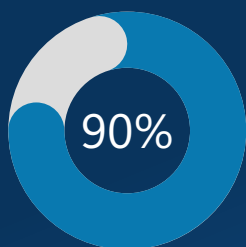
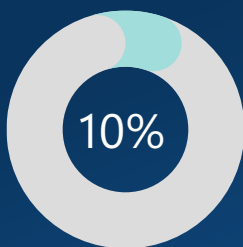


Internal and external collaboration across business units and organizations is essential to driving productivity and achieving results. In today's dynamic workplace, the exchange of critical information with external partners cannot be limited — but it must be enabled securely and efficiently. However, unstructured data and uncontrolled file sharing often lead to a lack of visibility into who accesses the information, how it is used, and under what permissions. This challenges collaboration, slows down processes, and increases operational and reputational risks.



...of organizations have **sensitive data in the cloud exposed without access controls**, allowing unauthorized users or AI tools to view or manipulate it.

[2025 State of Data Security Report, Varonis.](#)

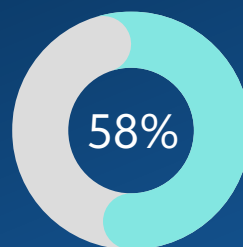


...of user or service accounts have privileges to **freely export sensitive information**, without any restrictions or oversight.



...of organizations have **sensitive data directly exposed to AI tools**, drastically expanding the attack surface and the likelihood of a data breach.

[2025 Control Third-Party Risk, SafePaaS.](#)

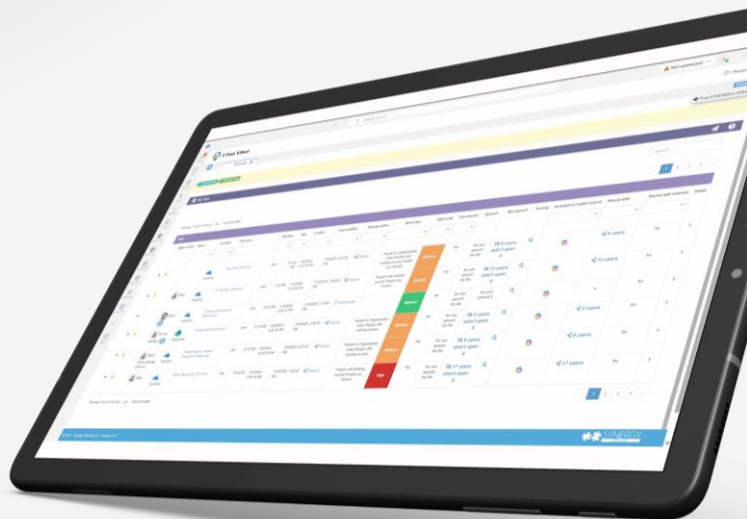


...of organizations have experienced security incidents related to **access by external users** such as customers, partners, or temporary collaborators.

Empowering users and organizations with the visibility needed to enable secure and responsible collaboration

Micro-Visor (Modern Work) provides both end users and administrators with a centralized, intelligent view of file sharing activity across Microsoft 365 — natively integrated into Microsoft Teams, where collaboration truly happens.

Designed for end users and business units such as support, IT, compliance, and security, Micro-Visor connects activity and access with risk exposure and file-level insights across Microsoft 365 data-at-rest repositories — all without disrupting productivity or team workflows.



Effective content sharing requires more than IT-defined access — it requires user empowerment, real-time insight, and simplified decision-making:

Alerts and Notifications

Deliver real-time alerts through Microsoft Teams mentions and chat messages — not more emails — to inform users of collaboration risks between internal and external participants, considering access type, data sensitivity, and sharing settings.



User Education

Provide intuitive, color-coded risk indicators and access logs to help users understand the implications of their sharing actions — including access type, file content, AI access, and encryption — enabling responsible decision-making.



Self-Service

Enable users to stop or modify sharing settings directly within Teams across SharePoint, OneDrive, and Teams workspaces — aligning with organizational policies while minimizing dependency on support teams.



Reduced Operational Costs

Simplified visibility and control empower users to resolve oversharing issues proactively, reducing incident response times and easing the burden on IT, compliance, and security teams.



