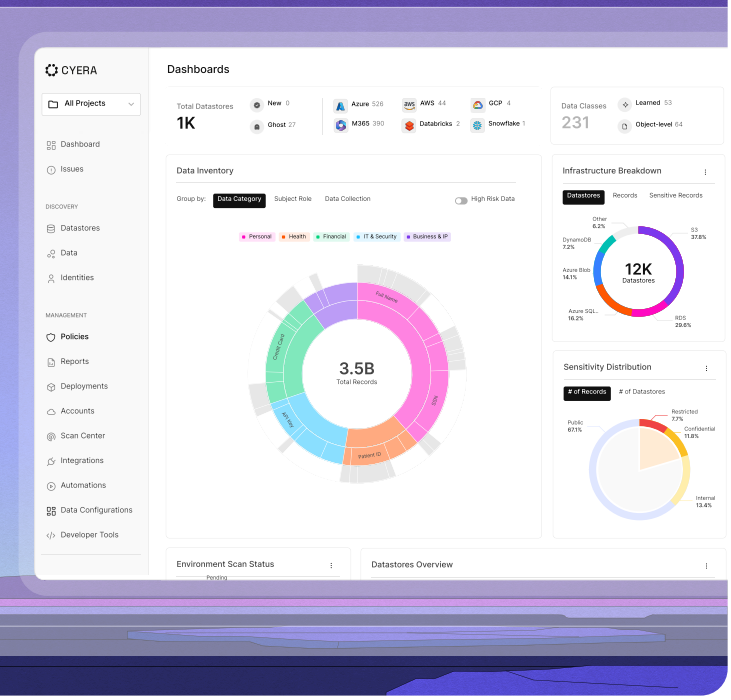
cyera | Microsoft

Solution Brief

Cyera + Microsoft

Secure your AI transformation with deep data insight and control

Cyera and Microsoft give you the data protection backbone to deploy AI with confidence - across your Microsoft estate and every cloud you use.



AI accelerates everything. Even your data risks.

As organizations roll out Copilot, build agents in Copilot Studio, and scale through Agent 365 and Azure AI Foundry, a compounding risk emerges: AI inherits the permissions and labels already in place, turning every deployment into a potential exposure. Microsoft provides the enforcement ecosystem. Cyera is the data intelligence layer that makes it work: precise classification that interprets context, continuous label validation, and automated policy evaluation and tuning.

Proven Results

98.5%+

classification accuracy across nearly 50B records, achieved by an enterprise financial institution using Cyera with Microsoft Purview

16,000→0

weekly false-positive DLP events eliminated at a large financial services firm across M365 and legacy file shares

150,000+

overshared M365 files eliminated within weeks of deployment across enterprise customers

The Challenge: Scaling Data Security for the AI Era

Microsoft Purview provides powerful tools for data security and governance. But as organizations scale to petabytes of data across cloud, SaaS, and on-premises environments, visibility often stays siloed within each platform, and accelerating AI adoption with Copilot and custom agents only widens the gap. Cyera addresses the enterprise-scale challenges Microsoft's platform wasn't designed to solve alone.

Classification at Scale

Microsoft Purview's SITs use pattern matching to find structured data, but a nine-digit number looks the same whether it's an SSN or a part number.

How Cyera solves it: Automated AI classification understands the data itself, then adds context Purview can't: who can access it, whether it's truly identifiable, and how it's being used.

Label Accuracy and Consistency

Sensitivity labels drive DLP, encryption, and access controls, but maintaining accuracy across millions of files is hard, especially as users mislabel content and labels drift over time.

How Cyera solves it: Build and manage the policies that keep labels accurate and consistent at scale, including for files that can't be labeled by design.

Alert Volume and Prioritization

DLP rules generate alerts, lots of them. At enterprise scale, even well-tuned policies produce enough noise to bury real incidents.

How Cyera solves it: Automated triage separates urgent from routine, surfacing the alerts that actually matter.

Copilot and Agent Readiness

Copilot respects existing permissions and labels, so your data hygiene directly determines what it can surface. Copilot Studio agents go further: they access enterprise data, call external APIs, and take autonomous actions at machine speed, without human review of each decision.

How Cyera solves it: Discover and protect sensitive data before Copilot and agents can access or expose it, closing the gap data hygiene leaves open.

