Enterprise Inspection Tool
E-Inspector

Enterprise-wide discovery, auditing, compliance, and encryption of sensitive information

Becoming ISO, GDPR or SOX compliant has proven to be a never-ending, but vital, task. When handling data, each regulation has its own requirements; having a complete inventory that includes each of those requirements means controlling stale data, old documents, new files and the permissions associated.

Business Driven Data at Rest Protection

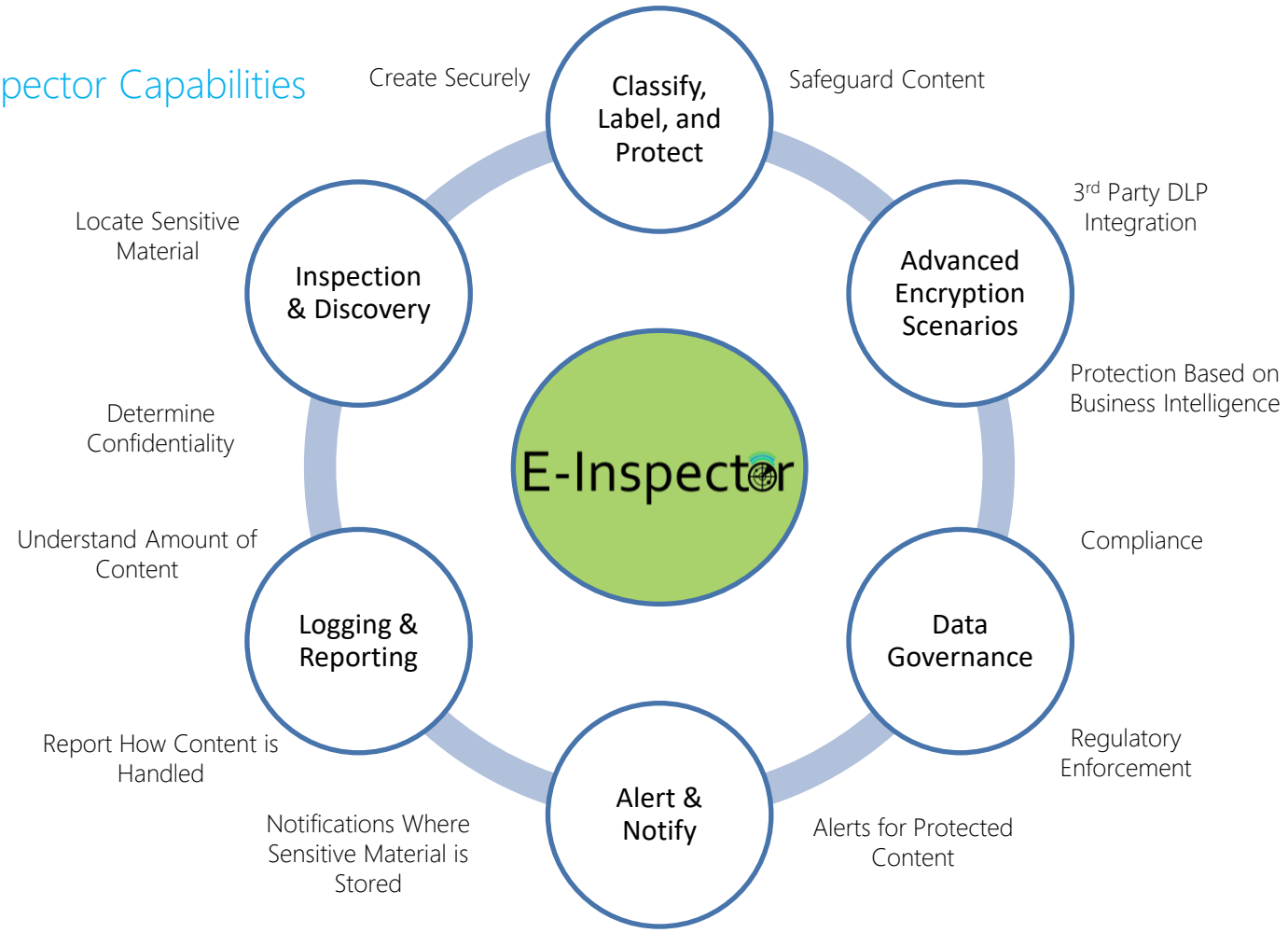
Centralized Inspection for Data Repositories

