

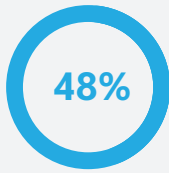
Centralize information in cloud repositories



Leverage the capabilities of modern environments

To optimize your unstructured data is to improve the visibility and security of your information, which is critical for reliable data to support intelligent decisions and for comprehensive file management.

Ponemon / Entrust



... of organizations say the biggest challenge is to know where their data is located



... of organizations in the United Kingdom failed a data audit



... of companies hesitate to incorporate their repositories into the cloud, due to lack of data protection strategies

How to achieve a safe transition of your data to the cloud?

Centralizing organizational information, taking advantage of the capabilities of cloud repositories and the document management capabilities they provide, is now possible in a secure manner, protecting data from end to end.

Synergy Advisors has developed a comprehensive offering for repository modernization and secure data migration to the cloud, including integration with cloud tools to ease the transition.



Custom plans

Basic	Standard	Enterprise
<ul style="list-style-type: none"> • Inspection of several data sources • Migration of the data to the cloud • Monitoring and reporting of the new environment performed by Synergy Advisors E-Suite solutions. 	<ul style="list-style-type: none"> • Inspection of several data sources • Detection of sensitive data • Migration of the data to the cloud • Monitoring and reporting of the new environment by E-Suite 	<ul style="list-style-type: none"> • Inspection of several data sources • Detection of sensitive data • Document protection using MIP and DLP • Migration of the data to the cloud • Monitoring and reporting of the new environment by E-Suite

Scope

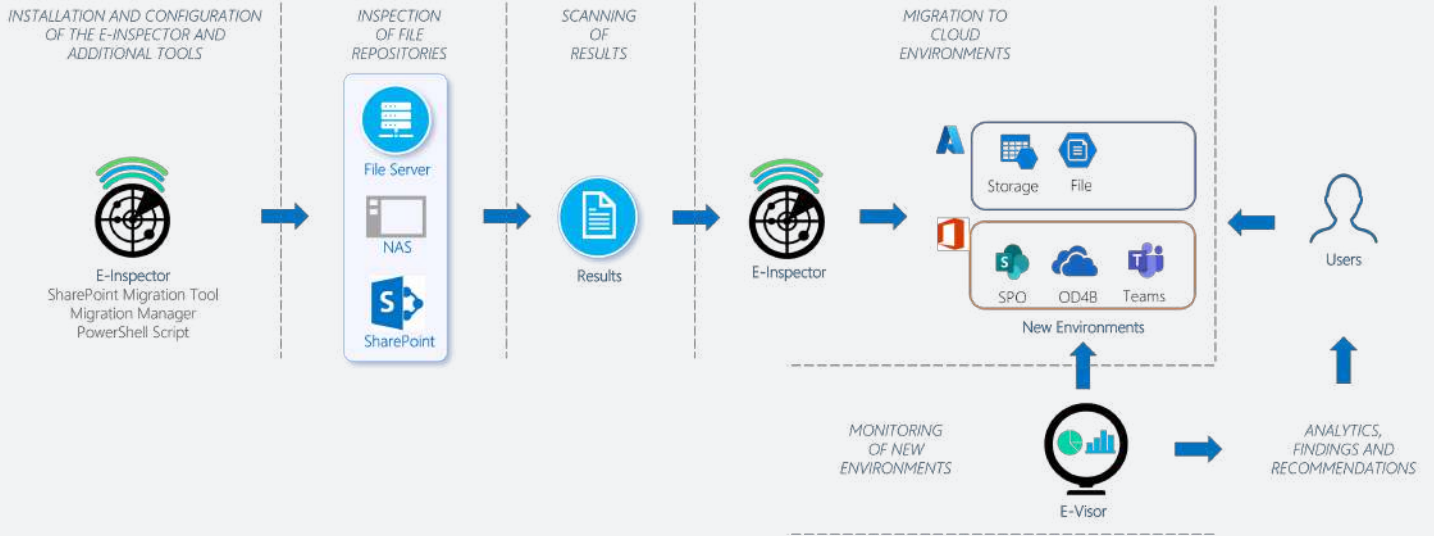
Modules	Inspection	Detection	Protection	Migration	Monitoring
Roadmap	Scan different repositories to determine the following information: 1. Repositories size (TB) 2. Type of files 3. Number of documents	Sensitive content type detection across the documents in the repositories	Usage of MIP and DLP to protect the documents and establish policies to label restricted information	Move the data from the original location to M365 or Microsoft Azure	Scan the new repositories and review the way your users work with the information
Basic	●			●	●
Standard	●	●		●	●
Enterprise	●	●	●	●	●

