sentra

How Sentra is different from Legacy or Other Data Security Platforms

Secure Your Data Everywhere

Sentra is the global leader in cloud-native data security for the AI era. Sentra ensures data is secured no matter where it travels by automatically detecting privacy and security risks, misconfigurations, over-permissions, unauthorized access, data duplication and other security issues. It achieves this by intelligently discovering and classifying sensitive data, proactively managing security posture, automatically protecting data and sensitive data access, and swiftly detecting and responding to threats. Its AI-powered platform automates complex tasks, adapts to evolving data landscapes, and provides enterprise-grade security with expert support.

Platform Overview	Sentra's Data Security Platform	Legacy or Other Data Security Platforms
Time to Value	Install quickly in minutes. Immediate value	9-12 months to be fully operational in large environments
Scanning Architecture	Agentless, continuous and autonomous data discovery across IaaS, PaaS, and SaaS Includes known and unknown data	Limited discovery requires agents and network connectivity. Can not discover unknown (shadow) data
Low Operational Cost at Petabye Scale	1000X faster and 100X more compute efficient. Scans dozens of petabytes in a week using advanced ML-based clustering and sampling	Very expensive and compute intensive. Limited scalability Scan costs are 100X higher compared to Sentra
Robust Scan Settings	Highly customizable scans. Enterprise-ready	Too simplistic. No options to customize different scanning strategies

Data Classification	Sentra's Data Security Platform	Legacy or Other Data Security Platforms
Automatic and Accurate	Keeps pace with >95% accuracy in detecting PII, PCI, PHI, secrets and more AI-powered classification	Manual. Relies on regular expressions and customer-specific rules which create many FPs
Dynamic	Adapts itself to detect sensitive, organization-specific data, such as intellectual property and customer data	Generalized and limited to common sensitive data types only. Doesn't align to the organization's classification schema
Context Rich	Deep context on the data's business use, data residency, data security, and more	Missing critical context required by security, such as whether the data is real or synthetic.

Security Use-Cases	Sentra's Data Security Platform	Legacy or Other Data Security Platforms
Data Exposures	Rich context helps automatically map real exposures, such as shadow data, to compliance frameworks	Alerts on many false positives due to missing context. Does not help to reduce the data attack surface
Flexible Policy Engine	Allows users to easily create custom policies that match their security programs	Limited policies that do not allow to express security team requirements
Threat Detection	Data-aware detection of suspicious data access/activity. Stop data breaches in the cloud. Cloud DLP built for cloud-native attacks	Does not detect data-aware threats in data lakes and databases in IaaS and PaaS
Automatic Labeling	Tag and label data automatically. Integrates with DLP, SASE, and Data Governance tools	Limited to M365 and Microsoft Purview tags only
Data Similarity and Perimeters	Automatically detects when data moves and travels across designated data stores and data perimeters	Does not provide any detection when data is being duplicated or copied across zones
Secure and Responsible AI	Extends protection to GenAI/LLM applications, for strong risk posture and secure training sets, prompts, and outputs.	Many tools do not support AI services (within cloud providers)