Monitoring, Alerts, Notifications, and Auditing of Sensitive Files

On-Premises
- ✓ NAS
- ✓ File Servers
- ✓ SharePoint Server

Microsoft Cloud
- ✓ SharePoint
- ✓ Exchange
- ✓ Teams
- ✓ OneDrive
- ✓ Azure
- ✓ MCAS

E-Inspector Capabilities

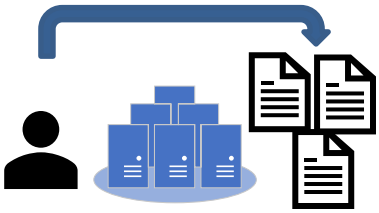


Enterprise Inspection Tool E-Inspector

Information Discovery, Inspection, and Protection

E-Inspector will help with discovery, inspection, and protection of sensitive content

End user uploads/downloads files using a data repository for **content discovery, inspection, and re-location** (Data-at-Rest)



Content inspection is performed **[Data payload / Security Clearance]**

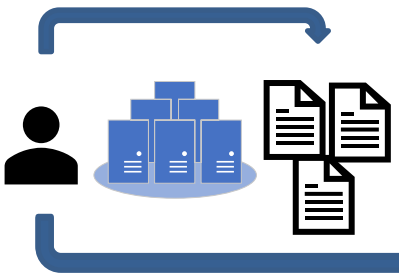
Administrators are now able to **view reports, see logging, and optionally have data relocated** based on policies

E-Visor

Business Rule Context inspection is performed **[User, Role, Clearance, Location, Department, etc.]**

Content is processed and **notifications and alerts can be sent according to compliance**

End user uploads/downloads files using a data repository for **content discovery, inspection, and re-location** (Data-at-Rest) Potential integration with SaaS applications via API



NAS integration with most popular providers*

Microsoft Azure file and/or blob storage also available

Storage blob

Content inspection is performed **[Data payload / Security Clearance]**

Administrators are now able to **view reports, see logging, and optionally have data relocated** based on policies

E-Visor

Business Rule Context inspection is performed **[User, Role, Clearance, Location, Department, etc.]**

Content is processed and **notifications and alerts can be sent according to compliance**

*Integration restrictions apply depending on customer environment

Enterprise Inspection Tool

E-Inspector

Versions

Standard

Scope
- Windows based file servers and shares discovery
- File inventory (including standard file system metadata, access control list for folders and files and file system audit events collection and reporting)
- Content classification and protection based on business rules
- Content ownership enforcement by content potential classification or protection status

Scenario
- Sensitive content location across the organization
- Look for Content based on
  - Path
  - File ACL and Attributes/Metadata
  - Share Folder ACL and Attributes
  - File Content (payload)
  - Existing data classification / RMS Protection

Reports
- Location
- ACLs
- File View
- File Share Service Activity (Windows)

Advanced

Scope
- Integrates with the most popular Network Area Storage (NAS) providers*

Scenario
- Alerts, Notifications using workflows
- Integration with Microsoft Azure IP Scanner
- Integration with Microsoft Azure IP Analytics
- Admin activity monitoring
- Sensitive content and files change notification for content owners and administrators
- Automatic sensitive data retention and relocation enforcement by business rules and policies

Reports
- File Share Service Activity (NAS)
- Data Retention Report

Enterprise

Scope
- Business Intelligence correlation with business via Microsoft AADP
- AADP user activity data integration and correlation
- Elastic content analysis support for large file inspection and analysis loads

Scenario
- Custom third party DLP rules integration
- Look for Content based on
  - DLP Rules

Reports
- All Available Reports (Including users) via E-Visor Advanced for AIP

*Integration restrictions apply depending on customer environment

E-Visor for E-Inspector [E4I] + SIEM