Module processes

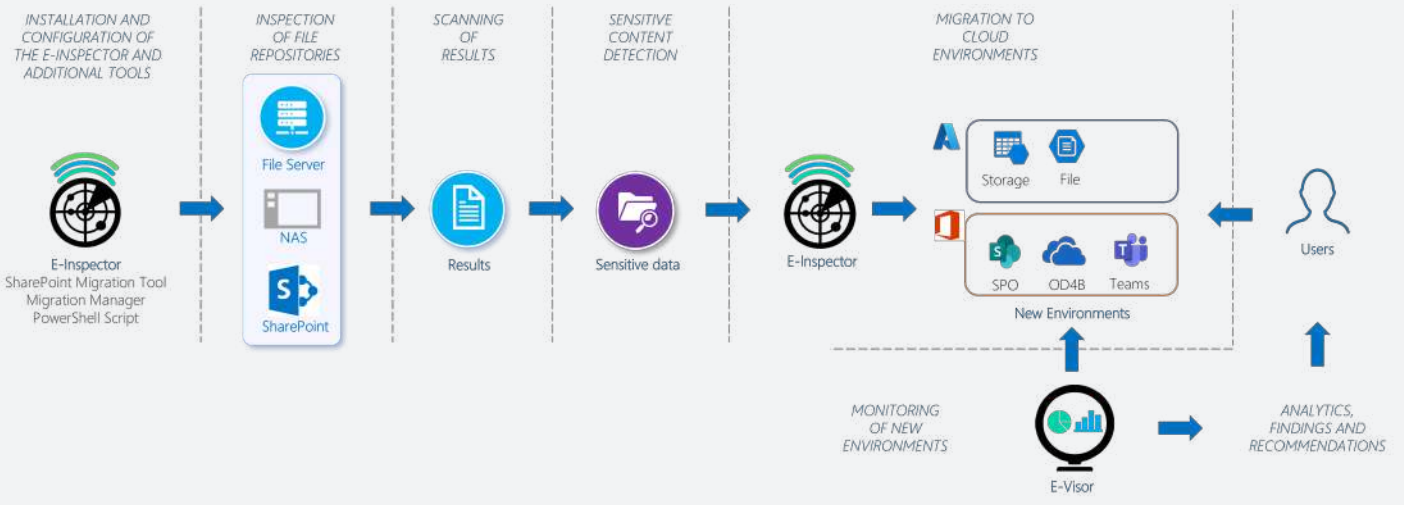
 Inspection	 Detection	 Protection	 Migration	 Monitoring
<p>Design</p> <p>Objective Meet with the information owners to identify the data source, permissions, and size of the repository</p> <p>Repositories 1. NAS 2. File Server 3. SharePoint On-premises</p>	<p>Scan Files</p> <p>Objective Use E-Inspector to scan the information inside the documents to create a map by document type</p> <p>Activity Scan all files inside the data source to create a map to identify the location of the confidential information</p>	<p>MIP</p> <p>Objective Create Microsoft Information Protection labels and policies to tag the documents</p> <p>Activity Auto-tagging can be enabled in the cloud or in the local environment</p>	<p>E-Inspector</p> <p>Objective Migrate the data from different data sources to the new environment</p> <p>New environment 1. SharePoint Online 2. OneDrive For Business 3. Teams 4. Azure File Share</p>	<p>Scan</p> <p>Objective Scan the new repositories in M365 and Microsoft Azure adding migrated and new documents</p> <p>Repositories 1. SharePoint Online 2. OneDrive for Business 3. Teams 4. Azure Files</p>
<p>Prepare environment</p> <p>Objective Access to the different data sources, install and prepare the different tools to get the information (scripts, specialized tools)</p> <p>Tool: 1. E-Inspector 2. SharePoint Migration Tool 3. Migration Manager 4. PowerShell Scripts</p>	<p>Sensitive info by type</p> <p>Objective Determine the sensitive information inside the local repositories and recommend a security label</p> <p>Activity Use E-Inspector and MIP to determine the sensitive info by type</p>	<p>DLP</p> <p>Objective Create Data Loss Prevention policies to work with MIP labels and detect possible information leaks</p> <p>Activity Control the information shared with internal and external users</p>	<p>Additional tools</p> <p>Objective Use specific tools to migrate additional information</p> <p>Activity Work with Microsoft FastTrack to migrate additional information</p>	<p>Detect</p> <p>Objective Detect new content, review the use of tags and policies, include new documents in the metrics</p> <p>Activity Review the new documents, the sensitive info types, and labels in the new environments</p>
<p>Scan repositories</p> <p>Objective Run the different tools to know the information related with the number of documents, repositories size, and type of the documents</p> <p>Scan process 1. Get the information from the different tools 2. Reports are rendered as.CSV files</p>		<p>E-Inspector</p> <p>Objective Scan and label documents inside the data source following the MIP and DLP rules</p> <p>Activity Label the document before migration to the new environment</p>	<p>Adoption</p> <p>Objective Define the training topics related with the new environments</p> <p>Activity Training sessions with the final users to show them the new tool capabilities</p>	<p>Notify</p> <p>Objective Notification of violations related to MIP and DLP</p> <p>Activity Notification to the admin team and end user when document violations appear in the environment</p>
<p>Review scanned data</p> <p>Objective Determine how many repositories could be migrated to the M365 and Microsoft Azure environments</p> <p>Repositories 1. Size 2. Type of files 3. Quantity</p>				<p>Report</p> <p>Objective The information will be up to date in a Power BI report dashboard and shared with the admin</p> <p>Activity Consolidate the information related with the different data sources</p>

How does each scope work?

