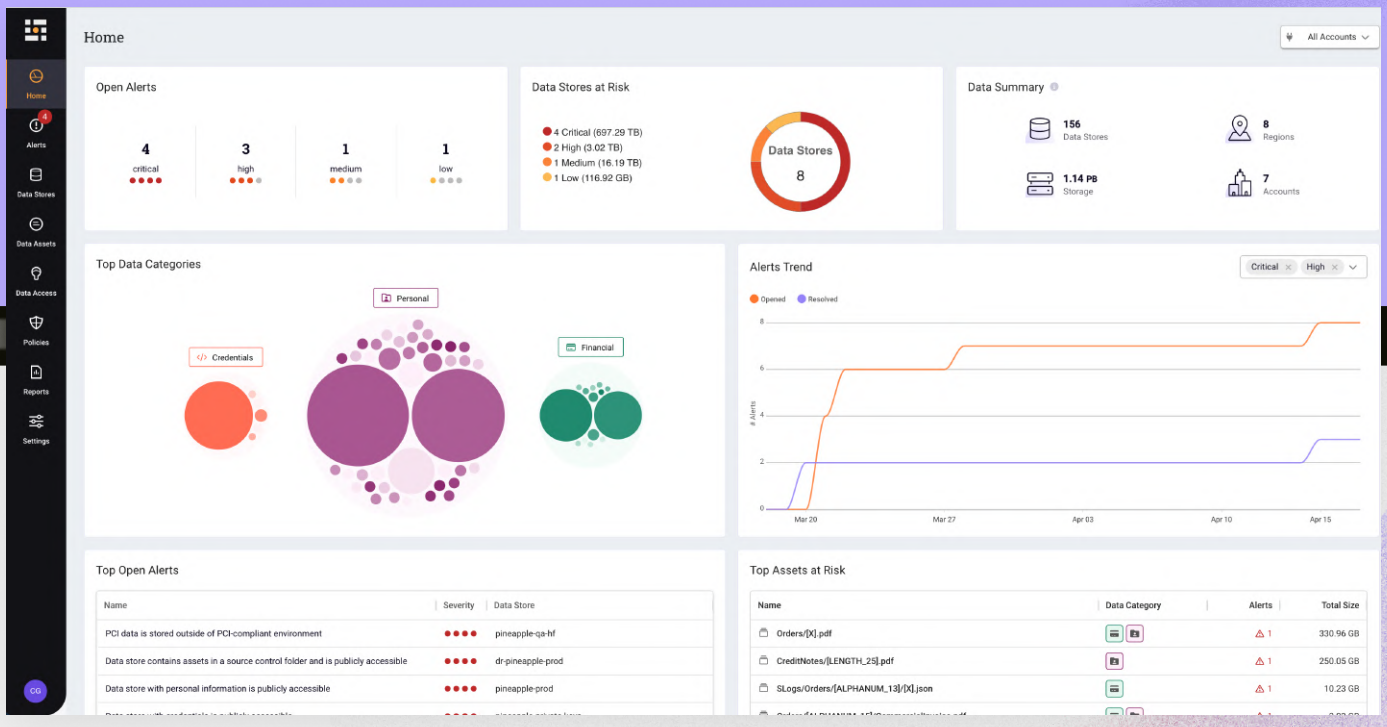
sentra

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. 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 and unmanaged databases, data warehouses, data lakes, data pipelines, and metadata catalogs across all major public cloud providers.



Here is how we do it in a nutshell:

Sentra's platform connects to your cloud infrastructure within minutes and supports all major cloud providers. Our agentless setup is a simple process of provisioning a few cloud resources in your cloud provider account. This provides Sentra's SaaS with the necessary permissions using IAM Role Delegation.

We analyze the data within the VPC and generate prioritized alerts, within the systems and productivity tools that you work with.

Sentra can run in a separate Virtual Private Cloud (VPC) within each existing cloud account for analyzing your data. Alternatively, customers can choose a deployment model that will run in a dedicated cloud account.

We then automatically discover and classify data without introducing any privacy risks. Our unique data classification leverages ML and AI, with the ability to detect any type of sensitive data that is proprietary to each of our customers.

Sentra's 3 Principles

1. Everything is read-only, and API based

It's extremely easy 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 the CloudFormation StackSet.

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

This is achieved by using API requests when possible, for example, when scanning S3 buckets, Sentra uses API requests to scan the object storage.

