

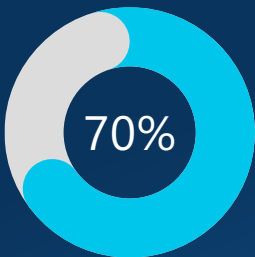
INTRODUCING

Micro-Visor



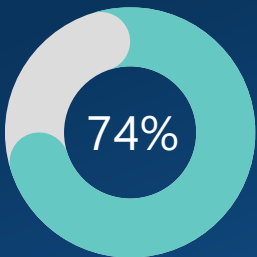
Empower your teams with unified, intelligent, and secure operations

In modern organizations, fragmented digital operations across multiple platforms create silos that reduce efficiency and responsiveness. This lack of integration leads to delays, misaligned processes, and increased operational risks—hindering productivity and strategic alignment.

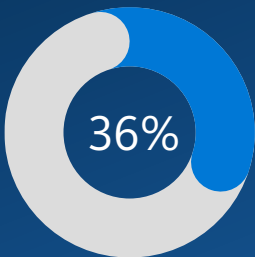


...of employees spend over 20 hours per week searching for information across disconnected systems, resulting in major productivity losses and hidden operational costs.

[IDC, "The State of the Digital Workplace," 2023.](#)

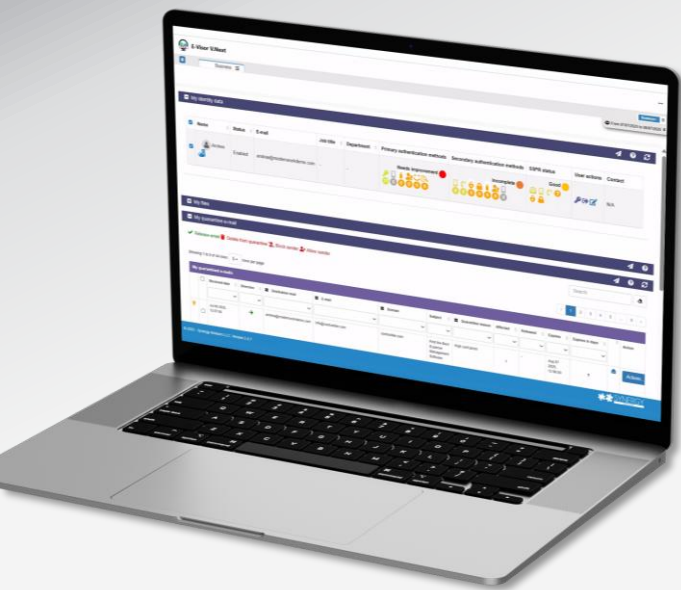


...of companies operate within fragmented technology ecosystems, directly impacting operational efficiency and slowing down decision-making processes.



...of cybersecurity professionals report that their current toolsets are overly complex and time-consuming to manage, which slows response times and increases operational risk.

[Sophos, "Cybersecurity teams are wasting time, money and effort dealing with tool sprawl and multi-vendor ecosystems," 2023](#)



Introducing Micro-Visor: Seamless integration of security and productivity

Micro-Visor is a solution developed by Synergy Advisors that centralizes identity, collaboration, security, and compliance management within Microsoft Teams, enabling users to operate in a visual, intuitive, and secure way.

Micro-Visor empowers both end users and administrators with self-service tools, granular visibility into data and risks across different areas, and contextual education — all without leaving the Teams environment.

Maximizing Operational Impact Through Intelligent, User-Centric Experiences

Our solution redefines how organizations interact with their digital environment by placing control, visibility, and agility directly in the hands of end users. By streamlining processes, reducing friction, and enabling smarter decision-making, the solution generates measurable impact across the organization. The following capabilities illustrate how Micro-Visor enhances the overall digital experience while supporting a more proactive, efficient, and scalable operation:

Alerts and Notifications

Receive alerts and notifications about key activities within the digital environment, enabling continuous monitoring and proactive responses to relevant organizational events.



User Education

Promote efficient and secure use of technological tools, encouraging best practices that enhance security, compliance, and productivity.



Self-Service

Empower users to manage configurations and respond to events independently, enhancing productivity and the overall digital experience.



Reduced Operational Costs

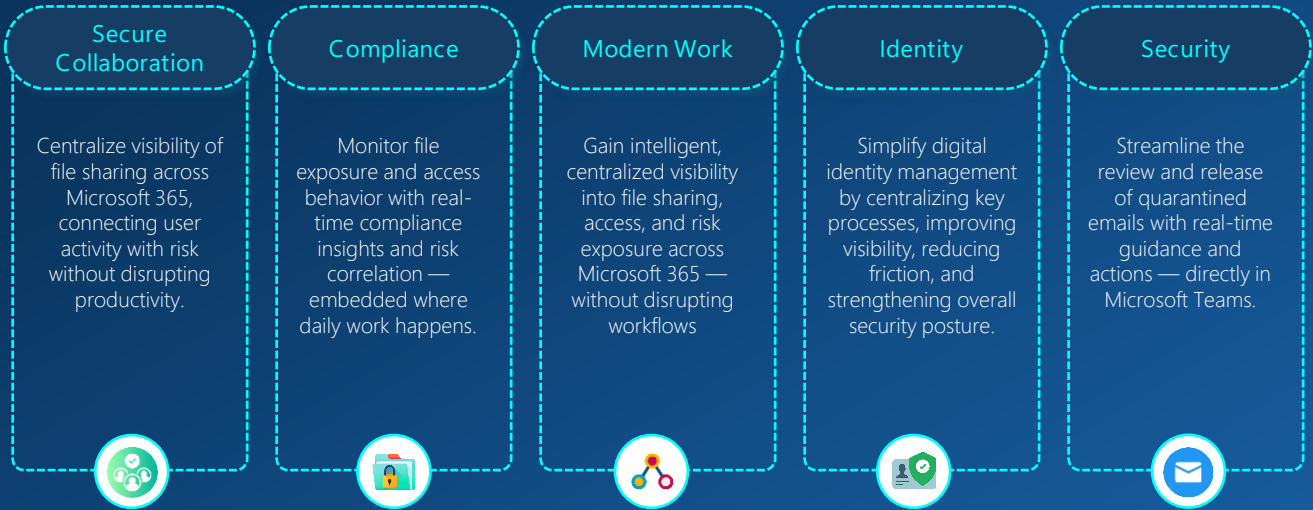
Optimize technological resources by reducing the need for technical support and improving operational efficiency, contributing to a more strategic IT management.



To address the operational, regulatory, and security needs of modern organizations, Micro-Visor is structured around five key capabilities that work together within Microsoft Teams. These capabilities connect business processes with collaboration tools, strengthen regulatory compliance, protect digital assets, and enhance the experience of both end users and administrators — all within a unified, intelligent, and adaptable environment.

Micro-Visor

Centralize your digital operations with intelligence, control, and security



Introducing Micro-Visor (Secure Collaboration)

Micro-Visor (Secure Collaboration) empowers both end users and administrators by providing a centralized, intelligent view of file sharing activity across Microsoft 365 — with a native experience in Microsoft Teams, right where collaboration happens.

