sentra

Ensure Secure and Responsible AI

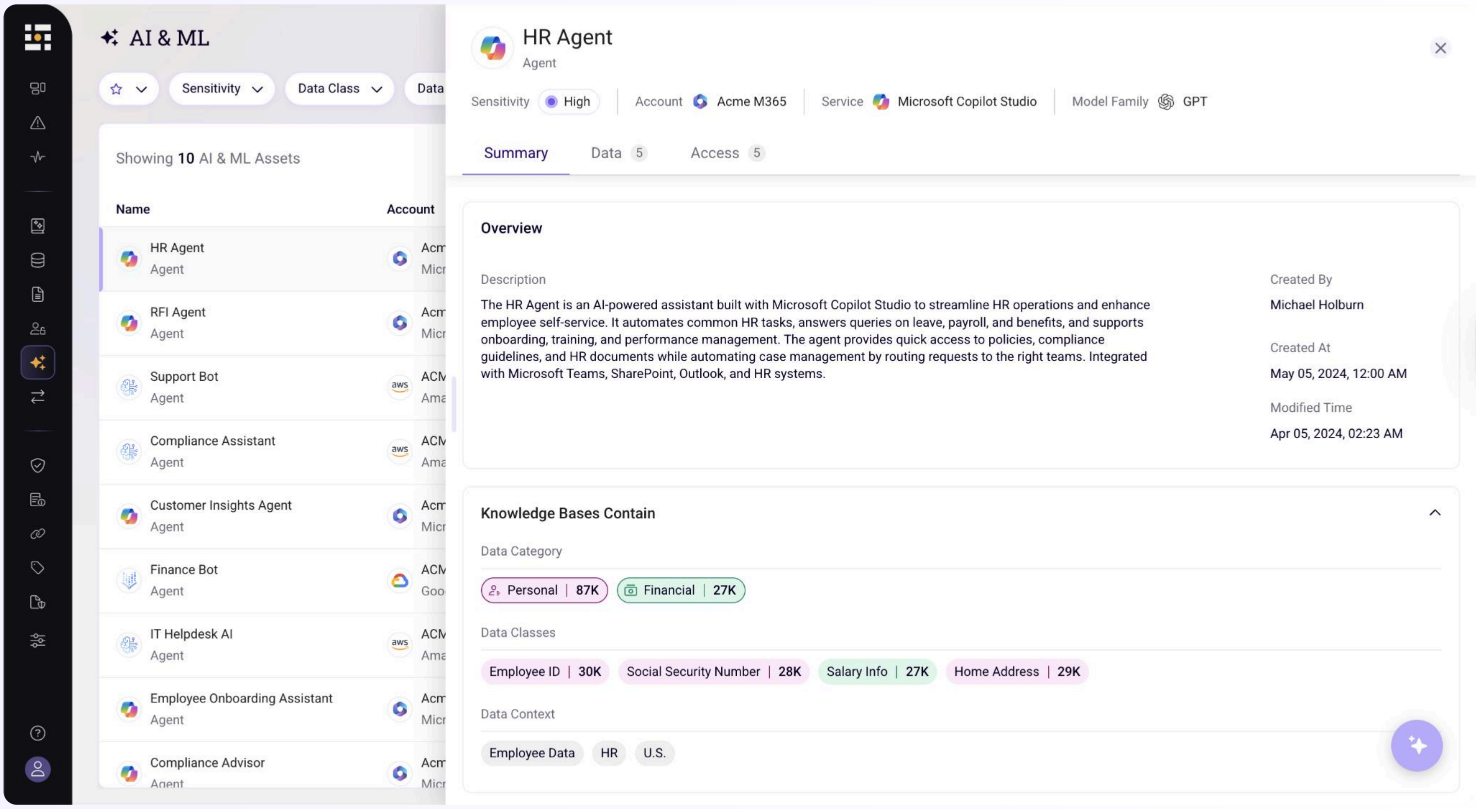
Control the data your AI uses to avoid leakage, privacy and compliance violations.

The Data Blind Spots Holding Back GenAI

As enterprises adopt GenAI and LLMs, data governance struggles to keep up. Unclassified training data and augmentation (RAG) data, and AI agents and copilots that access sensitive data create privacy and compliance risk. AI systems require the same data classification, access control, and enforcement as other regulated environments. Sentra brings enterprise-grade protection to the AI stack, securing training and augmentation data stores and monitoring sensitive data access to identify risky behaviors across the cloud.

