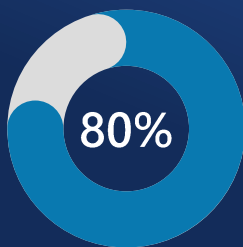


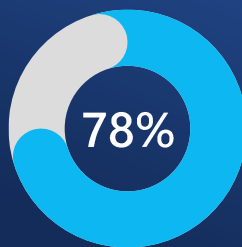
Uncontrolled AI adoption compromises security, privacy, and compliance.

Organizations are rapidly adopting artificial intelligence (AI) tools to boost productivity. However, **the lack of visibility and governance over these technologies creates multiple challenges** that jeopardize data security and regulatory compliance.



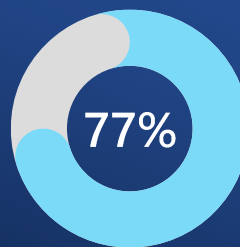
...of leaders cite the leakage of sensitive data as their primary concern.

First Annual Generative AI study: Business Rewards vs. Security Risks, Q3 2023, ISMG.



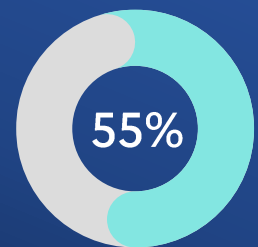
...of users are using AI on their own, without oversight or validation from IT.

2024 Work Trend Index Annual Report, Microsoft and LinkedIn, May 2024.



...of organizations express concern about emerging threats, such as indirect prompt injection attacks.

Gartner Peer Community Poll – Concerns about indirect prompt injection attacks, 2024.

