



SENSITIVE INFORMATION PROTECTION

Assessment and scanning for structured
data at rest

TODAYS MARKET

AI is everywhere! This is true today, not sometime in the future. A year ago, we heard this was coming... and now it is a reality. Above and beyond the "trending" aspect, we need to recognize that users see so many benefits from solutions like Microsoft 365 Copilot and those benefits enable the organization to get the most out of their investments in AI:

- Optimized collaboration
- Easy data search across all collaboration repositories
- Meeting summaries
- E-mail and document crafting and summarization

THE CURRENT BUSINESS LANDSCAPE

- Users have access to multiple communication channels
- Users access data from multiple, and possibly unprotected, devices
- Uncontrolled access to sensitive information
- Lack of security controls to properly manage files
- Lack of good practices in the protection of information
- Lack of analytics for information security decision-making

SENSITIVE DATA IS EVERYWHERE

- Credit card numbers
- Financial information
- Social security numbers
- Intellectual property
- Personal information
- E-mail password
- Intellectual property
- Confidential medical information
- Biometric or genetic information

- Patents
- Business and marketing plans
- Customer and suppliers' information
- Financial data
- Intellectual property
- Patents
- Applications access credentials
- Sales secrets
- Pricing information

Protection of sensitive information directly affects regulatory compliance



CHALLENGE

While many of these amazing capabilities can provide tremendous benefits to the business, many organizations may have to prepare their environment to get themselves ready to get the most out of Copilot without taking the risk of data exfiltration.

RISK

AI can do things at the speed no human can do; however, organizations must do their due diligence before they can simultaneously meet both the CIO and CISO objectives. The collaborative and efficiency benefits provided by Copilot are game changers. At the same time, they cannot come at the cost of oversharing of your sensitive information, potentially across the entire organization and beyond!

Let's look at the following scenarios:

SCENARIO I

A person asks Copilot about "business re-orgs/upcoming strategic plans/firing situation" and, if proper controls are not in place, the requestor might be able to see a confirmation of upcoming personnel decisions with specific details, including names, performance reviews, and more.

SCENARIO II

A person asks Copilot about "compensation details" and, just like the example above, if proper controls are not in place, requestors can see as many details as they ask for in the prompt, including salaries, bonuses, financial numbers, and names.

SCENARIO III

N – Serve yourself, yes you got it! Through any "creative" prompt to Copilot, a requestor can surface sensitive and confidential information that should not be shared with that person.

But what are the current security controls that could mitigate these scenarios and prevent leaked and oversharing of sensitive information?

Existing Mitigation Strategies:

Access Permissions (ACLs)

- People will not see information in Copilot's answer from content stored in repositories that the user does not have permission to access

Questions:

- Has the organization implemented user access governance?
- Has the group management and, more importantly, group nesting implementation been reviewed, tested, and documented so you can identify potential changes?



- Do you grant anonymous or “anyone” (all tenant) access or B2B access to data at rest?

Encryption (via labeling)

- People will not see information in Copilot’s answer from content where the user does not have encryption permissions to the file (typically encrypted with Purview IP)

Questions:

- Does the organization have granular labels implemented across M365?
 - Is all data labeled AND encrypted?
 - Adding visual markings through headers and footers is not enough.
 - Even if a document is encrypted, Copilot may still use those files on behalf of the user.
 - Is the user allowed to export data from those documents? If so, Copilot can return those results.
- Is group management and, more importantly, group nesting reviewed, tested, and documented so you can identify potential changes and risk within your data classification and the people allowed to access certain data labels?

Future Mitigation Strategies

- As of this writing, you cannot set exceptions for paths to be “scanned” by Copilot; we hope Microsoft provides this capability in the future.

Bottom line, we are looking at a critical tradeoff between business, technology, and compliance.

Copilot can clearly do what is “fair” and right:

People with “explicitly” defined access can receive responses to the queries listed above.... But this makes a HUGE assumption of your environment. What is sensitive data to your organization, who should be able to see it, and is that configured correctly across your Microsoft 365 platform? Can any organization really assume that their environment is perfect and every file (while in use, in motion and at rest) has authors, contributors, and administrators who have set the right access and content permissions? And yes this applies across M365 and to wherever you keep unstructured documents and other files.....

Well now what can you do? Read the rest of this blog and the following series for the strategy that Synergy Advisors, an information protection and governance consulting company with more than 20 years of experience in the market working with top 100 accounts across multiple countries and segments, can recommend to QUICKLY assess and remediate your environment in preparation for Microsoft Copilot.


NEXT LEVEL OF PROTECTION

Even at rest, your data is dynamic with multiple servers and locations, multiple access vectors and actors, multiple copies of the data, and multiple administrators. Keeping control is complex!

INTRODUCING EDOs: E-SUITE DISCOVERY OFFERINGS FOR DATA GOVERNANCE

Synergy Advisors offers you the way to enhance your data governance and information protection strategy through the E-Suite Discovery Offering (EDO): assessments and scans carried out on your on-premises, multi-cloud, and software-as-a-service (SaaS) data locations, enabling you to proactively discover, protect, and manage sensitive information within your organization. Discovering what type of data, where it is located, and who accesses it in your organization is the most effective first step to develop a protection and mitigation strategy.

We can help you build an inventory and analysis of your data at rest to establish a data protection and mitigation plan



Discover what kind of sensitive information you have and where it is



Understand who is accessing your sensitive information and in what way



High-level action plan to optimize your security controls

HOW DOES AN EDO WORK?