You can't govern agents if you don't know they exist, what data they can reach, and what that data actually contains.

Joint Solutions

Cyera for Microsoft Purview

Enforce enterprise-grade data protection with precision labeling from Cyera and Purview. Cyera integrates with Purview via the Microsoft Graph API to close the classification gaps that prevent your policies from working as designed.

Label files accurately.	Tag sensitive data with 97% precision using Cyera's AI-powered classification engine, which understands context, identifiability, and severity, not just pattern matches, extending coverage to custom categories and file types beyond standard SITs.
Automatically fix gaps.	Detect missing or incorrect labels and apply the right sensitivity tags using AI-powered grouping that prioritizes the data that actually carries risk, either in bulk with a single click or fully automated, with no manual review or re-classification work required.
Enforce policies with confidence.	Cyera applies and keeps labels accurate across OneDrive and SharePoint, and once labeled, Purview policies enforce protection everywhere those labels travel, including Azure and Exchange, so your protections hold even as data moves and changes.

Cyera for Microsoft Purview DLP

Unify your siloed data loss prevention tools and move from reacting to orchestrating. Cyera Omni DLP works with Purview to give security teams the signal they need to act on what matters.

Build SITs and policies from real data, not assumptions.	Cyera analyzes your actual data estate to generate custom Sensitive Information Types, then builds DLP policies combining one or more SITs around them. We also test what you already have and recommend changes to make it more accurate and precise, drastically cutting the time it takes to manage Purview DLP policies.
Shrink DLP false positives by up to 98%.	AI-driven analysis surfaces real incidents and cuts through the noise, so your team spends time on the alerts that actually matter.
Tune policies and resolve alerts in minutes.	Cyera shows you what happened, why it triggered, and what to do next, then lets you tune policies and push the changes back to Purview, no more hunting for context across fragmented consoles.

Cyera for Microsoft 365 Copilot

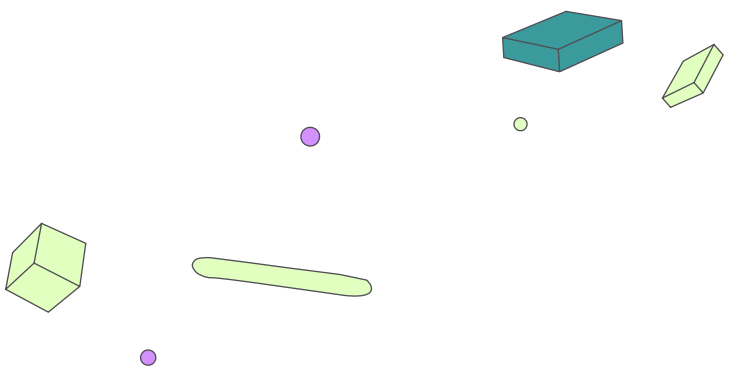
Secure AI adoption starts with securing data at the source. Cyera discovers and protects sensitive data before M365 Copilot can access or expose it, spanning the full deployment lifecycle from pre-launch hygiene to runtime monitoring.

Discover AI-accessible data before deployment.	Know exactly what Copilot will access before you turn it on. Find sensitive files without labels, overshared data, and excessive permissions, and fix them first.
Classify all data, human or AI-generated.	Apply sensitivity labels so Purview policies cover everything Copilot can reach, regardless of file type, age, or who created it.
Detect AI misuse and data leakage.	Log and analyze Copilot prompts and responses to catch misuse, data leakage, unauthorized access, and prompt injection attempts.

Cyera for Microsoft 365 Data

Cyera gives you full visibility into sensitive data across your M365 estate: OneDrive, SharePoint, Teams, and Exchange. Know exactly where risk lives and act on it before it becomes a problem.

Discover sensitive data across your M365 estate.	Scan OneDrive, SharePoint, Teams, and Exchange to understand what sensitive data exists and who can access it, then apply accurate sensitivity labels across OneDrive and SharePoint.
Remediate overshared data and excessive access.	Identify files exposed too broadly, revoke excessive permissions, and close the access paths that put sensitive data at risk before an incident occurs.
Maintain data hygiene as your estate grows.	Continuous classification keeps new data, new users, and new workspaces in scope automatically. No manual re-scans required.