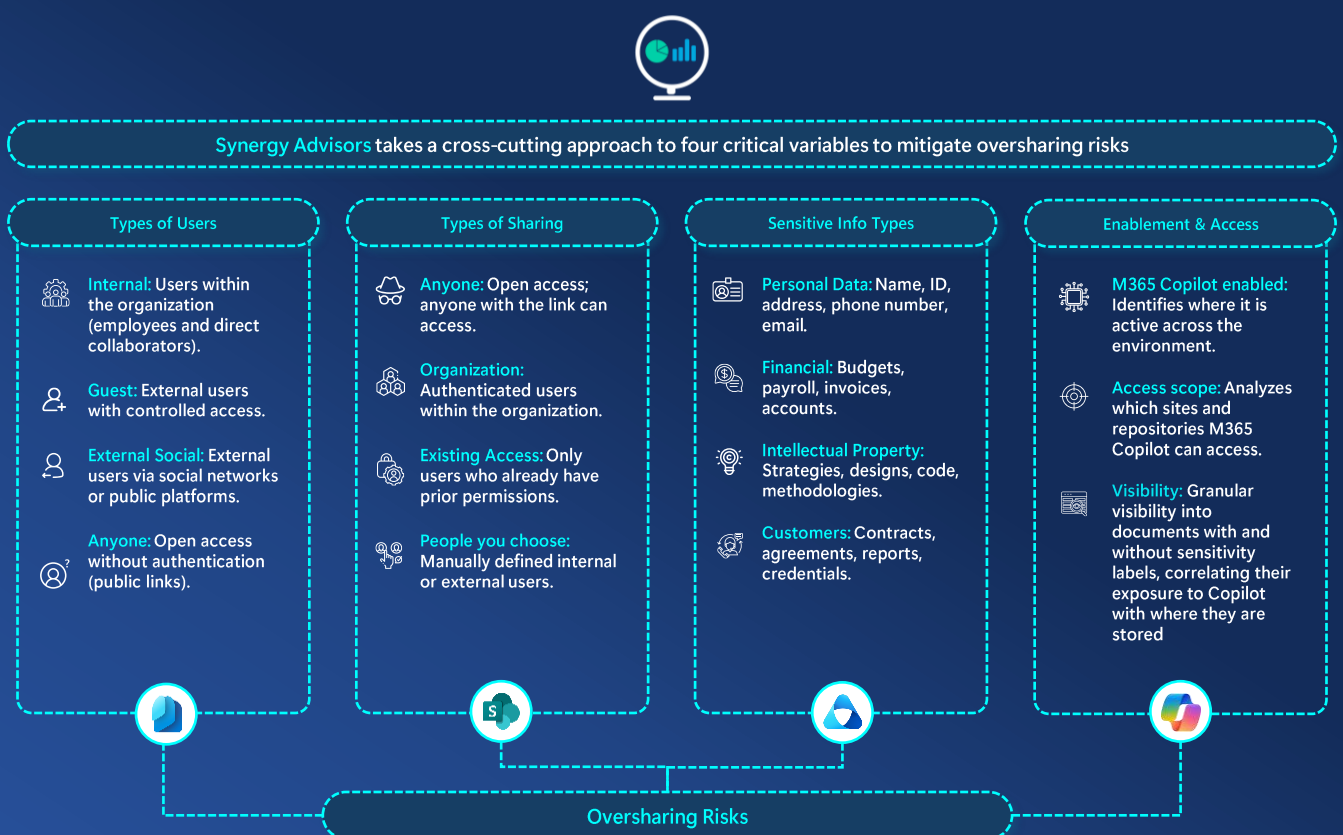


...of leaders do not understand how to regulate AI or how to meet related compliance requirements.

Oversharing: A Structural Risk Exacerbated by AI

Oversharing of information is not a new phenomenon, but **artificial intelligence has amplified its scale and impact**. Many organizations focus solely on the technological risks of AI, overlooking the fact that the root of the problem remains structural and human.

To truly understand the scope of this challenge, it's essential to examine the three components that drive it:



Based on a detailed analysis of the identified challenges and risks, we have developed a comprehensive solution designed to proactively mitigate current threats, aligning with your organization’s strategic objectives in information protection, regulatory compliance, and productivity:

Intelligent Insights & Governance for Your M365 Data Landscape

E-Visor is an analytics and visualization platform built to enhance data protection, governance, and AI-driven insights across Microsoft 365. It leverages Microsoft Purview and M365 capabilities to deliver clear visibility into sensitive data, usage patterns, lifecycle events, and potential exposure risks.

Designed to support informed decisions, it helps strengthen governance, reduce risk, and improve the organization’s overall security posture.



Right-Sized Visibility and Governance for Microsoft 365

E-Visor is available in three versions, each offering increasing levels of visibility, governance analytics, and AI-powered capabilities. This structure enables organizations to adopt the version that best aligns with their risk, compliance, and operational maturity goals:

Solution	Description	Key Capabilities (Insights)
E-Visor for M365 Data Sensitivity & AI Insights	Deep visibility into sensitive data and AI exposure across Microsoft 365 to support secure Copilot adoption.	• Purview Information Protection (Labels, SITs) • SharePoint Online • OneDrive for Business • Microsoft 365 Copilot • Microsoft Entra
E-Visor for Advanced M365 Data Sensitivity, Governance & AI Insights	Full and comprehensive visibility of governance for sensitive data, retention, and AI-driven compliance scenarios in Microsoft 365.	• Purview Information Protection (Labels, SITs, EDM, Trainable Classifiers) • Purview Data Lifecycle • Records Management • SharePoint Online • OneDrive for Business • Microsoft 365 Copilot • Microsoft Entra
E-Visor for M365 Data Governance & AI Insights	General data governance and lifecycle management with AI insights to strengthen compliance across Microsoft 365.	• Purview Data Lifecycle (Retention) • Records Management • SharePoint Online • OneDrive for Business • Microsoft 365 Copilot • Microsoft Entra

Thanks to its advanced capabilities, our solution serves as a strategic enabler to strengthen information governance and proactively mitigate operational risks:



Centralized Risk Visibility: Detects sensitive information in exposed files and consolidates insights into a single view.



Accelerated Regulatory Compliance: Reflects the use of labels, encryption, and key policies to visualize the current state of your unstructured data.

