



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



### 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, rich 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

### Findings, recommendations, and monitoring

Optimized operationalized action



### Set Inspection resources

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



### Set Inspection Scope

Multiple locations  
Cloud & on-prem



### Set inspection criteria

Multiple criteria  
Location, content, metadata



### File Lifecycle

File Relocation [optimization/security risk mitigation]  
Copy [for review]  
Delete [compliance/security risk]



### Information Protection

Apply information protection  
By label, by policy, and more  
Support for customized permissions



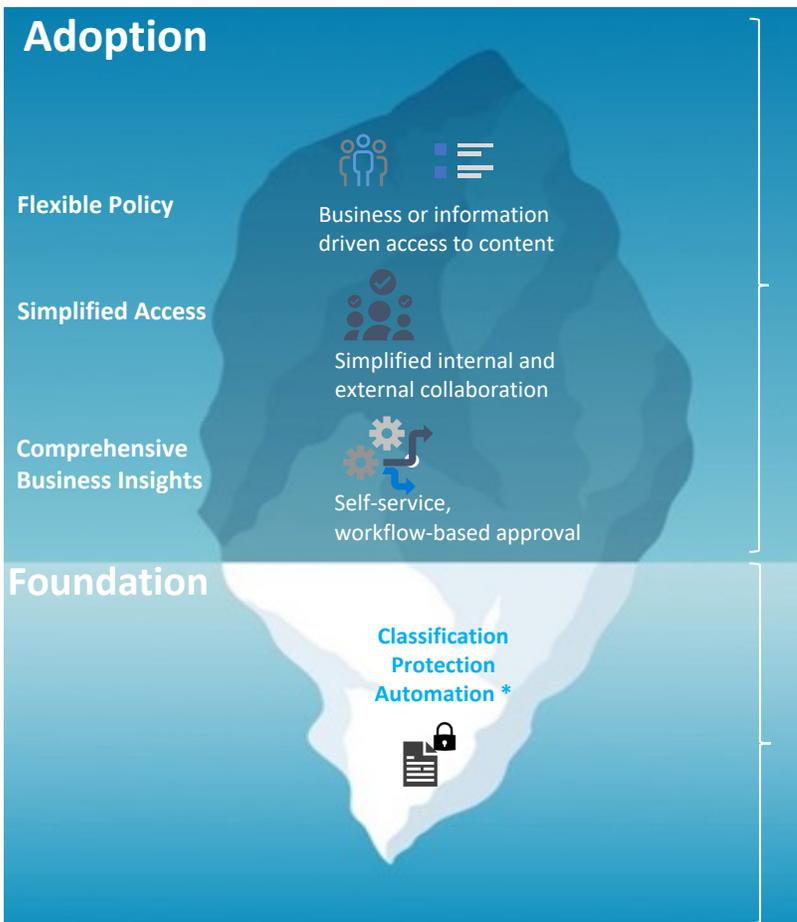
### Reporting & Analytics

Discover sensitive data  
Set parameters and customizations





## E-Inspector implementation Turning over the iceberg



### 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)

## Some of Challenges solved by E-Inspector

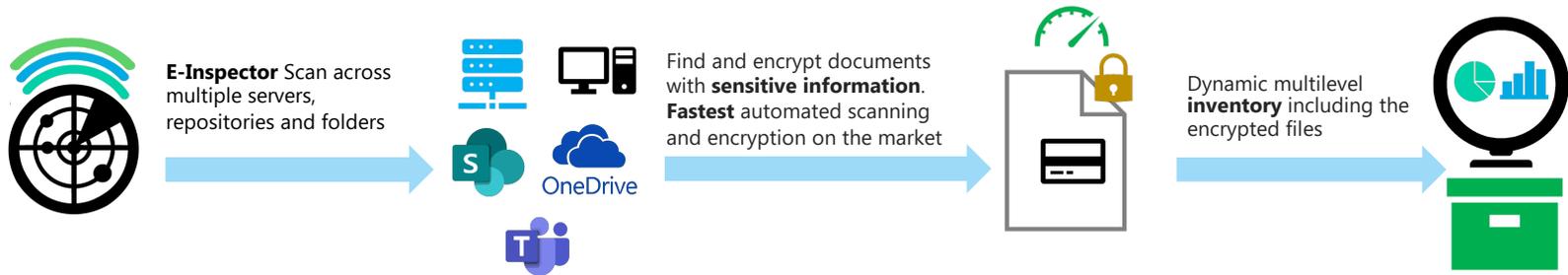
- ? Identify what type of data (e.g., credit card numbers, personal data, etc.), where it is stored and who is accessing it.
- 🔍 Understand the types of information stored in specific repositories (SPO, Teams, OD4B, On-Prem, etc).
- ⬆️ Migrate files to the cloud excluding specific data
- ↔️ Change document permissions when the user is no longer part of the organization
- 🔒 Encrypt files by data type, area, users and specific location



# E-Inspector

## Day-to-day scenarios

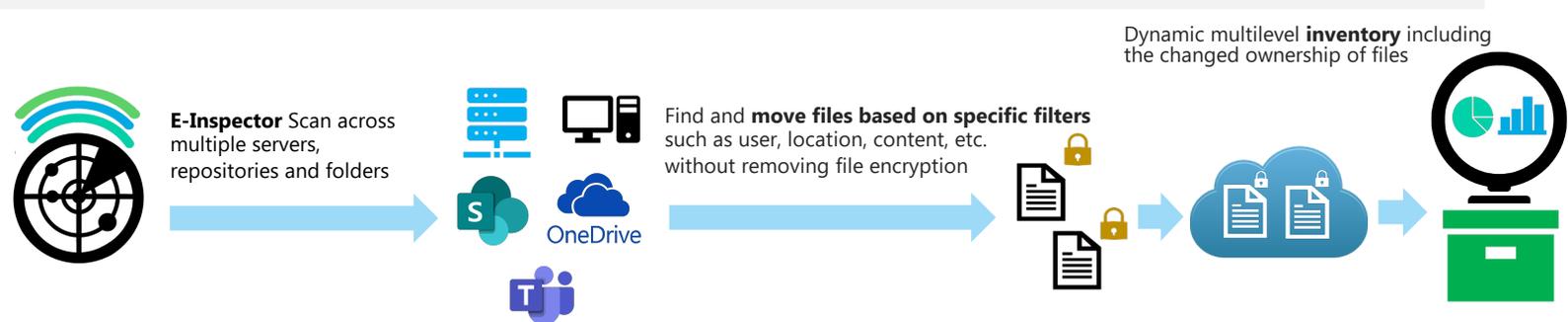
### Encrypt sensitive information



### Change file owners



### Relocate Files



Need more?

Contact Us. Free demo and Training

<https://synergyadvisors.biz/e-inspector>