Many organizations focus on the technological risks, overlooking the structural and human factors at the core of the problem. In the context of secure collaboration, addressing oversharing requires more than just technical controls — it demands a deeper understanding of how people work, communicate, and interact with information across the organization. To truly grasp the challenge, let us examine the three key components that drive it:



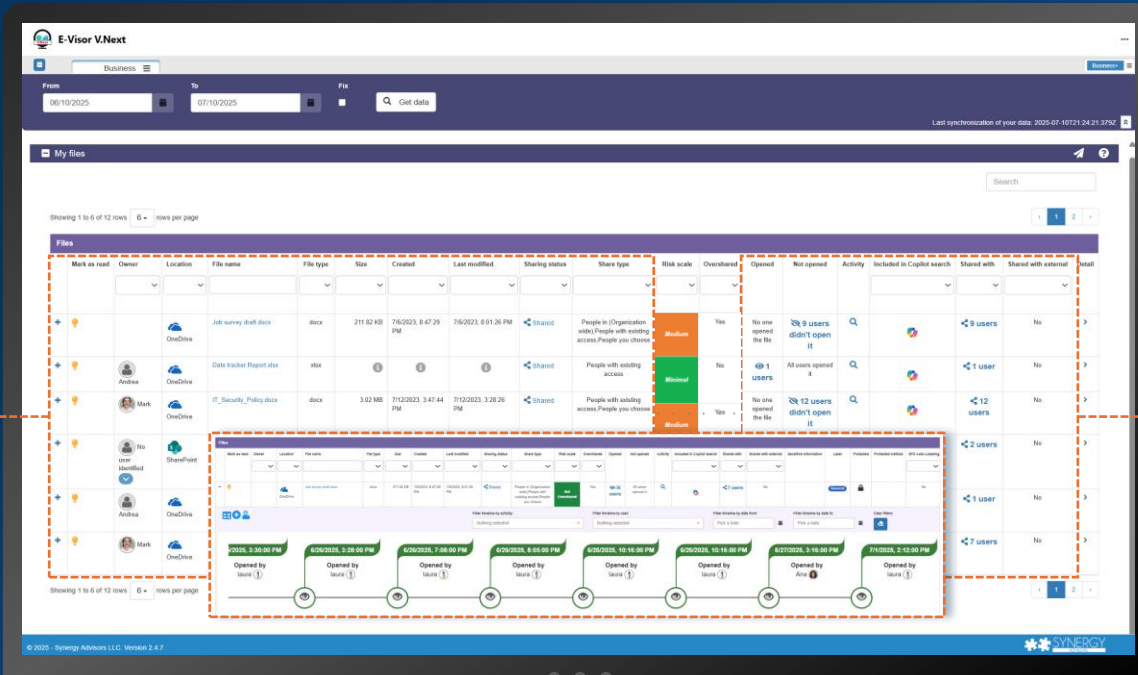
Synergy Advisors Oversharing Risk Framework: An end-to-end perspective backed by decades of expertise in data protection and collaboration

At **Synergy Advisors**, we apply a structured risk classification model to assess file exposure in collaborative environments. This methodology enables us to identify critical scenarios that compromise information security and take proactive steps to mitigate them.

Risk Scale	Color	Sensitive Information	Protection (Label + Encryption)	High Exposure	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	The file does not contain sensitive information, but it is widely shared.
1 – Low	Yellow	No	No	No (limited)	The file does not contain sensitive information and is shared with few users.
0 – Minimum	Green	Yes / No	Yes / No	Anyone	The file does not contain sensitive data, or it is properly protected.

