E-Inspector

Enterprise automated discovery, audit, and protection of stored sensitive information

SYNERGY ADVISORS

E-Inspector is a proprietary solution from Synergy Advisors that supports advanced data detection and reporting to discover everything you need to know about your file repository, providing inventory and inspection of content both in the cloud and on-premises.

Main features

Audits and enforces security and status classification

Inspect encrypted or un-encrypted files for sensitive content or matches to policy

Search and control data in file repositories, the endpoint, and cloud applications

Notifications and alerts according to compliance policies work together with proactive responses provided by Microsoft flow

Search and control data in file repositories, the endpoint, and cloud applications

Monitoring, alerts, notifications, and auditing of sensitive files

Advanced content, auditory and inspection

=

Security

+

Productivity

Why E-Inspector?

DISCOVERY AND INVENTORY

Find sensitive information by file content, metadata, and more

- Business-driven, efficient, and dynamic inventory
- Discover sensitive files by information type
- ISO, GDPR, and SOX compliant

GRANULARITY

Discover and protect multiple files based on specific data attributes

- Scan by multiple filters such as location, type of information, users, and much more
- Apply Information Protection with flexible, information-driven, strong policies

OPTIMIZATION

Dynamically apply file lifecycle actions

- Bulk copy, move, and delete actions for files, based on multiple parameters
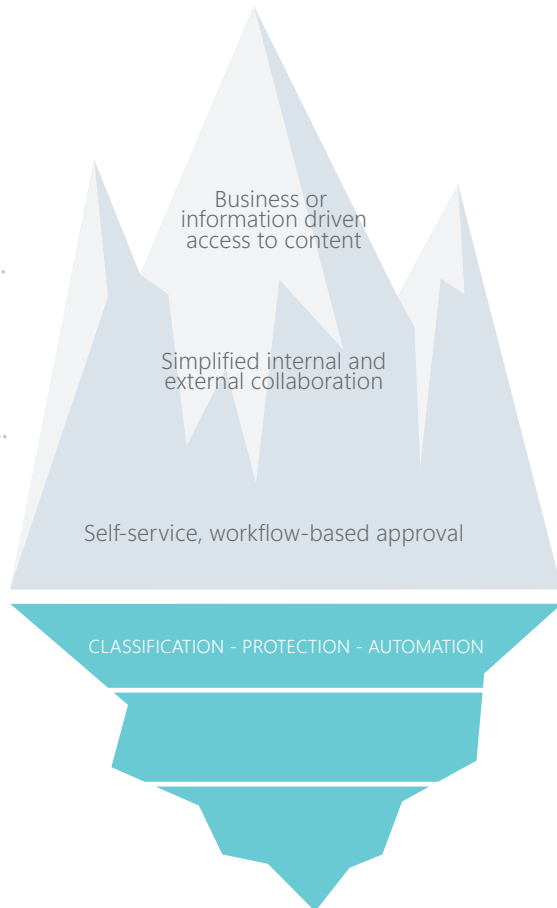- Manage owners, change file permissions, and apply or remove encryption to files

PRODUCTIVITY AND SECURITY
WORKING AS ONE

E-Inspector operating lifecycle

Set Inspection Resources

Select a single server, multiple servers, a cluster, or multiple clusters

Findings, Recommendations, and Monitoring

Optimized operationalized actions

Set Inspection Scope

Multiple locations cloud and on-premises

File Lifecycle

- File relocation: optimization, security and risk mitigation
- Copy: for review
- Delete: compliance / security risk

Set Inspection Criteria

Multiple criteria, location, content, metadata

Information Protection

Apply Information Protection by label, by policy, and more. Support for customized permissions

Reporting & Analitycs

Discover sensitive data, set parameters and customization

E-Inspector implementation

ADOPTION

Fexible policies

Simplified access

Comprehensive Business insights

Business or information driven access to content

Simplified internal and external collaboration

Self-service, workflow-based approval

FOUNDATION

CLASSIFICATION - PROTECTION - AUTOMATION

INFORMATION GOVERNANCE

- Centralized policy inspection definition for both on-premises and cloud
- Rich data inventory
- File metadata
- Location-based context inventory (ACLs)
- Workflow-based actions
- Actions beyond content protection and marking
- Copy, move, delete, archive, etc.
- Reporting and analytics

INFORMATION PROTECTION BASELINE

- Inspection and protection based on file content only
- On-premises * (File server, SP)
- Cloud – O365 Data ** (SPO, OD4B)

What challenges does E-Inspector help you solve?