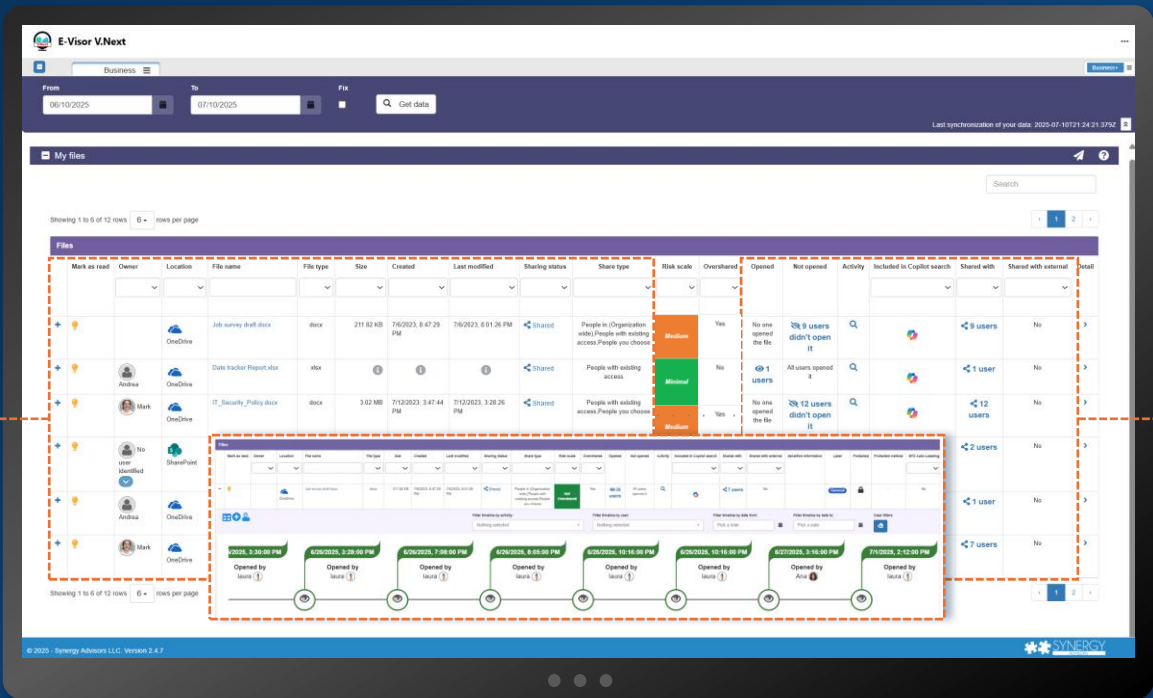
Built for end users and multiple business units — such as support, IT, compliance, and security teams — it seamlessly integrates user activity and access with risk exposure and data for every single active file across the user's Microsoft 365 data-at-rest repositories, providing the necessary guidance — all without interrupting productivity or team workflows.

Effectively managing shared content requires more than just access settings configured by IT — it demands end-user visibility into potential risks, crisp and clear guidance, reduced operational load, and real-time traceability:



Micro-Visor Enables Truly Secure Collaboration through Modern Work and Compliance — Better Together

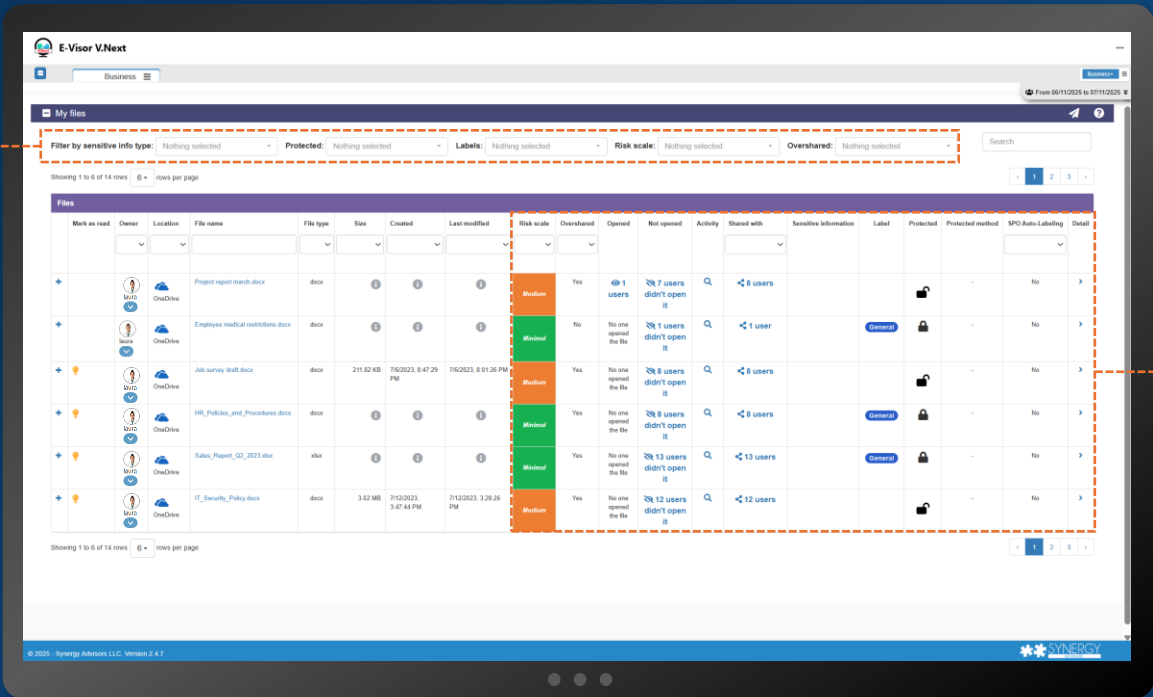
Personal Document Management and Tracking (Modern Work)



Allows 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.

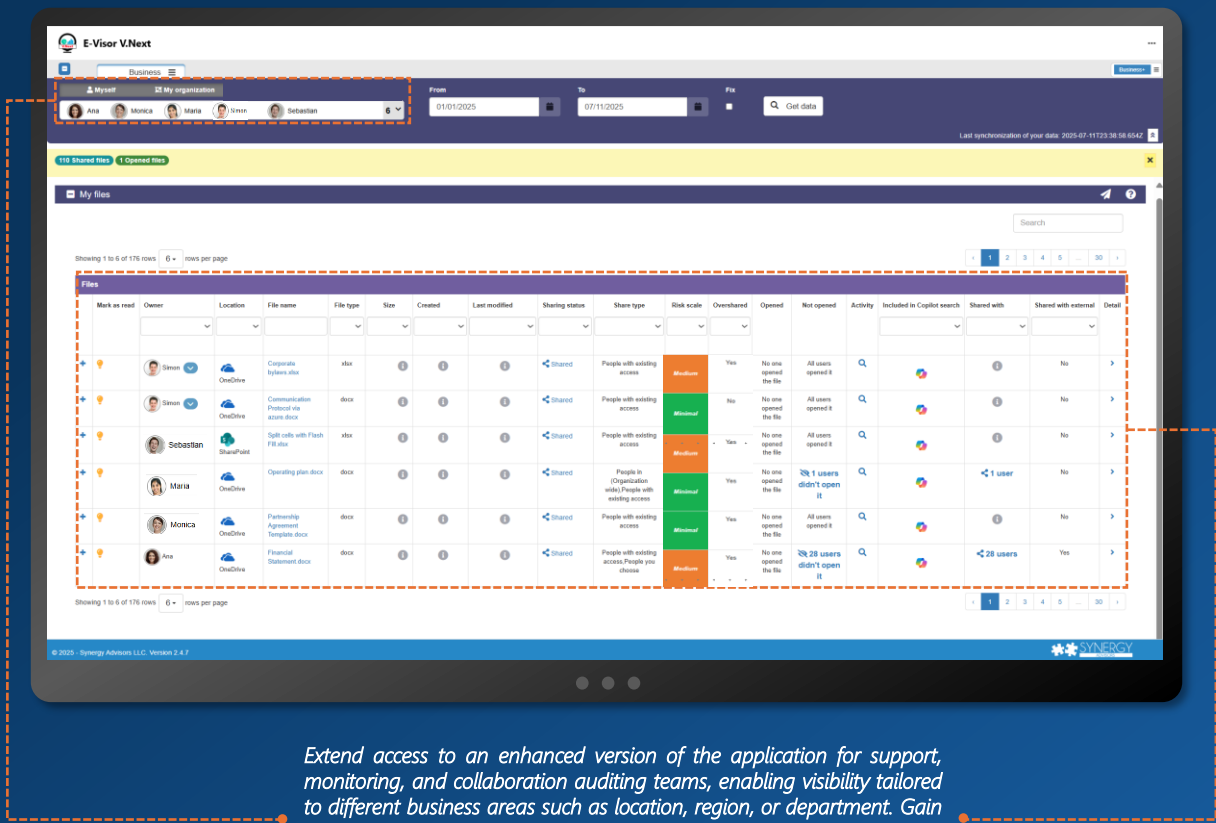
View user activity across all individuals with access to your documents, highlighting who has or hasn't accessed the files, edited them, downloaded copies, among other actions — all through a detailed activity history. Users can also understand whether AI technologies have access to summarize or extract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