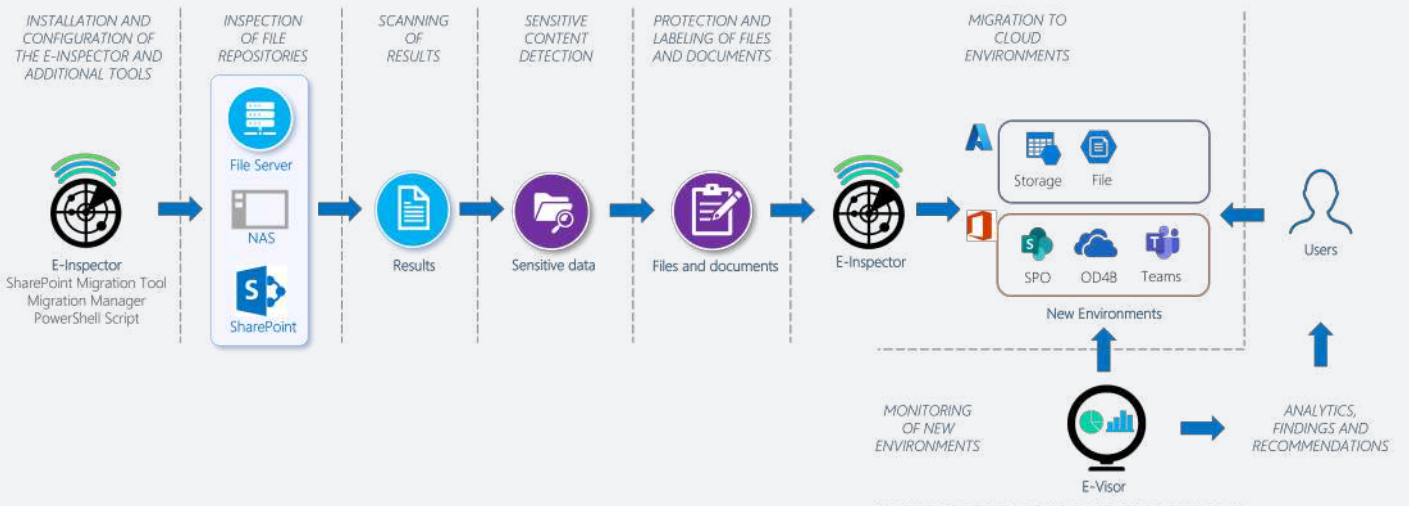
Basic



Standard



Enterprise



Main benefits of this modernization



Better use of available cloud storage located



Local hardware lightweighting



Proactive centralization of information for better management



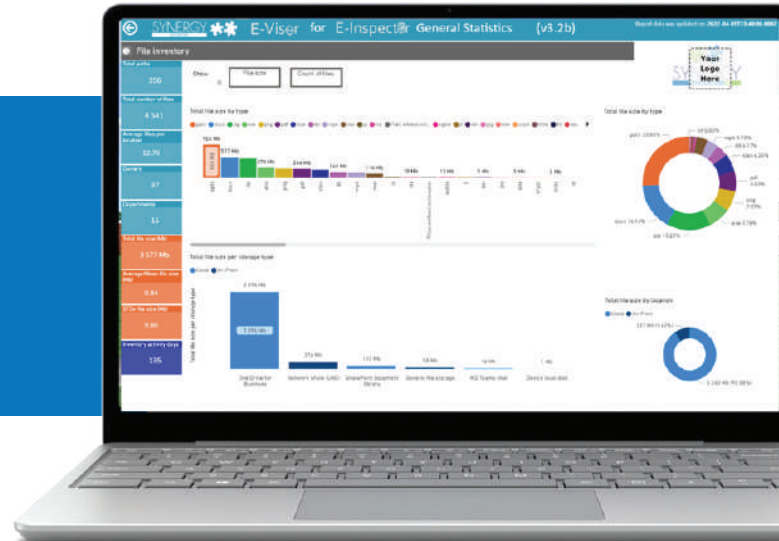
Leveraging the benefits and protection capabilities of Microsoft cloud environments



Take advantage of the document features provided by cloud repositories

Plus!: Power BI experience for detailed and strategic analytics in multiple views

Rich analytics for comprehensive visibility and better decision-making to effectively manage the information across your cloud environments.



About Synergy Advisors

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 baseline
- 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 baseline



Threat Protection

- Users (Internal / external)
- Devices
- Identities
- Endpoints
- Cloud
- Monitoring
- Infrastructure
- Security baseline

Contact us to get a quote for your organization's needs [HERE](#)

E-mail us and get a free consulting session: ww-marketing@synergyadvisors.biz