• Automate discovery, auditing and protection of sensitive information stored by the company

• Search optimization and complete document inventories

• Discover sensitive information by info type, spot duplicated files, and access stale or old files

• Identify stored type of data (e.g., credit card numbers, personal data, etc.), where it is stored, and who is accessing it

• Monitor all SharePoint Online locations from 1 place

• Monitor data in OneDrive and Teams by user, groups and domains (branches)
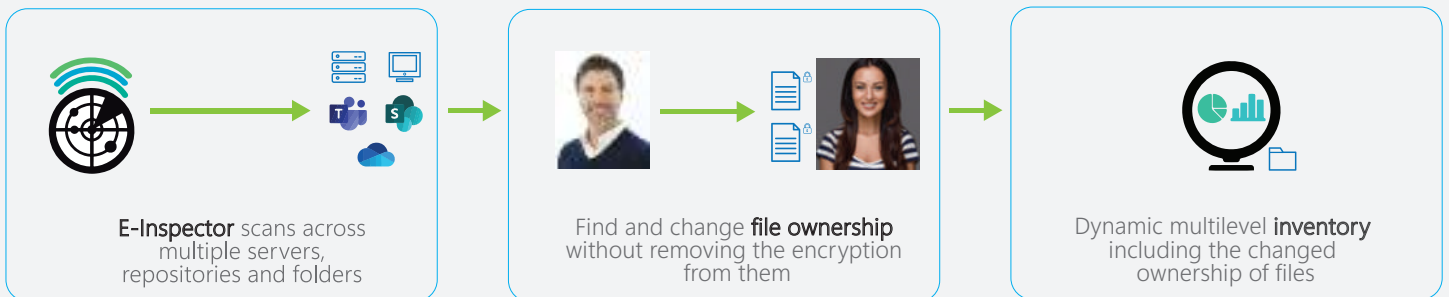
• Understand the types of information stored in speci¬fic repositories (SharePoint Online, SharePoint Server, Teams, OD4B, on-premises, and more.)

• Migrate ¬files to the cloud, excluding speci¬fic data

• Change document permissions when the user is no longer part of the organization

• Encrypt ¬files by data type, department, users and speci-fic location

• Empower users with actions such as moving information to another, migrating data to the cloud, and more

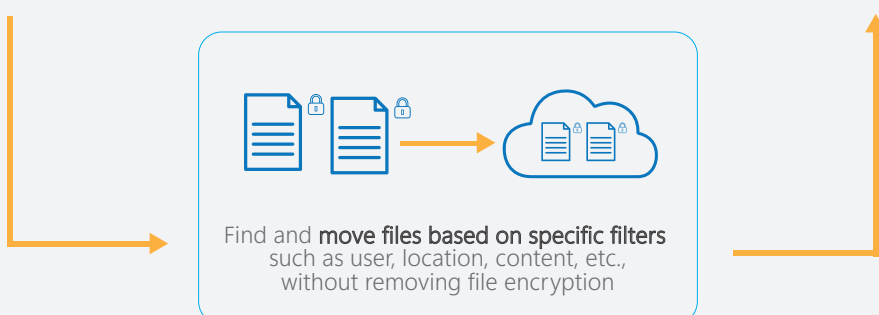• Centralized administration from one single platform

Some use cases

ENCRYPT SENSITIVE INFORMATION

Find and encrypt documents with **sensitive information. Fastest** automated scanning and encryption on the market

CHANGE FILE OWNERS

E-Inspector scans across multiple servers, repositories and folders

Find and change **file ownership** without removing the encryption from them

Dynamic multilevel **inventory** including the changed ownership of files

RELOCATE FILES

Find and **move files based on specific filters** such as user, location, content, etc., without removing file encryption

Plans and scope

AREA	STANDARD	ADVANCED	E-SUITE IP
Information-centric policies Content-based policy [tag/template, content rights, expiration, update, others]	✓	✓	✓
Business-centric policies Policies based on business structures [director, partner, region, group, others]	✓	✓	✓
External collaboration	✓	✓	✓
Workflow approval Workflow-based approval of business roles	✓	✓	✓
Integration with Microsoft Teams E-Inspector Teams App, E-Bot (chatbot) support	✗	✓	✓
Application integration using API Integration of line-of-business applications [LOB] using the E-Inspector API	✗	✓	✓
Integration with SIEM Data exportable to SIEM	✗	✓	✓
E-Viewer Service Analysis and Logging for E-Inspector [E4E]	✗	✓	✓
Advanced E-Vigilant for MIP alerts and notifications	✗	✗	✓
E-Visor **end-user analytics for MIP**	✗	✗	✓
Advanced Data Inspection by E-Inspector	✗	✗	✓

Why choose 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 base line
- Threats
- Data Leak Mitigation

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

Threat Protection
- Users (internal / external)
- Devices
- Identities
- Endpoints
- Cloud
- Monitoring
- Infrastructure
- Security base line

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