Comprehensive visibility into document security and compliance posture



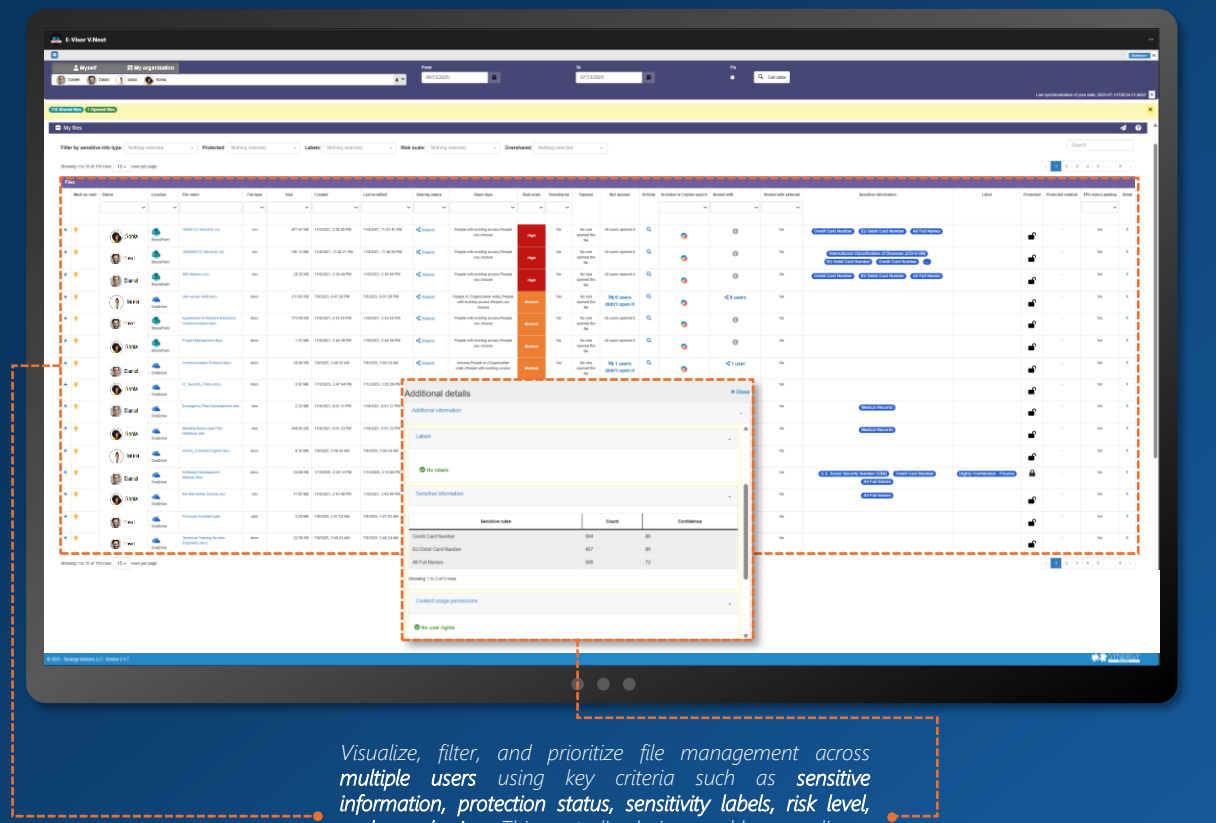
Visualize, filter, and prioritize your files with precision using key criteria such as **sensitive information**, **protection status**, **sensitivity labels**, **risk level**, and **oversharing**. Make informed decisions and focus your efforts where they truly matter.

Centralized view of file activity across the organization
(Modern Work)



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.

Compliance monitoring and data risk management at the organizational level



Visualize, filter, and prioritize file management across multiple users using key criteria such as sensitive information, protection status, sensitivity labels, risk level, and oversharing. This centralized view enables compliance teams to make informed decisions and focus their efforts where it matters most.

Micro-Visor (Compliance) empowers both end users and administrators with a centralized and intelligent view of file exposure and access across Microsoft 365 — natively embedded in Microsoft Teams, right where daily activity occurs. Designed for compliance, security, IT, and risk teams, it correlates user behavior and file access with risk indicators and sensitive data, giving complete oversight across data-at-rest repositories. Micro-Visor delivers real-time guidance to reduce compliance violations and data misuse — all without disrupting productivity or team workflows.

The diagram consists of four rounded rectangular boxes arranged horizontally, each with a dashed border and a light blue background. Each box contains a title, a descriptive paragraph, and a circular icon at the bottom. The icons are: a bell for Alerts and Notifications, a person for User Education, a hand pointing at a screen for Self-Service, and a stack of coins with a dollar sign for Reduced Operational Costs.