DETAILED ASSESSMENT, SCANNING, AND FINDINGS

QUICK ASSESSMENT [1-2 WEEKS MAX]

- Minimal organizational impact
- Minimal organizational resources needed

FINDINGS AND RECOMMENDATIONS

- Detailed automated findings
 - Powered by Synergy Advisors E-Suite products
 - Leverage existing/trial M365 E5 / Azure capabilities
- Synergy Advisors expert review and advisory session(s)



LET'S CONTINUE THE PROTECTION JOURNEY:

SCANNING FOR STRUCTURED DATA

Synergy Advisors brings an assessment to be carried out on your structured data file storage locations, that enables your organization to strengthen its data governance strategy, through the following components:

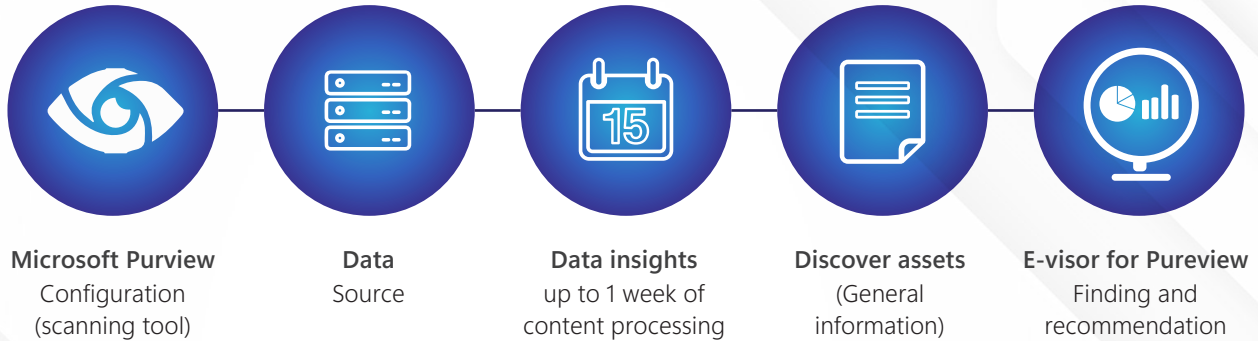


EASY PROCESS FOR GREAT RESULTS



HOW DOES THE ASSESSMENT WORK?

Synergy Advisors extends Microsoft Purview capabilities to scan structured data and then presents a comprehensive report with business and technical-driven analytics through our E-Visor tool.



SCOPE OF THE ASSESSMENT

WORK PRODUCT
Package
Scan configuration +
inventory inspection + data scan

- Azure SQL Database
- 10 Gb / 1 Week + E-Visor for Purview

DELIVERABLES

- Findings and recommendations
- E-Visor for Purview report
- Discover sensitive files by info type and custom patterns
- File discovery by metadata

WHAT DO YOU NEED TO KEEP PROTECTING YOUR SENSITIVE INFORMATION?

AZURE

Existing subscription or...
Request an Azure Pass
(available for non-Azure customers as a trial)
Existing Azure SQL Database

MICROSOFT 365

Office 365 E3 + Enterprise Mobility + Security E5 (Existing or Trial)
Office 365 E3 + Microsoft 365 Information Protection and Governance (Existing or Trial)
Microsoft 365 E5

WHAT WILL YOU RECEIVE AFTER THE ASSESSMENT?

ACTION PLAN ROADMAP

Co-creation of an expert plan for your specific scenarios, potential impact analysis, and mitigation steps.

FILE INVENTORY

Complete file inventory and data metrics through E-Visor and Power BI exportable reports, with recommended MIP label and sensitive data found.

PLUS!: POWER BI EXPERIENCE FOR DETAILED AND STRATEGIC ANALYTICS IN MULTIPLE VIEWS



Sensitive data inventory and storage

Type and location

Sensitive data classification

BOOST YOUR DATA GOVERNANCE STRATEGY WHILE PROTECTING SENSITIVE DATA

WHY CHOOSE SYNERGY ADVISORS AS YOUR STRATEGIC PARTNER IN DATA GOVERNANCE?

Through our solutions and services, we can show you the status of the information ecosystem of your organization's structured and unstructured data, on your Microsoft 365 technology, on-premises infrastructure, or SaaS services, enabling you to optimize your investment in Microsoft technology.

ABOUT US

Synergy Advisors is a premier Microsoft Certified Partner that specializes in Microsoft 365, Identity, Azure B2C and B2B Collaboration, Security, Management, and Cloud technologies. We help you digitally transform and implement a more secure collaborative infrastructure, reduce your IT costs, and meet your regulatory requirements through our comprehensive portfolio and experience in consulting and managed services.



Secure E-mail

- Users
- Apps
- Services
- Hygiene
- Threats
- Data Leak Mitigation



Secure Collaboration

- Users (internal / external)
- Apps
- Services
- Hygiene
- Threats
- Data Leak Mitigation



Device Protection

- Applications security
- O.S. security
- Security base line
- Threats
- Data Leak Mitigation



Information Protection

- Data in use
- Data at rest
- Data in transit
- Application integration
- Data Leak Mitigation
- Structured and unstructured data protection



Platform Protection

- Monitoring / Services analysis/ Alerts and notifications
- Security base line

CONTINUE THE PROTECTION JOURNEY WITH THE FOLLOWING EDOs:

- EDO for unstructured data: [Let's go!](#)
- EDO Plus – unstructured and structured data: [Let's go!](#)

OTHER EDOs FOR A COMPREHENSIVE STRATEGY

Synergy Advisors provides a complete portfolio of discovery offerings that enable you to cover your strategy from Security, Compliance, Identity, and Cloud perspectives. Click [here](#) to learn more.

Contact us for more information: [HERE](#)
Or e-mail us at: ww-sales@synergyadvisors.biz

LET'S START!



Synergy Advisors LLC



Synergy Advisors



@Synergyadvisors



Synergy Advisors



@SynergySEC