When scanning a database, Sentra takes a snapshot of the data store, and then scans and analyzes the snapshot in our isolated environment.

3. Your data never leaves your environment

Sentra only sees metadata from your cloud environment to display in our SaaS application. Sentra uses AWS PrivateLink, which provides private connectivity between your VPC and Senta's VPC, ensuring that metadata can be transferred without exposing it to the internet

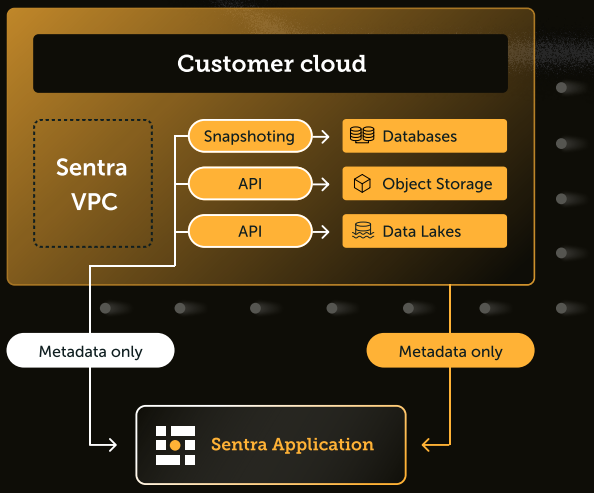
Sentra's Technology

Discovery & Scanning

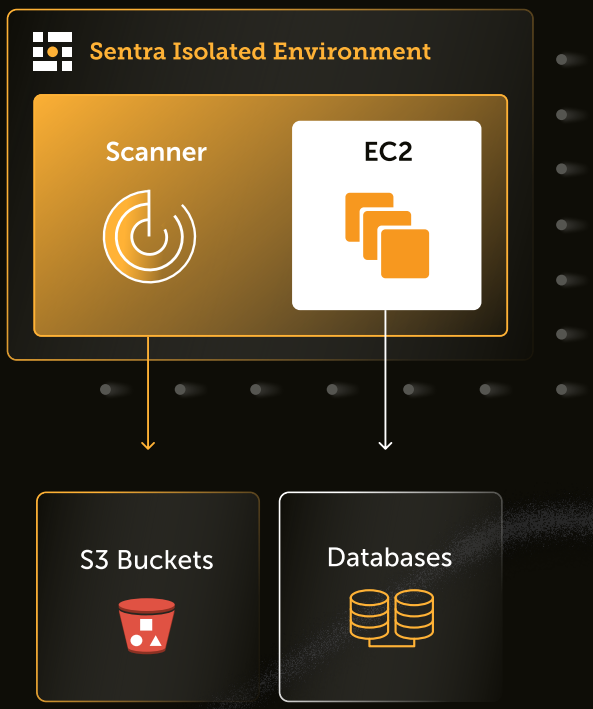
Sentra's unique smart sampling approach enables us to scan your cloud environment at the speed of data creation by understanding the different types of data assets that your environment contains and selecting the right data to scan.

This means that any new data that appears anywhere will be quickly tracked, ensuring that no sensitive data is ever missed.

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



Client Environment



- As part of Sentra's CloudFormation template, Sentra creates two S3 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 an EC2 instance (called canner) in our isolated VPC (residing in your cloud account).
- To scan unmanaged databases, we create snapshots of the EC2 EBS volumes and create volumes out of these snapshots, which are later attached to the Scanner instance.
- 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 both files and databases and extract unstructured data e.g. text and images as well as structured (tabular) data.

Structured and unstructured data are classified using different methods of classification, relying on different 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.

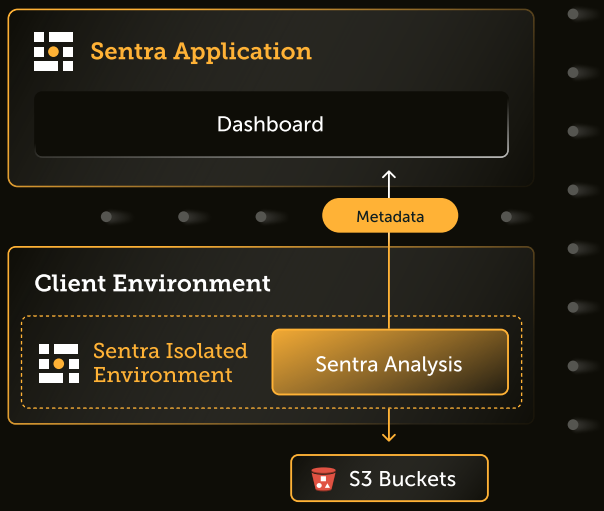
The classification engine collects metadata such as:

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

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

After the loading process is complete, Sentra deploys the compound classification engine which aggregates the scanning results alongside other metadata and user configuration.