- Alerts and Notifications**

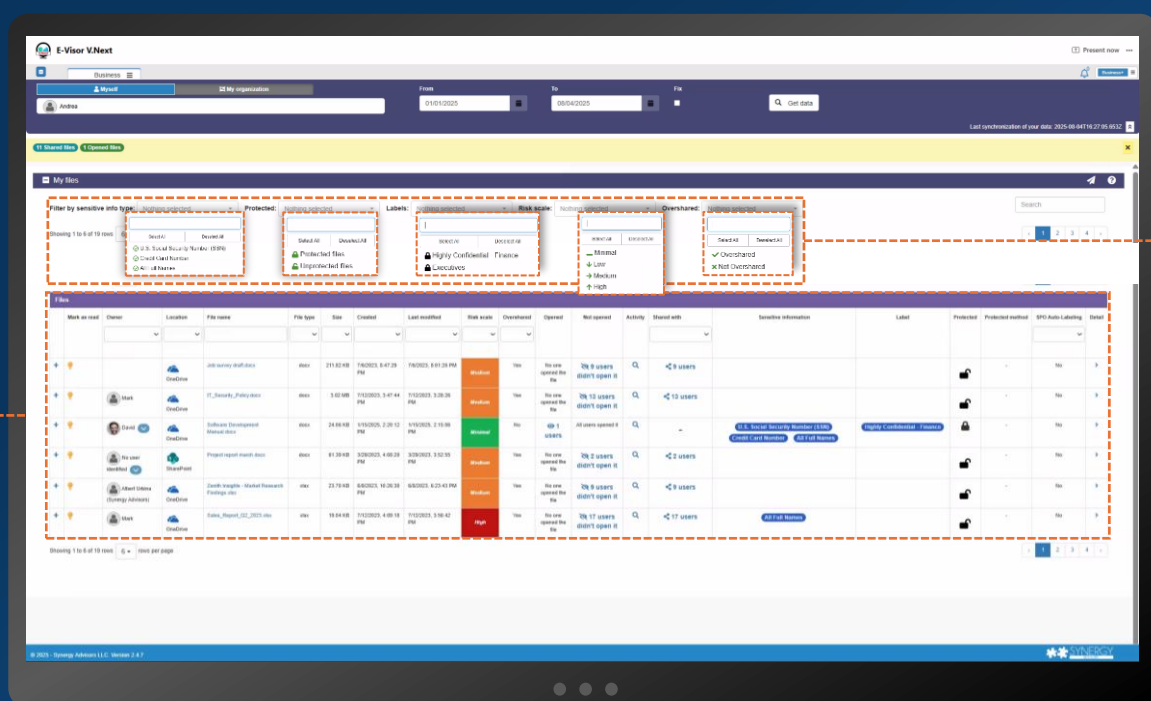
Notify users directly in Microsoft Teams when potential data exposure risks are detected — considering file sensitivity, access type, and configurations that may introduce compliance vulnerabilities — without relying on email.
- User Education**

Help users understand data misuse and compliance risks through a visual interface showing access logs and risk levels, with color-coded indicators based on file type, encryption, content sensitivity, and unauthorized access attempts.
- Self-Service**

Enable users to independently correct non-compliant settings from within Teams, guided by data protection policies — enabling immediate action without external intervention.
- Reduced Operational Costs**

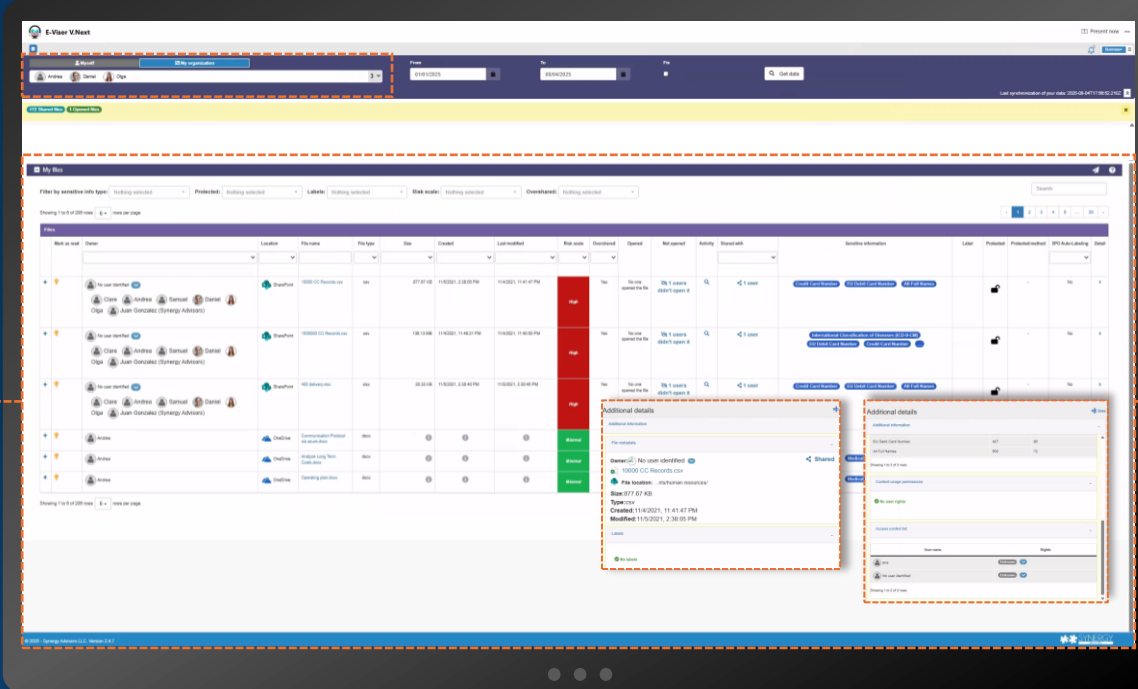
By providing a clear view of risk and enabling user action, the organization enhances its incident response capabilities, reduces time spent on compliance management, and minimizes unnecessary exposure of sensitive information.

Personalized Risk Detection and Compliance Control



Intelligent filters for focused analysis: Dynamic filtering by risk levels, sensitivity labels, protection status, and more, enabling fast, precise exploration, optimizing user time and prioritizing critical compliance cases.

Administrative Visibility of User Collections for Proactive Actions



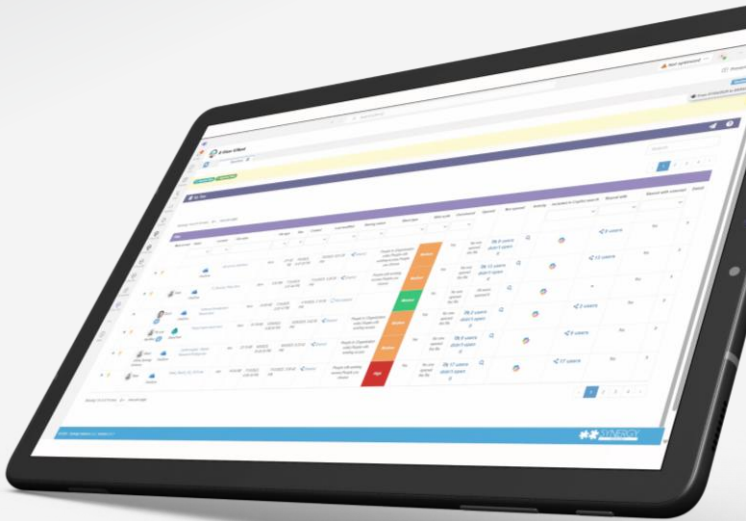
Administrative view: "My Organization" view provides administrators with centralized oversight of user collections. Advanced filters enable the visualization of each user's risk and compliance status, facilitating comprehensive security management.

Visibility for proactive action: Detailed information about users and their files, enabling administrators to make informed decisions and take proactive actions to enhance security and compliance across the organization.

Introducing Micro-Visor (Modern Work)

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.