Enables Truly Secure and Productive Collaboration through Modern Work

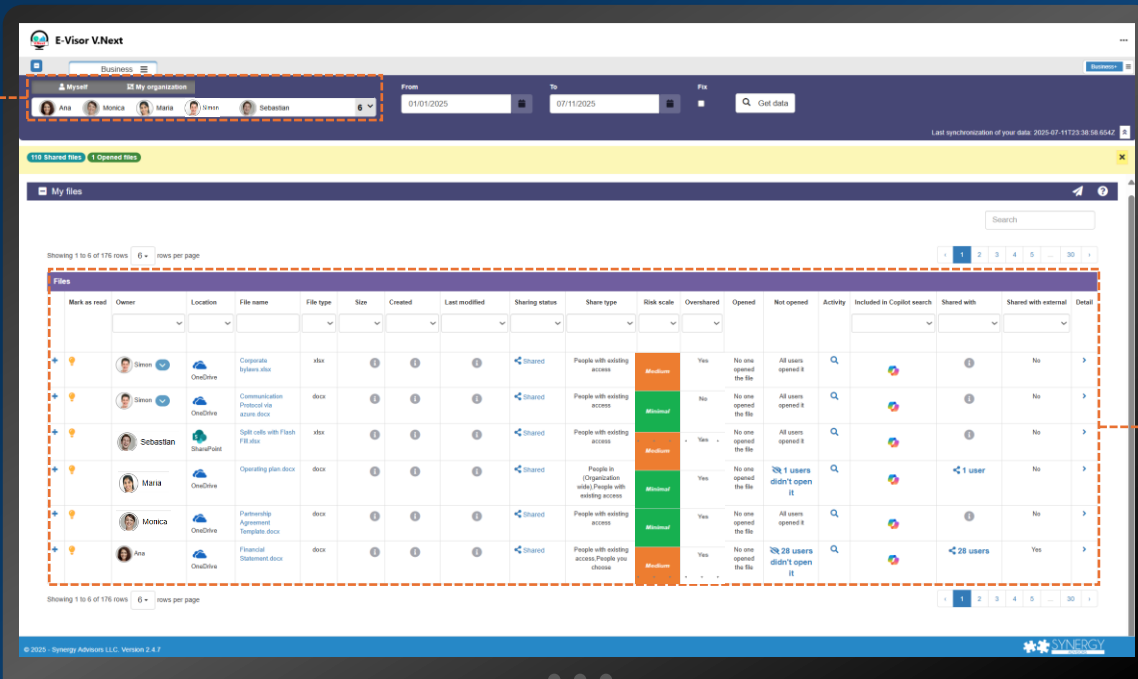
Personal Document Management and Tracking



Enable users to view and manage all the files they have interacted with across multiple workloads in Microsoft 365 — including detailed information about each file, sharing status, and sharing type — to measure the level of access granted internally and externally.

View user activity across all individuals with access to your documents, highlighting who has or has not accessed the files, edited them, downloaded copies, and more — all through a detailed activity history. Users can also understand whether AI technologies have access to summarize or extract information for advanced collaboration purposes.

Centralized view of file activity across the organization



Extend access to an enhanced version of the application for support, monitoring, and collaboration auditing teams, enabling visibility tailored to different business areas such as location, region, or department. Gain insights through user collections within your organization—simply select user groups or specific segments to understand how they collaborate and manage their files.

Optimize, Protect, and Scale: The real value of Micro-Visor

Micro-Visor (Modern Work) is more than just a monitoring tool—it is a strategic solution that transforms how organizations manage secure collaboration. Regardless of your AI adoption stage, Micro-Visor provides peace of mind and tangible risk controls that every user and organization can benefit.

By providing clear visibility into file exposure and enabling users to take informed action, Micro-Visor helps reduce risk, strengthen information protection, and foster a culture of secure, efficient teamwork. With Micro-Visor, collaboration becomes a controlled advantage, not a vulnerability.



Why choose Synergy Advisors as your strategic partner?

At **Synergy Advisors**, we provide specialized consulting and managed services to help your organization modernize its collaboration strategy. Our Micro-Visor solution delivers centralized visibility, intelligent insights, and automation to reduce the risks of oversharing and enable more effective teamwork.

We go beyond technology by working closely with your teams to drive adoption, simplify collaboration workflows, and support secure, scalable productivity. With **Micro-Visor (Modern Work)**, your organization gains the clarity and control needed to protect valuable information—without compromising agility or collaboration.

If you would like to learn more or explore additional Micro-Visor capabilities, [click here](#).



Consulting Services

Over 14 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.



Managed Services

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



E-Suite

E-Suite: 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, feel free to contact us
at: micro-visor@synergyadvisors.biz

[Learn more](#)