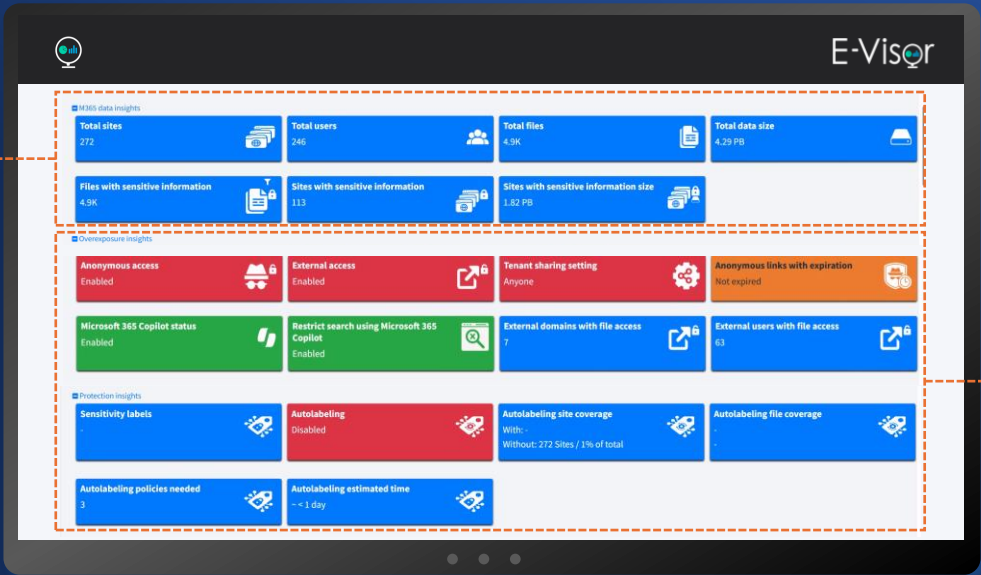


Data-Driven Decision-Making: Reports and dashboards that prioritize actions based on real evidence.



Security Policy Optimization: Assesses the configuration of the services where your data is stored to strengthen the security posture.

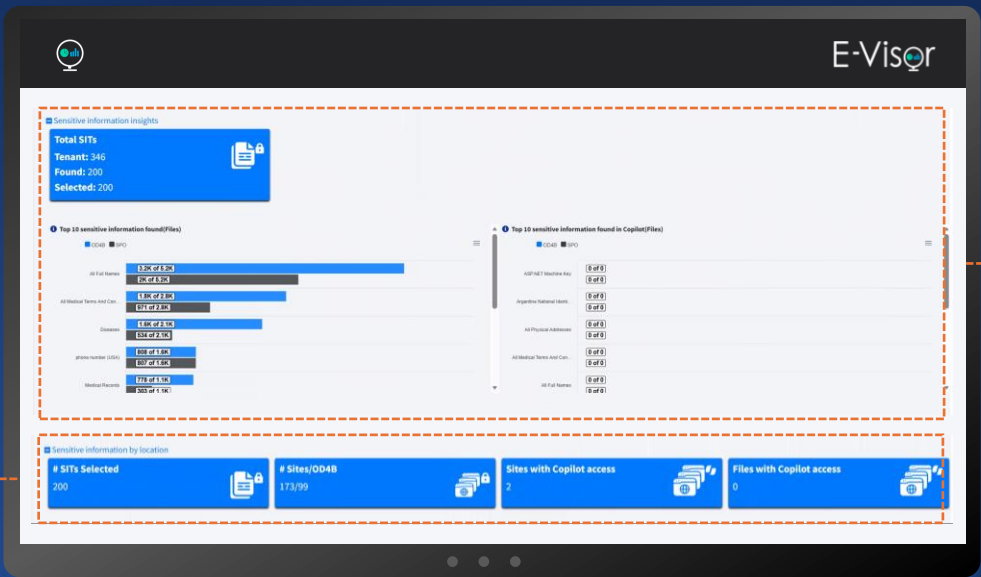
M365 Data, Overexposure, & Protection Insights



Shows total sites, users, files, and data size in your M365 environment, plus identifies where sensitive information resides in files and sites. Enables a complete view of data volume and critical locations.