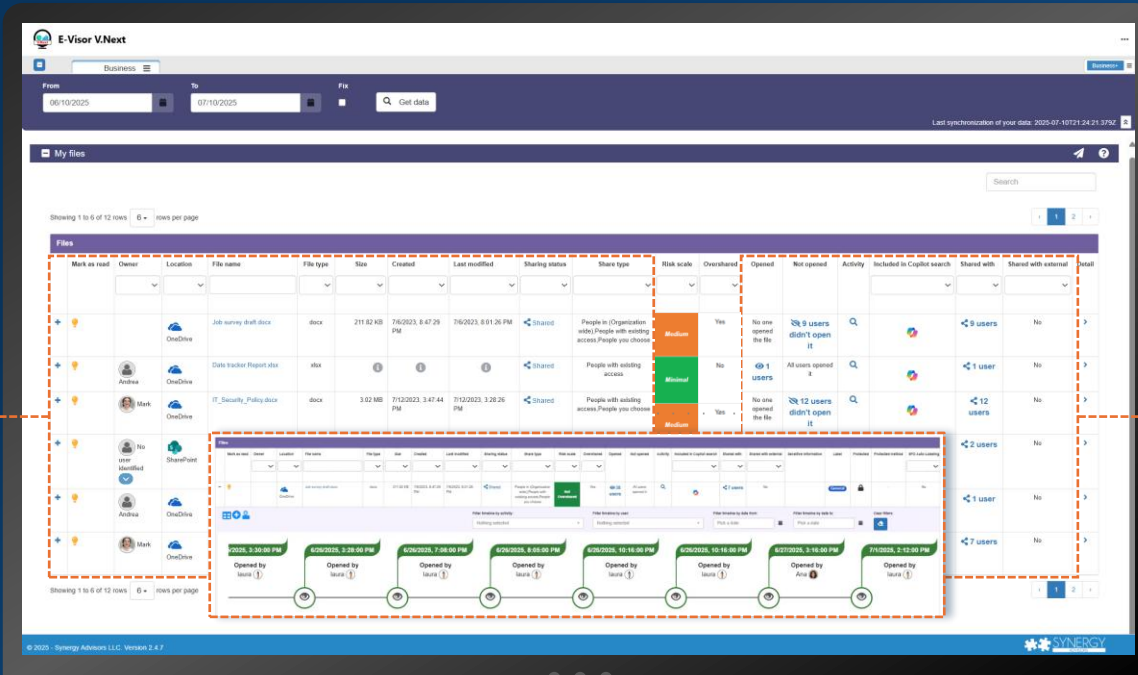
Reduced Operational Costs

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.



Enables Truly Secure and Productive Collaboration through Modern Work

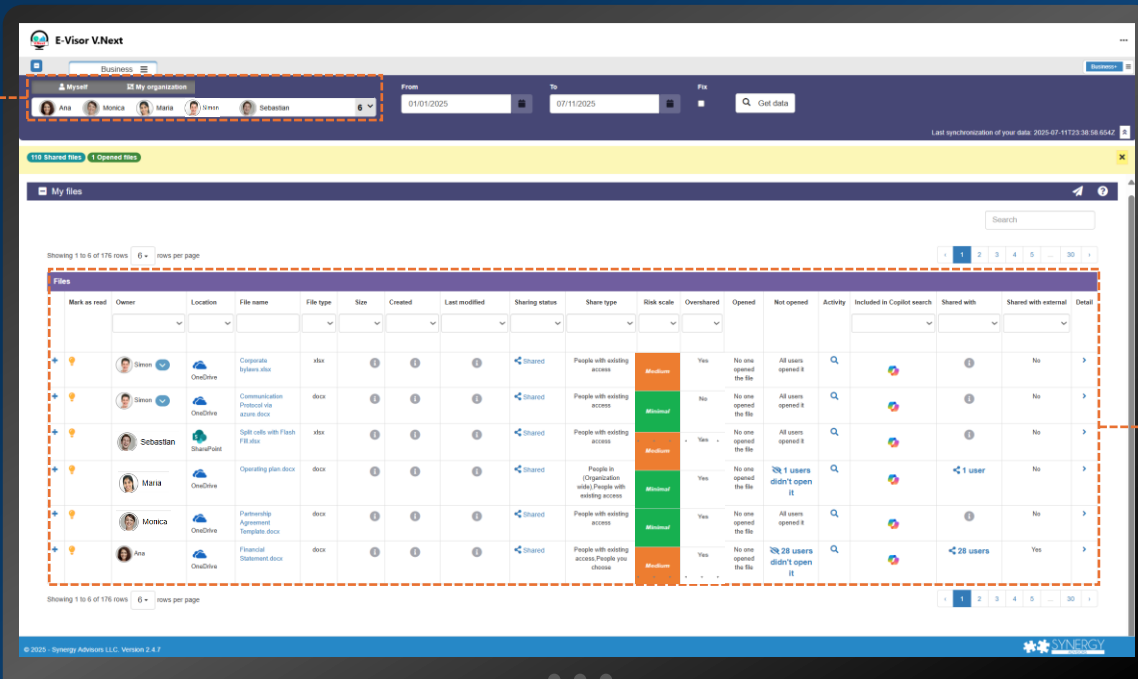
Personal Document Management and Tracking



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.



Introducing Micro-Visor (Identity)

Micro-Visor (Identity): a solution designed to simplify, secure, and streamline digital identity management directly within Microsoft Teams. Empower both end users and administrators by centralizing key identity-related functionalities in a collaborative workspace. Micro-Visor incorporates a set of technical capabilities that enhance the user experience and optimize identity-related processes, strengthening the organization's overall security posture while reducing friction through centralized and simplified management.

Alerts & Notifications

Receive alerts about key identity events—such as changes to authentication methods or password expirations—enabling proactive responses.



IT Cost Reduction

Optimize IT resources and improve operational efficiency by enabling users to manage their own credentials.



End User Education

Guide users on the recommended use of credentials through a friendly, contextual interface that promotes security best practices and compliance.

