sentra Microsoft Purview

Solution Brief

Go beyond Microsoft Purview

Better visibility. Smarter protection with Sentra.

Are your files labeled correctly? Who actually has access to them? What could Copilot surface next? Purview enforces your labels and DLP policies. Sentra makes sure they act on the right data, without replacing the controls you already rely on.

91%
precision for Sentra's latest file-level models, up from 71%

~1,000
"General Use" files found holding highly confidential personal data

9 PB
scanned in under 72 hours in a Fortune 500 side-by-side test

140+
file types, including emails, archives, attachments and scans

The challenge

Purview is only as accurate as the labels and access data behind it

Confidence is not accuracy
A SIT's confidence level reflects corroborating evidence, not whether the match is right, so business documents trigger floods of false positives.

English-only custom classifiers
Custom trainable classifiers support English only and can't be retrained once published, a gap for global organizations.

Blind spots beyond Office files
Labeling centers on Office documents and PDFs. Emails, archives, attachments, images and scans are easy to miss.

Oversharing you can't see
Even a correctly labeled file is at risk if it's shared too widely, and Copilot makes that exposure one prompt away.

Six ways Sentra makes Microsoft Purview better

01

More accurate classification

Context-aware, multilingual AI that understands what a file actually contains.

02

Trustworthy sensitivity labels

Safe, automated labeling that Purview DLP and encryption can act on.

03

Oversharing control

Every exposure path in SharePoint and OneDrive, tied to how sensitive each file is.

04

Remediation with owners

Policy-driven fixes that don't bottleneck the security team.

05

Visibility at M365 scale

Every file inventoried and searchable, at petabyte scale.

06

Protection beyond M365

The same controls across Azure, other clouds, SaaS and on-premises data.

© Sentra 2026. All rights reserved. Confidential.

01

More accurate classification

Classification that reads context, not just patterns

Business and privacy context

Personal vs. business tax IDs, real vs. test data, and whose data it is (customers, employees, patients).

Every language

Recognizes invoices, payslips, contracts and bank statements by content, across languages and local formats.

Every file type

140+ types across structured and unstructured data, including emails, archives, images and scans.

Global identifiers

National IDs, tax IDs, bank details and passports across Europe, LATAM and APAC, out of the box.

Custom classes

Combine entity- and file-level classes, and add rule-based or AI classifiers for your own data.

Tune without rescanning

Classification changes apply to already-scanned data in hours, not weeks.

In the field: file-by-file comparison at a global enterprise

~59,000
files matched by Purview across all confidence levels

<900
left at Purview's own "High" confidence tier, mostly customs and finance paperwork

~1,000
"General Use" files Sentra found holding highly confidential personal data

02

Trustworthy sensitivity labels

Labels Purview DLP and encryption can act on

Apply and upgrade labels

Reads Purview labels at file and site level, then applies or upgrades them from classification.

Simulate first

Every policy can run as a simulation with per-file reasoning: current label, proposed label, why.

No downgrades

Existing labels are never overridden or downgraded. Signed documents stay intact.

Mismatch detection

Flags under- and over-labeled files, and sites labeled below the files they hold.

Posture policies

Catch sensitive files that are unencrypted, public or outside their region. No code needed.

Private investigations

Findings show as metadata and masked samples, so no one reads employee files.

03

Oversharing control

Stop oversharing before Copilot finds it

Every exposure path

Anyone links, external users, guests, trusted domains, org-wide access and nested groups.

Why access exists

Sharing link, direct grant or group inheritance, view or edit, across every path to the file.

Attribution and history

Who shared, with whom, when and how, kept as evidence and exported daily.

Site and folder level

Sites labeled below their files, and folders shared externally or anonymously.

Granular policies

Group-size thresholds plus label, data class and context conditions in one builder.

Stale and shadow data

Unread sensitive files, duplicates and orphaned OneDrives that Copilot can still reach.

Next: 04 · Remediation with owners, page 3 →

Precision figures compare Sentra's latest models with its previous models on a held-out sample of 20 customer organizations.

© Sentra 2026. All rights reserved. Confidential.

04

Remediation with owners in the loop

Close exposure without bottlenecking security

Policy-driven fixes

Remove anonymous links, external or org-wide sharing, specific access or stale permissions, one at a time or in bulk.

Owners in the loop

One email or Teams message per owner. Fix it or accept the risk with a reason. Unresolved issues escalate.

Context for your stack

Classification, access and activity context flows to DLP, SIEM, SOAR and catalog tools via API, exports and webhooks.

05

Visibility at Microsoft 365 scale

Every file in SharePoint, OneDrive and Teams

9 PB

scanned in under 72 hours in a Fortune 500 side-by-side test

Predictable cost

About $40,000 a year to scan 100 PB, with a clear signal when classification is complete.

Searchable catalog

Filter every file by class, label, access and activity, not just site, folder and file name.

06

Protection beyond Microsoft 365

The same protection wherever data travels

Data Detection and Response

Extends real-time threat detection beyond Purview IRM to Azure and non-Microsoft environments.

Data perimeters

Alerts when sensitive data leaves its perimeter across Microsoft 365, Azure and other clouds.

AI data security

Monitors datasets that train and ground AI, including Copilot, for privacy violations and misuse.

A richer Purview catalog

Adds access-governance metadata and automated GDPR and CCPA assessments.

Code and structured data

GitHub, Azure DevOps, Azure SQL, Cosmos DB and Snowflake.

In-place scanning

AWS, Google Cloud, Databricks, Salesforce, ServiceNow, Jira and file shares. No egress charges.

At a glance

Area	Microsoft Purview	Sentra adds
Classification	SITs and trainable classifiers	**Context-aware, multilingual AI that drives labels**
Enforcement	Labels, DLP, encryption, Copilot controls	**Accurate labels so enforcement fires on the right files**
Access	Sharing settings per site and file	**Every exposure path, ranked by sensitivity, fixed with owners**
Threat detection	Insider Risk Management for M365 apps	**DDR across Azure and non-Microsoft environments**

See Sentra and Microsoft Purview working together

Find mislabeled and overshared files in your own tenant, before Copilot does.

Book a demo

© Sentra 2026. All rights reserved. Confidential.