Cyera for Microsoft Agent 365

Agent 365 is Microsoft's control plane for the AI agent ecosystem: it governs agent lifecycle and enforces policy across the tools that build, identify, and run agents at enterprise scale. Entra Agent ID gives every agent a verifiable identity. Copilot Studio is where most enterprise agents get built. Azure AI Foundry is where models are trained and deployed. Cyera secures the data layer underneath all of it, so the data agents can reach is classified, governed, and safe to act on.

Cyera for Entra Agent ID:

Know which agents can reach your most sensitive data.

Cyera maps Entra Agent IDs to the sensitive data each agent can access across SharePoint, OneDrive, Azure, SaaS, and databases, so you can see where agent access creates the highest risk and act before it becomes an incident.

Cyera for Copilot Studio:

Secure the data agents can touch.

Ensure agents built in Copilot Studio don't reach into sensitive, regulated, or improperly labeled data. Cyera classifies the underlying data estate so agent permissions reflect actual risk, not assumed access boundaries.

Cyera for Azure AI Foundry:

Govern the data that trains and grounds your models.

Classify sensitive data in Azure storage, data lakes, and databases before it's used as training data or RAG context. Cyera enforces Purview policies at the point of ingestion so only labeled, authorized data enters Foundry workflows, and continuous classification keeps your security posture as AI workloads scale.

Cyera for Microsoft Azure

See your data risks in Azure and every other cloud with Cyera's DSPM. Cyera connects agentlessly to 40+ data sources: Azure, AWS, GCP, SaaS, IaaS, and DBaaS.

Assess your data security posture.

Understand your attack surface with insights from identities, access, encryption, backups, and the location of sensitive data across every environment you use.

Classify with unmatched breadth and depth.

Discover and classify files and records with 95%+ precision and enriched business context, using one engine that works consistently across every infrastructure and SaaS platform. See all your sensitive data in a single view and act where real risk is highest.

Automate remediation at scale.

Eliminate public exposure, correct sensitivity labels, notify data owners, and trigger workflows automatically, shortening the find-and-fix cycle significantly.

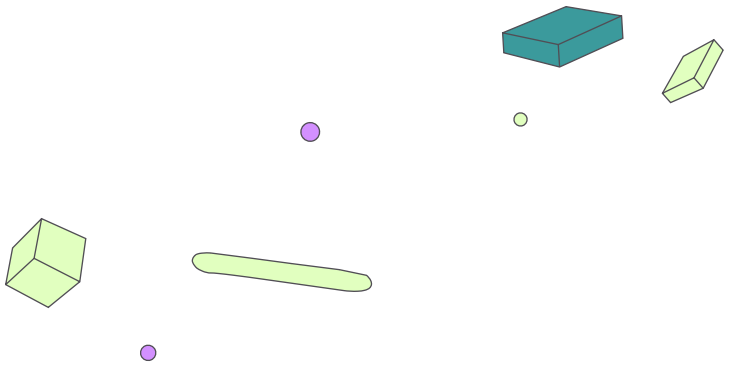
Cyera for Azure AI Foundry

Azure AI Foundry enables organizations to build, tune, and deploy AI models at enterprise scale. Cyera ensures the data that trains, grounds, and flows through those models is classified, governed, and safe to use.

Secure the data that trains and grounds your models.	Classify sensitive data in Azure storage, data lakes, and databases before it's used as training data or RAG context, keeping PII, IP, and regulated data out of model inputs.
Apply policies before data reaches AI pipelines.	Use Cyera's classification to enforce Purview policies at the point of ingestion, so only labeled, authorized data enters Foundry workflows.
Maintain visibility as AI workloads scale.	Continuous classification keeps pace with AI-driven data access so your security posture holds as adoption grows.

Unified AI-powered policy engine for posture and runtime across channels

- Integration with Microsoft and 40+ other data sources
- AI-powered classification with 95%+ precision
- Agentless deployment with fast onboarding
- Granular identity and data access visibility
- Risk-based prioritization and policy recommendations
- Automated remediation for Azure and M365



See what Copilot can already reach across your environment.

Request your free Copilot Risk Report →

Learn more at cyera.com/partnerships/microsoft →