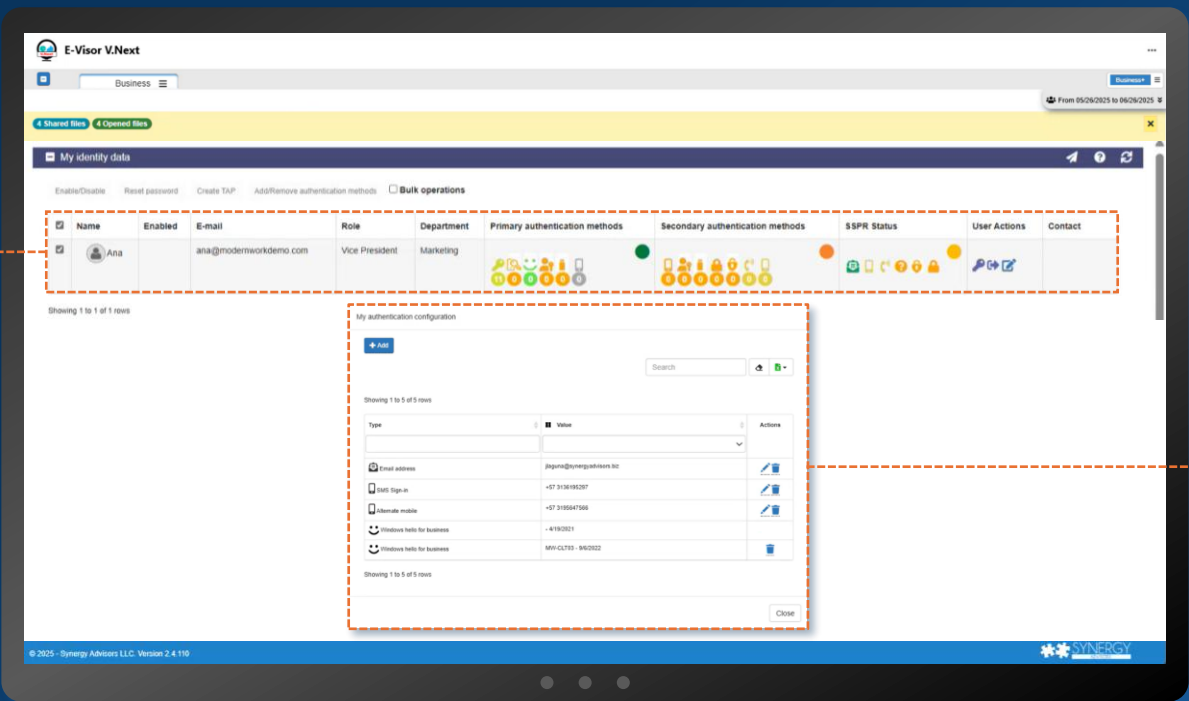


Self-Service

Empower users to register methods, review configurations, and resolve common issues—all within their collaborative environment.



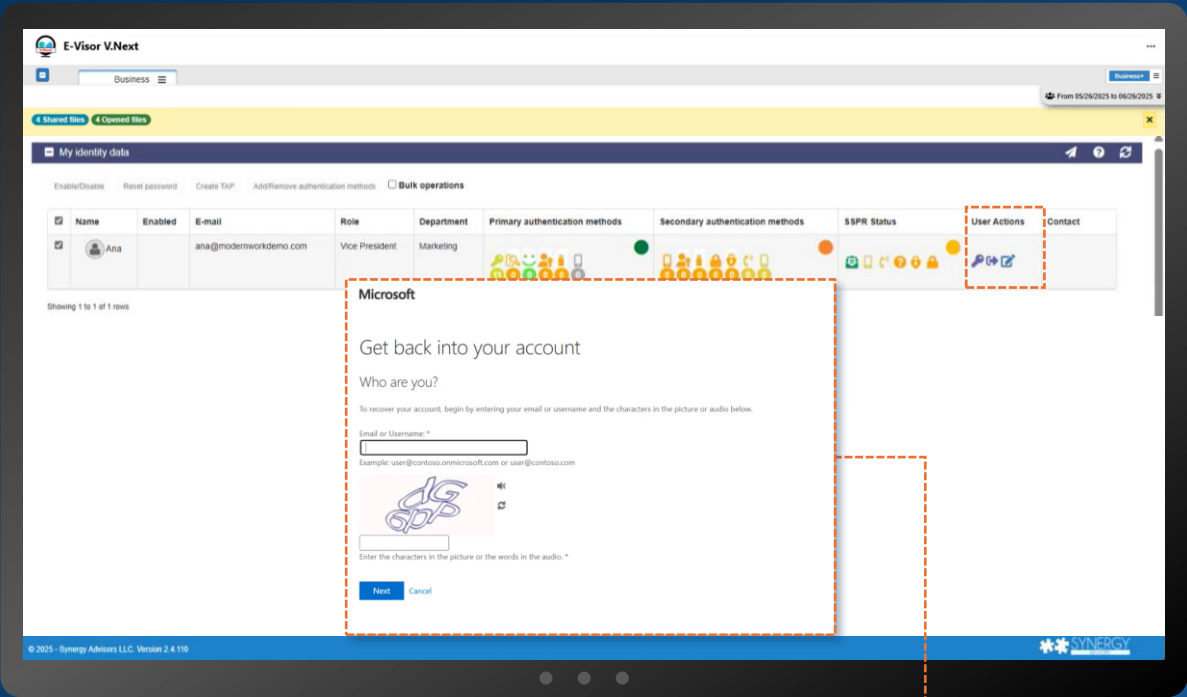
Authentication method management (My self)



View key account information such as name, email, role, department, enablement status, primary and secondary authentication methods, password reset (SSPR) status, available actions, and contact details.

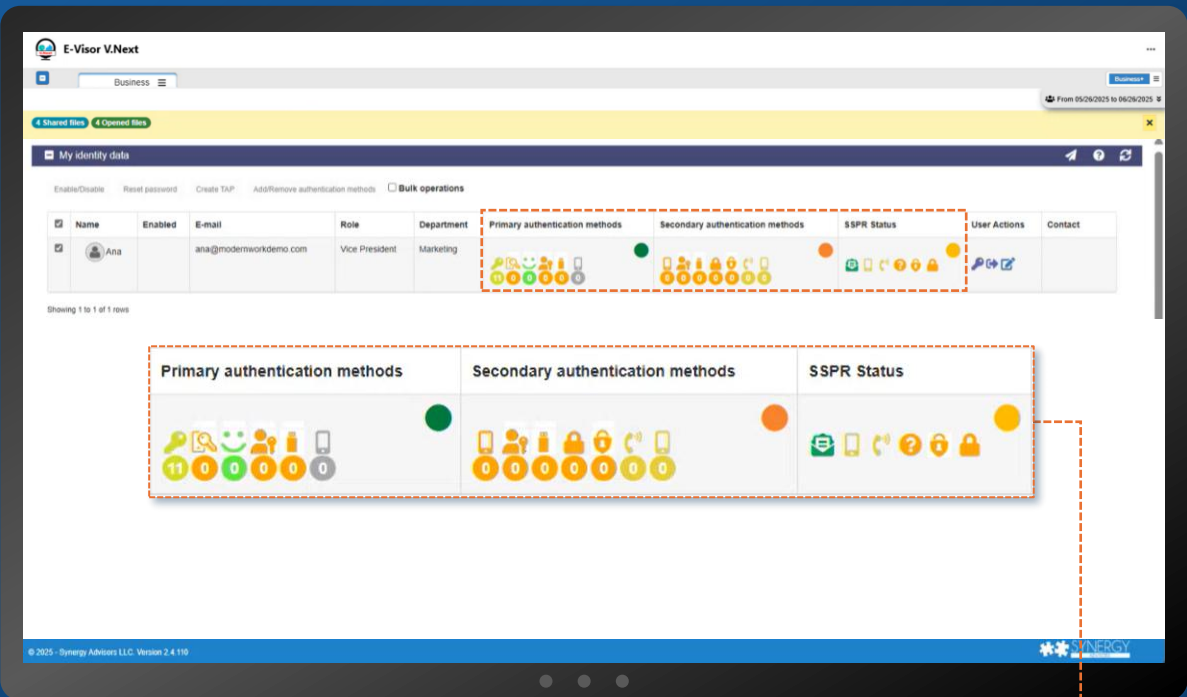
Add, configure, or remove your authentication methods—such as email, SMS sign-in, alternate mobile, and Windows Hello for Business—quickly and securely.