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



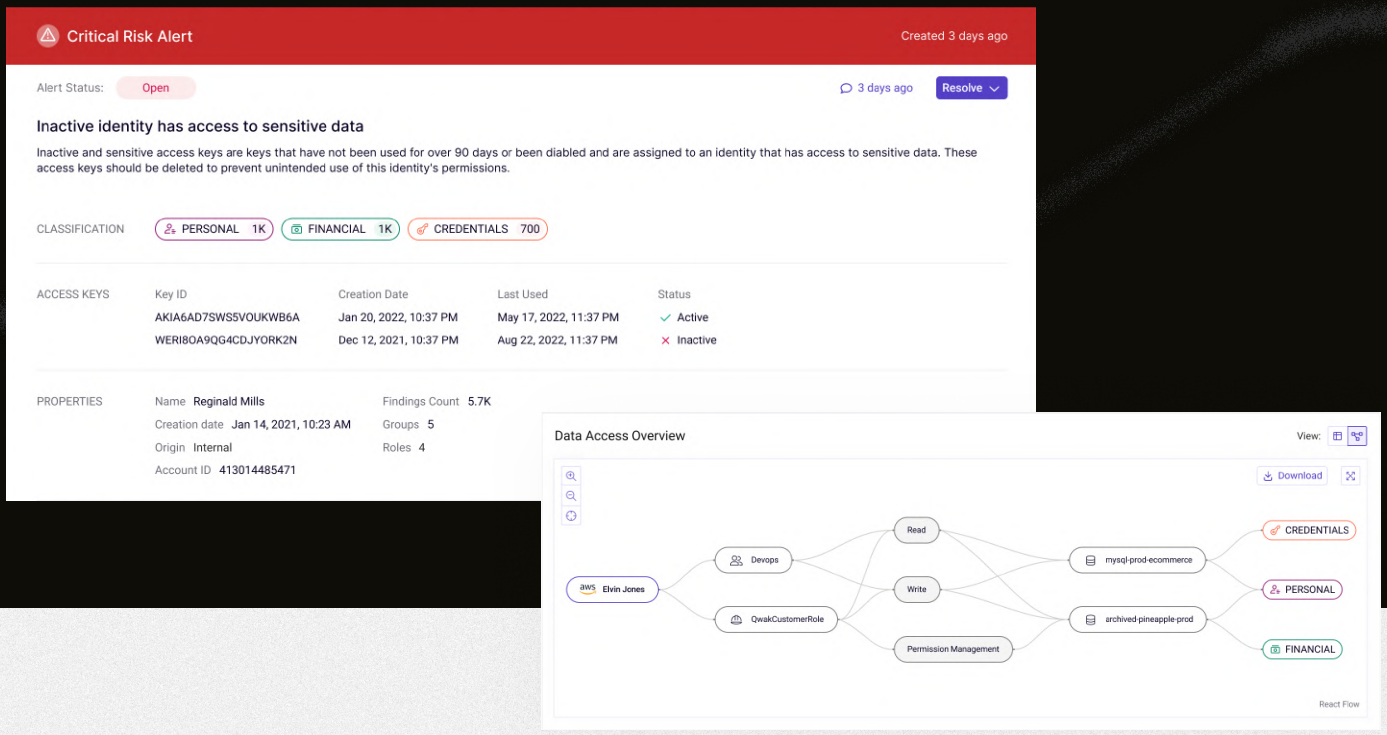
Deep Analysis of Data Sensitivity and Security Posture

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

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

Results and Remediation

Sentra automatically generates alerts that are triggered based on policies and prioritized according to the criticality of the data risk score assigned to your sensitive data assets. You can easily drill down into each individual alert to gain a deeper understanding of 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 on new alerts that are created, or automatically create a ticket in JIRA for every new critical alert.

sentra.io