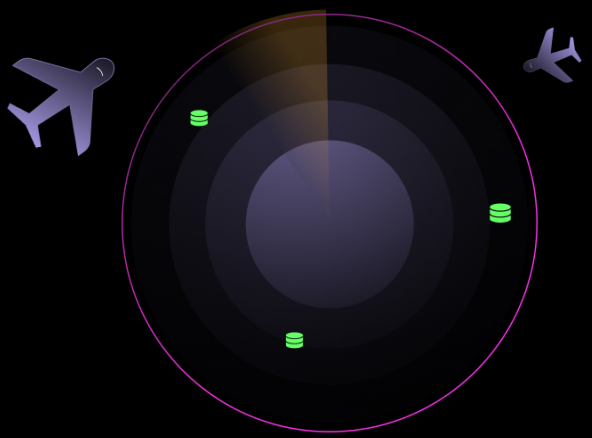
sentra

Securing Petabytes at Scale: How a Global Travel Platform Gained Control of Its Cloud Data in Just 30 Days



The Company:

- Global travel tech platform
- 100s of PBs customer data
- 600+ AWS accounts

The Challenge:

- Lack of cloud data visibility and control
- Manual tagging
- Data blind spots
- Reactive data security

Results:

- Discovery of sensitive data
- Streamlined governance
- Accurate classification
- Reduced false positives and alert fatigue
- Improved PCI DSS and GDPR compliance

In an industry where speed, data, and customer trust intersect, one of the world's top travel technology companies found itself at a critical inflection point. With hundreds of petabytes of sensitive data dispersed across more than 600 AWS accounts, their security team lacked the visibility and control required to manage risk at scale.

Traditional DLP tools weren't built for today's multi-cloud reality—they offered limited insights and reactive alerts. Manual data tagging was slow and error-prone. As compliance demands grew and insider threats became more complex, the organization needed a new approach.

That's where Sentra came in.

By adopting Sentra's Cloud-native Data Security (DSPM) platform, the company gained visibility into its sprawling data estate in just 30 days, compared to other solutions that take an entire year to fully implement. Sentra replaced manual tagging with AI-powered classification, and built a scalable framework for enforcing security policies. The result: enhanced risk posture, reduced manual effort, and a powerful partnership built on rapid innovation and enterprise-scale performance.

The Challenge:
Lack of Cloud Data Visibility and Control

Before Sentra, the company's data security strategy relied heavily on legacy DLP solutions that only flagged data after it left the environment—far too late to prevent exposure. This reactive approach created dangerous blind spots in environments where data was constantly moving.

Manual tagging compounded the problem. It was resource-intensive, inconsistent across teams, and prone to human error. With more than 600 AWS accounts and hundreds of petabytes of data, the organization had no reliable way to understand what data existed, where it lived, or how it was being accessed.

And while their cloud footprint had grown rapidly, their ability to govern data hadn't kept pace. Sensitive customer data was increasingly at risk of accidental exposure, misconfiguration, and noncompliance.

"The partnership has been really strong... we get custom features developed very quickly."

— Security Engineering Manager, Global Travel Platform

Why Sentra:
Scalable, Accurate, and Fast-Moving

After evaluating a broad mix of DLP and DSPM vendors the company chose Sentra for its unmatched combination of scale, classification accuracy, and flexibility.

Agentless discovery was key. Sentra's ability to scan vast, complex environments without requiring agents allowed for faster, broader deployment across the company's entire AWS footprint.

Automated classification replaced slow, error-prone manual tagging with accurate, AI-driven sensitivity labels that helped teams enforce access controls with confidence.

Scalability ensured fast time to value as Sentra efficiently handled hundreds of petabytes across hundreds of accounts—something many competitors couldn't match.

But what truly set Sentra apart was the partnership.

"The Sentra speed and support really stood out. We were able to quickly transform our approach to data security from reactive alerts to proactive discovery. We're not just detecting potential risks anymore; we're gaining a comprehensive inventory of our data landscape across hundreds of petabytes, enabling us to truly understand and protect our most critical assets."

— Security Engineering Manager, Global Travel Platform

Implementation: Tackling Scale and Complexity Head-On

The implementation targeted 600 AWS accounts, 170,000 data stores, and over 28,000 target S3 buckets, involving coordination across six internal stakeholder teams. The environment's complexity presented early challenges, including performance challenges related to scanning large, complex datasets that significantly expanded during processing.