Simplified password change (My self)



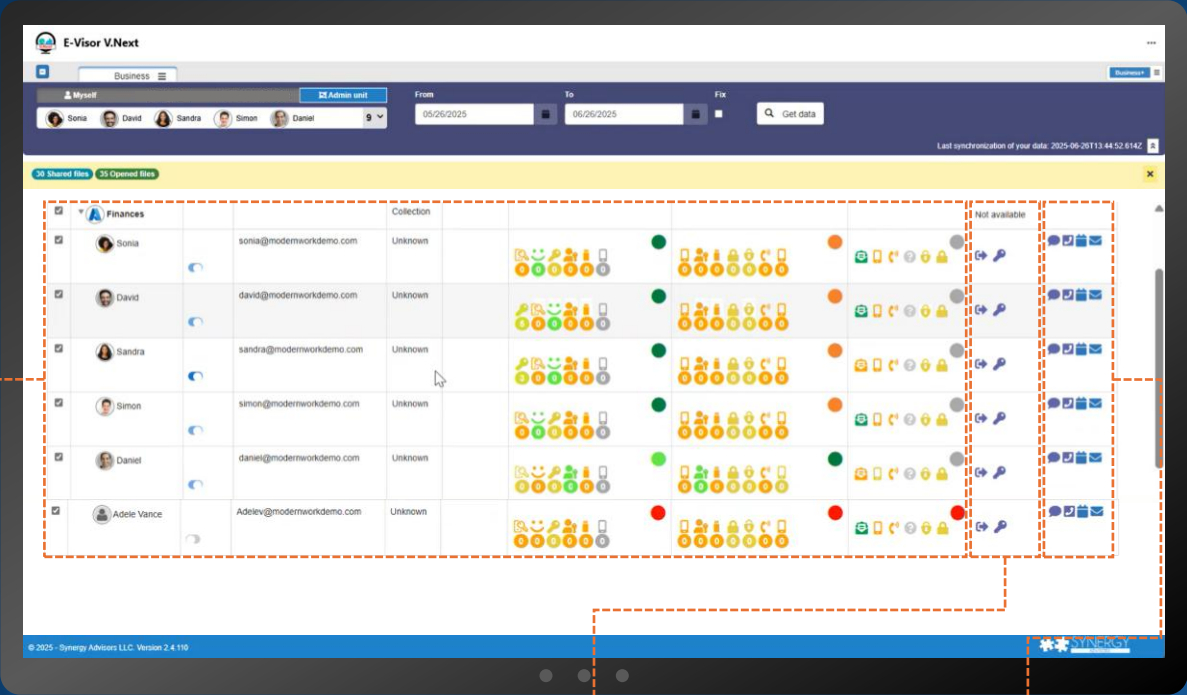
Securely change your password directly from the console, streamlining the process without the need to navigate through multiple portals or platforms.

Security status visibility (My self)



A comprehensive and centralized view of your authentication security posture through an intuitive color-coded scale that highlights levels of protection and areas requiring attention.

Administrative tools & actions (My organization)



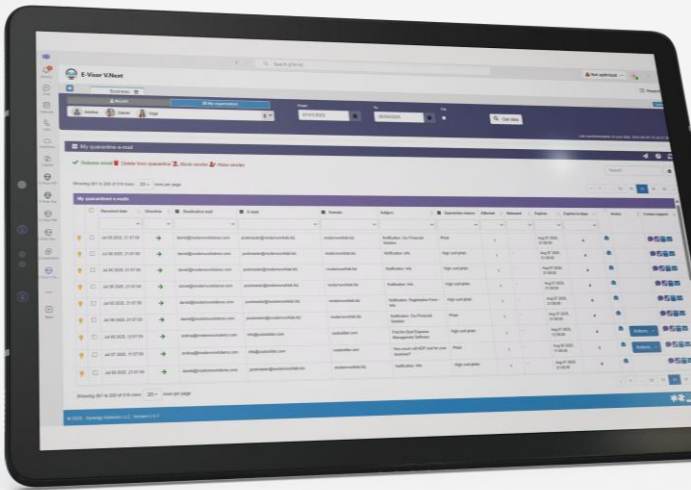
Centralized visibility into the authentication security status of users grouped by administrative units, with visual indicators that reflect protection levels and compliance.

Manage your users' authentication methods with individual or bulk actions, such as password resets using temporary or manually defined credentials.

Contact your users directly via email, Teams chat, call, or by scheduling a meeting to resolve issues related to their credentials and authentication methods.

Introducing Micro-Visor (Security)

Micro-Visor (Security) empowers both end users and administrators with centralized visibility and control over quarantined emails, ensuring that legitimate communications are not lost within advanced security filters — all seamlessly integrated into the Microsoft Teams experience. By providing real-time insights, guided actions, and streamlined workflows for reviewing and releasing messages, the solution enhances decision-making, mitigates potential threats, and reduces the operational burden on IT teams. This not only strengthens your organization's security posture but also ensures communication continuity across departments and business units.



Effective email management requires more than automated filters — it demands user empowerment, real-time visibility, and simplified decision-making:

Alerts and Notifications

Notify users directly in Microsoft Teams when they have quarantined messages, providing immediate access to review and take action — without relying on email-based alerts.



User Education

Display clear indicators and key details like sender, subject, and quarantine reason, along with message preview, to help users understand the context and make informed decisions.



Self-Service

Enable users to manage their own quarantined emails within Teams — including releasing or discarding messages — while administrators access user-grouped views for streamlined oversight and bulk actions.



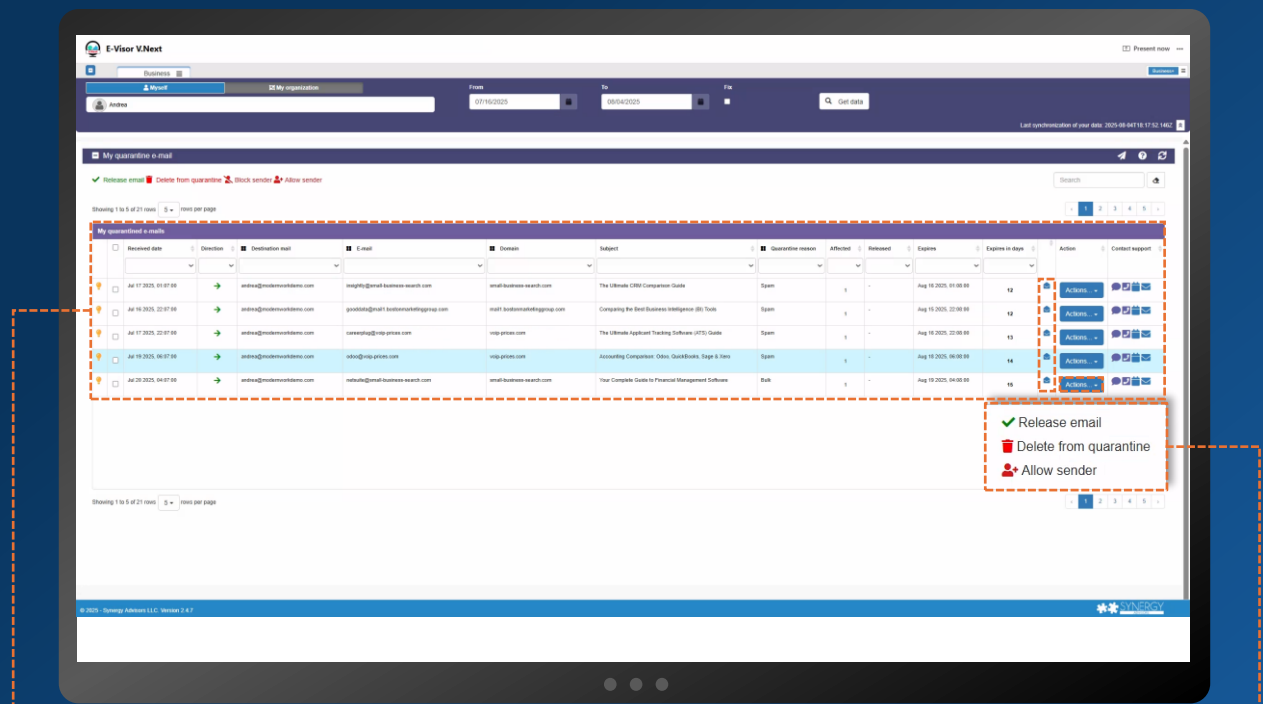
Reduced Operational Costs

By centralizing the experience and empowering both users and administrators, Micro-Visor (Security) reduces IT workload, minimizes ticket volume, and accelerates incident resolution.