Provides visibility into sharing configurations and external access while highlighting sensitivity label and auto-labeling status to assess exposure, protection, and automation readiness.

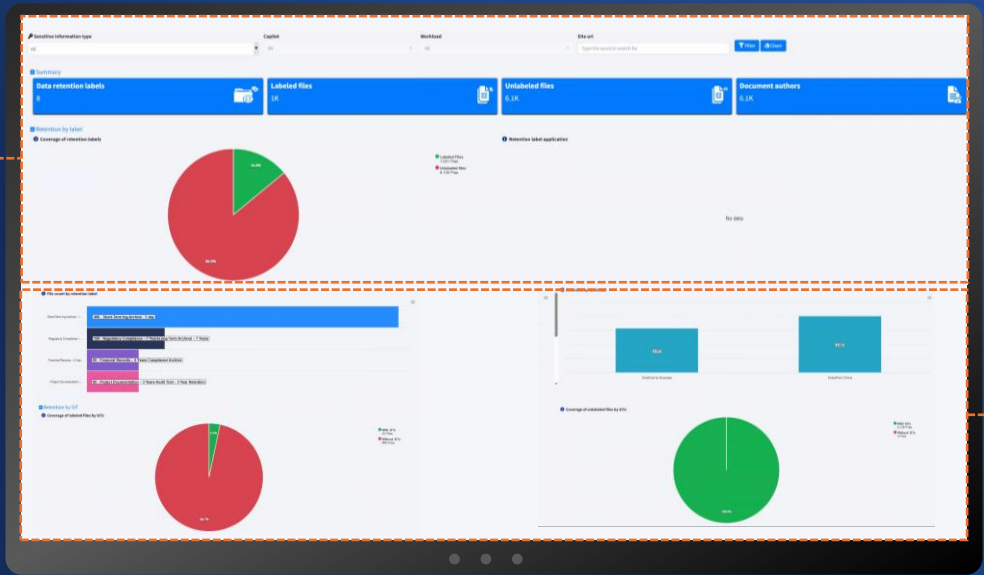
Sensitive Information Insights



Displays selected sites, data volume, and sites or files with Copilot access. Provides a quick view of where sensitive data is and its exposure level.

Shows total sites analyzed, plus top 10 sensitive data types found in files and in files accessible by Copilot. Helps identify critical data and AI exposure.

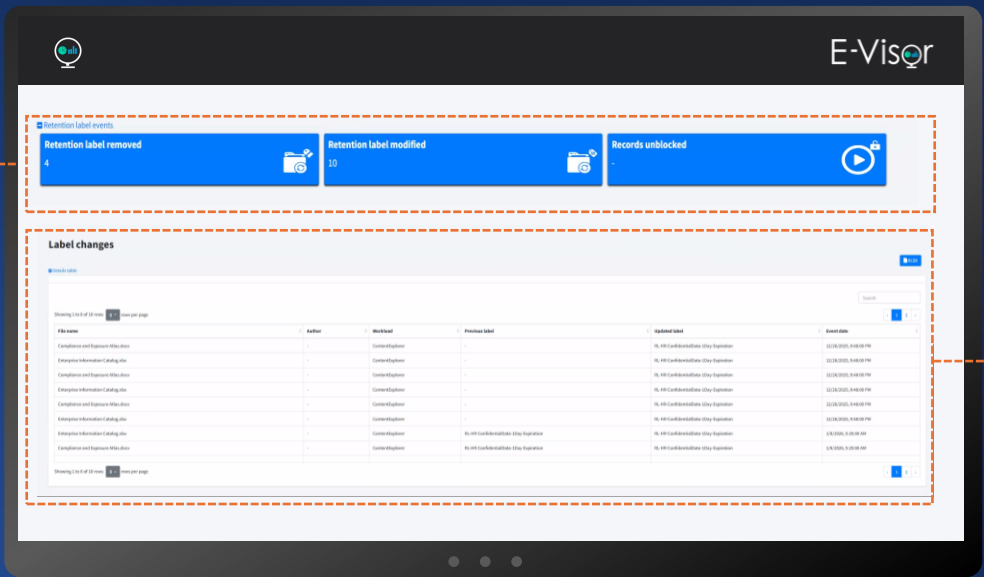
Data Retention and Classification Overview



High-level view of retention label adoption, showing how many files have retention policies compared to those that remain unlabeled.