See What Data is Exposed to AI Agent Users

Easily see who created the AI agent, when, for what purpose and the knowledge sources and users who can access it.



Showing **10** AI & ML Assets

Name	Account
HR Agent Agent	Acm Micr
RFI Agent Agent	Acm Micr
Support Bot Agent	ACM Ama
Compliance Assistant Agent	ACM Ama
Customer Insights Agent Agent	Acm Micr
Finance Bot Agent	ACM Goo
IT Helpdesk AI Agent	ACM Ama
Employee Onboarding Assistant Agent	Acm Micr
Compliance Advisor Agent	Acm Micr

HR Agent
Agent

Sensitivity: High | Account: Acme M365 | Service: Microsoft Copilot Studio | Model Family: GPT

Overview

Description
The HR Agent is an AI-powered assistant built with Microsoft Copilot Studio to streamline HR operations and enhance employee self-service. It automates common HR tasks, answers queries on leave, payroll, and benefits, and supports onboarding, training, and performance management. The agent provides quick access to policies, compliance guidelines, and HR documents while automating case management by routing requests to the right teams. Integrated with Microsoft Teams, SharePoint, Outlook, and HR systems.

Created By
Michael Holburn

Created At
May 05, 2024, 12:00 AM

Modified Time
Apr 05, 2024, 02:23 AM

Knowledge Bases Contain

Data Category
Personal | 87K
Financial | 27K

Data Classes
Employee ID | 30K
Social Security Number | 28K
Salary Info | 27K
Home Address | 29K

Data Context
Employee Data
HR
U.S.

Stop AI Access to Sensitive Shadow Data to Prevent Leaks

AI models and agents can't be governed if you don't know what data they touch and who has access to them. AI agents and copilots draw on dynamic production environment information that changes continuously. Sensitive information is often accessed or ingested into training datasets without proper classification, creating a risk of regulatory violations or sensitive data leakage. In a 2024 EY survey, 80% of CISOs expressed concern about AI agents exposing sensitive data, yet most lacked real-time monitoring. AI assistants can inadvertently access unclassified shadow data and leak internal knowledge outside the organization. Without clear lineage, access governance, or runtime oversight, organizations are blind to AI-related risks and unprepared for safe, secure, and accountable adoption of AI.

Sentra Secures the Full AI Data Lifecycle - From Ingestion to Output

Sentra helps enterprises secure the full AI data lifecycle from model training and evaluation to AI agent interaction. The platform automatically discovers, classifies, and protects sensitive data such as PII, PHI, and proprietary content before it enters AI or machine learning (ML) workflows, ensuring training datasets are sanitized and compliant. Sentra continuously monitors prompts, outputs, and AI agent behavior for signs of sensitive data exposure or misuse. Sentra also enforces identity-aware access controls and applies encryption, anonymization, and residency policies across multi-cloud environments. It also aligns AI data usage with leading frameworks like NIST AI RMF and ISO/IEC 42001, helping organizations reduce risk, meet regulatory requirements, and build secure, responsible AI applications at scale.

Why Enterprises Trust Sentra to Govern AI Data Use

Discover and classify sensitive data across AI pipelines

Monitor prompts, outputs, and agent behavior for data leakage

Enforce identity-based access controls, DLP, and security policies

Align and comply with NIST AI RMF and ISO/IEC 42001 AI data use frameworks

Global Retailer: Prevented AI Data Leaks and Achieved ISO Compliance

A leading global retailer used Sentra to govern sensitive data used in AI-driven supply chain forecasting and inventory optimization. As the company expanded its use of GenAI and LLMs across cloud platforms, Sentra identified unclassified PII and internal supplier data in training sets, helping prevent compliance risks and data leakage. The platform mapped data lineage across AI pipelines, enforced anonymization and residency policies, and monitored AI agent activity for unauthorized access. With AI-native classification and policy enforcement, Sentra enabled responsible innovation while maintaining GDPR and ISO 42001 compliance.

Ready to Secure Your AI Stack Before It Becomes a Liability?

Get A Demo

or learn more about how

AI in Data Security: Key Risks & How to Address Them

sentra