Sentra's engineering team worked closely with the customer to resolve the technical bottlenecks, tuning the system for high-memory formats and refining scanning cycles.
Deployment was completed on schedule, with phased implementation continuing as classification efforts expanded. Beyond scanning, Sentra helped identify **unknown sensitive data exposures**, cut down on **manual tagging errors**, and provided the foundation for a policy-based approach to least privilege and access control.

Real Business Impact:
Visibility, Compliance, and Control

Within months, the company achieved what had eluded them for years—true visibility into their data estate. With automated classification and context-aware enforcement, the security team could now respond proactively to risk and reduce operational overhead.

Key outcomes:

- **Discovery of sensitive data** that had previously gone unnoticed
- **Streamlined governance** across 600+ AWS accounts
- **Accurate classification** reduces false positives and alert fatigue
- **Improved compliance** streamlined ability to meet PCI DSS and GDPR requirements

Sentra enabled the travel tech company to quickly discover previously unknown sensitive data, improve data classification accuracy, and provide comprehensive visibility across their multi-cloud environment, ultimately enhancing their data security posture and compliance capabilities. As the evaluation concluded, the global travel tech giant engaged in a multi-year DSPM agreement with Sentra.

Sentra for Travel Tech:
Setting the Pace for Scalable, Intelligent Data Protection

By adopting Sentra's cloud-native Data Security Posture Management (DSPM) platform, this global travel technology leader gained real-time visibility into its massive, fast-moving data estate spanning hundreds of AWS accounts and petabytes of sensitive data including unique data types like booking and flight information, in addition to PCI/PII. Manual tagging gave way to AI-powered classification, enabling precise, automated enforcement of data security policies at scale.

In doing so, the company replaced reactive alerts with proactive governance and transformed data security from a compliance bottleneck into a strategic advantage. In an industry where agility, trust, and innovation are everything, Sentra has empowered this travel tech giant to protect what matters most—without losing speed.

Gartner Peer Insights Customers' Choice 2025

Gartner Peer Insights™

4.9 ★★★★★

By Sentra in Data Security Posture Management (DSPM)

Setting a New Standard in Data Security

>95% Accuracy

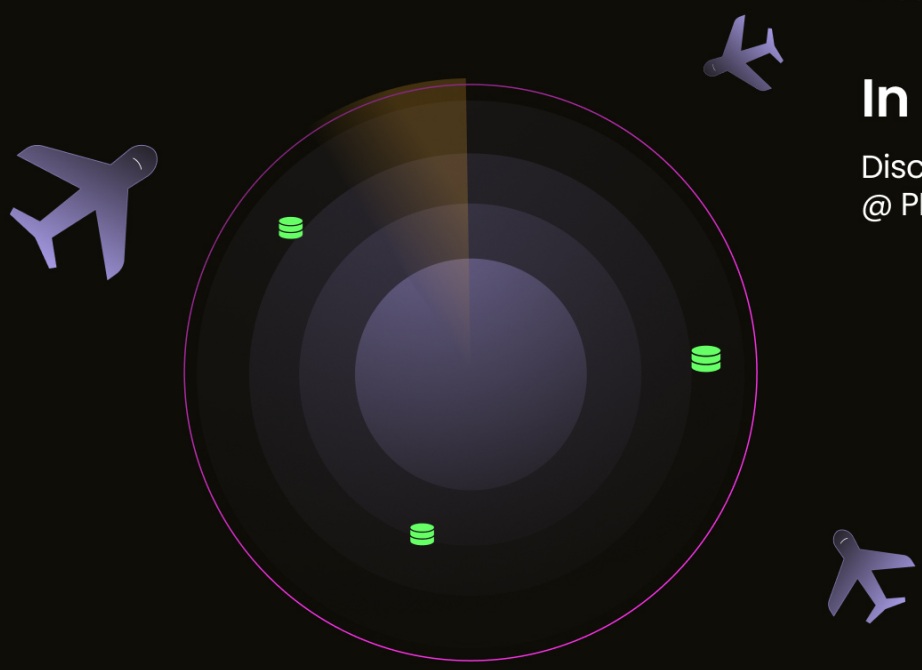
AI-powered classification

10x more efficient

In scanning compared to industry

In less than 1 week

Discover and assess data risks @ PB - scale



Visit www.sentra.io | Watch a demo

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