Detailed breakdown of retention labels, file distribution, and author activity to identify usage patterns and compliance gaps.

Retention Label Activity and Change Log

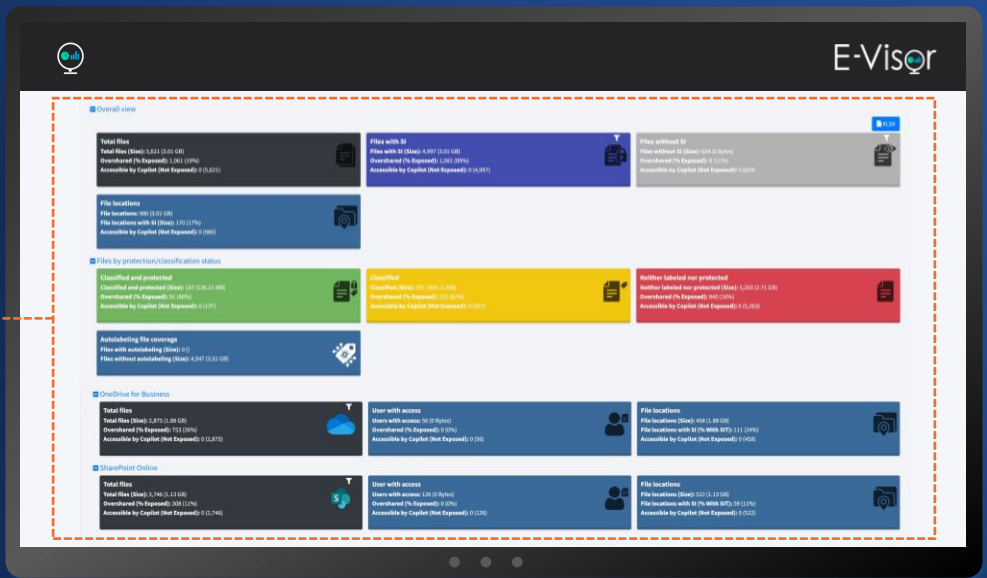


Summary of key retention-related events, including labels removed, labels modified, and records unlocked, providing a quick view of recent policy-impacting actions.

Detailed log of label changes, showing who modified each item, the workload involved, and the previous vs. updated retention labels for auditing and compliance tracking.