Redefine Quarantine Oversight with Intelligent Views and Self-Service Tools

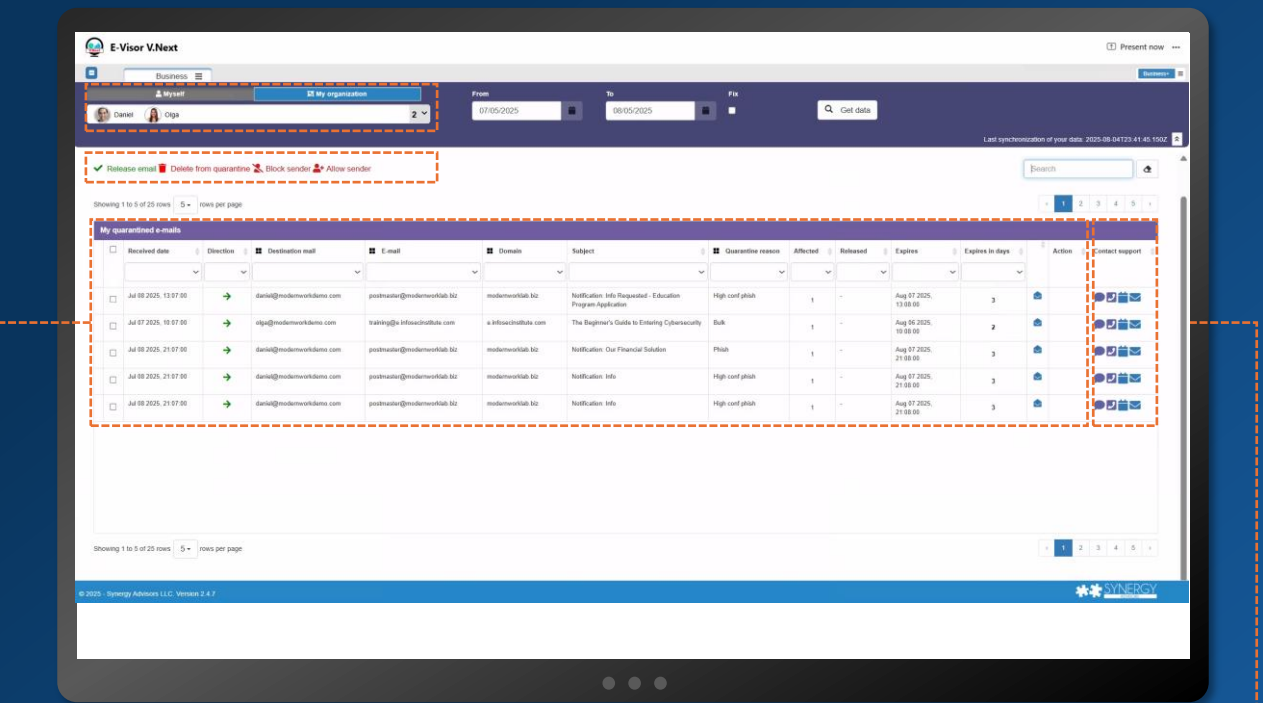
Managing & acting on quarantined emails



See all your emails in quarantine, with details such as the sender, subject, date of receipt, and the status of each email, giving you a clear overview of the emails that have been filtered and helping you manage them effectively.

Streamline operations by **previewing** the content of each email, and, depending on its relevance, either **release** it to your inbox or **delete** it if unnecessary, ensuring an efficient and secure management process.

Quarantined email administration: Control and actions by user



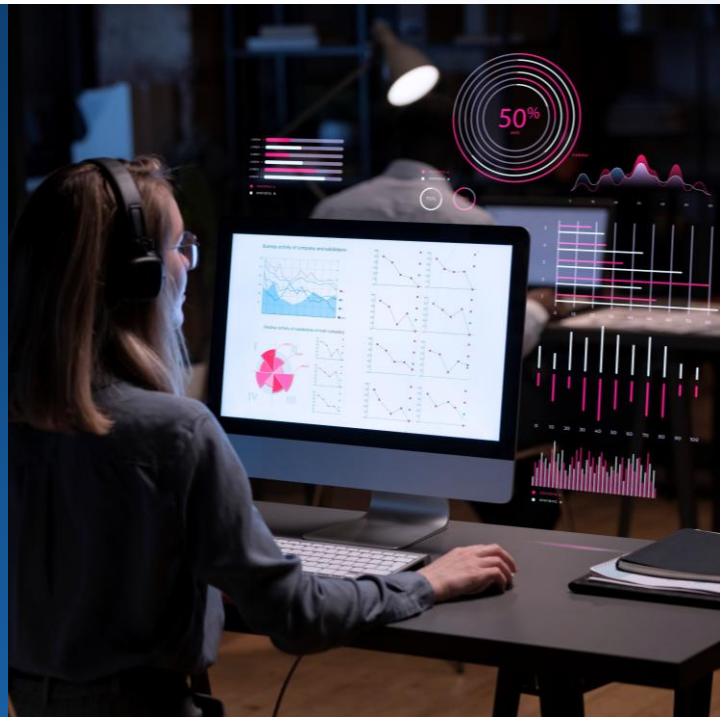
View all relevant details about quarantined emails from specific user collections within the organization. See key information such as sender, subject, date, email status, and more. Available actions include **previewing content, releasing or deleting the email, blocking the sender, and more, enabling efficient and controlled email management.**

When necessary, take a specific action, such as **initiating a chat, making a phone call, scheduling a meeting, or sending an email, enabling personalized resolution of issues related to quarantined emails.**

Empower Your Organization with Unified, Intelligent Operations

Micro-Visor delivers centralized, intelligent visibility across your organization's collaboration, identity, compliance, productivity, and security workflows — enabling both end users and administrators to operate with greater control, speed, and confidence.

By unifying insights, actions, and guidance in one platform, Micro-Visor simplifies daily operations, reduces risk, and enhances coordination across business and technical teams. Micro-Visor's intuitive experience enables organizations to protect critical assets, improve decision-making, and support agility without disrupting productivity.



Why choose Synergy Advisors as your strategic partner?

At **Synergy Advisors**, we provide specialized consulting and managed services to help you maximize the value of your Microsoft 365 environment through governance, automation, and adoption. Our Micro-Visor solution offers a unified experience that connects users, teams, and information across core operational areas — including collaboration, compliance, identity, and security — supporting smarter decisions and more efficient workflows.

Beyond the technology, we work closely with your teams to ensure successful adoption, simplify daily processes, and deliver lasting impact. With Micro-Visor, your organization gains clarity, oversight, and responsiveness — all without compromising agility or user experience.

If you'd 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](#)