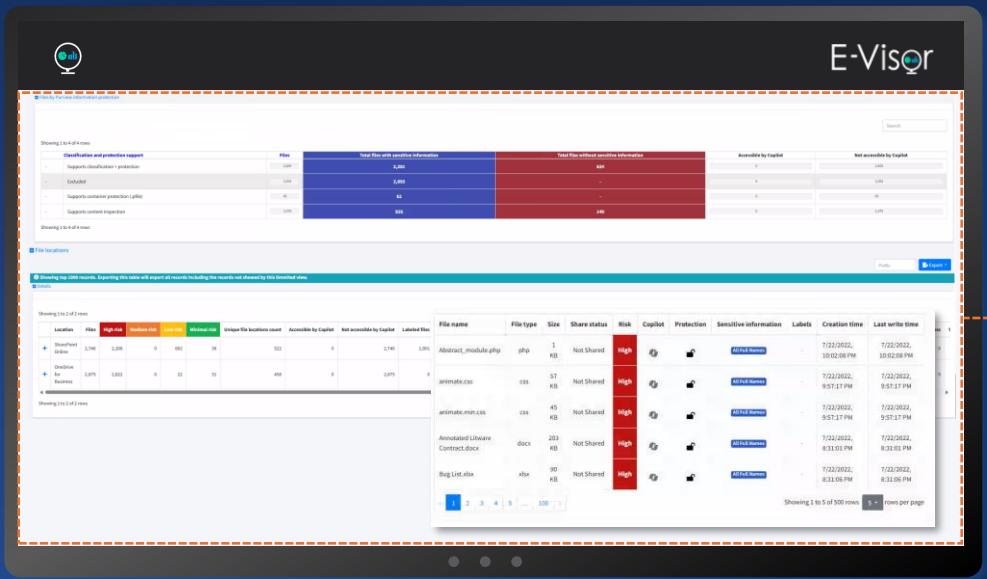
E-Visor – Detail Tab

Overview of content and protection and classification status



Provides a consolidated overview of the organization's file inventory across **OneDrive** and **SharePoint**, highlighting total file volumes, storage distribution, sensitivity coverage, classification status, and access metrics. It helps identify how information is stored, protected, labeled, and accessed, offering a clear understanding of overall data governance posture.

File Risk, Sensitivity, and Protection Analysis



Provides a consolidated assessment of files containing sensitive information, highlighting risk levels, protection status, labeling coverage, and accessibility. It also includes a detailed file-level table that surfaces critical attributes such as risk classification, sensitivity indicators, applied protections, and key activity timestamps, enabling efficient review and prioritization of high-risk items.

Risk Assessment Model for Information Security

At **Synergy Advisors**, we use a structured risk classification model to analyze file exposure in collaborative environments. This methodology allows us to identify critical scenarios that compromise information security.

Risk Scale	Color	Sensitive Information	Protection(Label + Encryption)	High Exposition	Description
3 – High	Red	Yes	No	Yes	The file contains sensitive information without protection and/or is widely shared.
2 – Medium	Orange	No	No	Yes	It does not contain sensitive information, but it is widely shared.
1 – Low	Yellow	No	No	No (limited)	It does not contain sensitive information and is shared with few users.
0 – Minimum	Green	Yes / No	Yes / No	Anyone	It does not contain sensitive data, or it is properly protected.

Based on this classification, we identify security gaps, prioritize corrective actions, and facilitate more efficient decision-making aligned with compliance and data protection objectives.



Get E-Visor from the Microsoft Azure Marketplace

E-Visor is available in the Microsoft Azure Marketplace. Deploy the solution quickly and securely within the Microsoft ecosystem, using your existing procurement processes to accelerate adoption across your Microsoft 365 data landscape, without added friction or complexity.

- Access E-Visor through Azure Marketplace and manage the solution centrally within your Microsoft environment.
- Rely on guidance from our team throughout the entire journey, from acquisition to implementation and go-live.



Why choose Synergy Advisors as your strategic partner?

Adopting a solution like **E-Visor** goes beyond automating reports or visualizing files: it represents a strategic approach to proactively managing sensitive data exposure, aligning information security with compliance, governance, and operational efficiency objectives.

E-Visor acts as an enabler, bridging technical data and business decisions by providing accurate visibility into configurations, access, and file classification. It enables you to identify critical gaps, prioritize corrective actions, and transform data monitoring into a sustainable competitive advantage.

		
Consulting Services	Managed Services	E-Suite
Over 15 years of experience working with hundreds of clients and thousands of users in market-leading organizations across various verticals, specializing in Security and Compliance, Modern Work, Azure Data and AI, and Azure Infrastructure. • Designing and implementing Microsoft solutions. • Focused on usability and protection to drive upsell and adoption in key use cases. • Integrated approach, creating synergies among Microsoft products.	Experts in cybersecurity, infrastructure, and Modern Work in Microsoft 365, Azure, and Windows 365. • Proactive and reactive services. • Continuous monitoring, optimization, and evaluation of new services and features. • Collaboration with other vendors, providing a single point of contact. • Support contracts available for escalation with native providers	<u>E-Suite:</u> Seamless integration with Microsoft 365 and Azure. Amplifies the features and reach of Microsoft workloads to address modern business, governance, and operational needs by leveraging analytics, workflows, and self-service; empowered end users through • Micro-Visor • E-Visor • E-Visor Teams App • E-Inspector • E-Cryptor • E-Vigilant • E-Migrator



For more information, please feel free to contact us at: e-visorforoversharing@synergyadvisors.biz