E-Visor Teams App

FRONTLINE WORKERS

Democratizing information access with high-level security for frontline workers

CONTEXT

58% — Of remote workers make choices which reduce security*

*Microsoft Digital Defence Report 2020

USD72 — The average cost to an organization to reset a user password*

*Forrester report

Most employees do not know if the information they are accessing is at risk

Leaders have no visibility or control of the information their teams access

In today's evolving workplace, collaboration and flexible access to resources is more important and more challenging than ever before. Organizations are seeking better ways to help frontline staff do more while controlling access based on risks and intelligence.

EMPOWER FRONTLINE WORKERS WITH E-VISOR TEAMS APP

E-Visor Teams App is a reporting and analytics app that helps frontline workers boost their security and productivity, directly from within Microsoft Teams. E-Visor Teams App collects data across different Microsoft portals to present it back to end users in a single location, where they can monitor their identity and device activity, while performing tasks ranging from updating their password, or viewing their Office 365 licensing to scheduling Teams meetings with their colleagues and partners.

WHY E-VISOR TEAMS APP?

Microsoft Teams is the single workspace that connects all team members and tools required to be productive, no matter where they are or what they do. The E-Visor for Teams App is a collaboration and analytics Teams - native app, tested by Top 100 financial organizations, designed to improve security and productivity at the end-user level.

ENABLE INFORMATION DEMOCRATIZATION

Self-service	IT time mitigation	Visibility and support from managers
• Identity • Alerts & notifications • Security and device status • Risk mitigation • Office 365 • Data • Tracking meetings	• Information I want to display • Alerts I want to receive • Actions I will alow my users to take	• Tool adaptation and customization • Viva • Modulation of information • Alerts & notifications • Security and device status

HIGHLIGHTED FEATURES

- Facilitate and limit help desk and support calls by providing Self-Service Password Reset (SSPR) management

- Help users enable and manage their Multi-Factor Authentication (MFA) and verify it is configured according to best practices

- Surface security alerts from Microsoft Defender, across identity, endpoint, and cloud applications, and enable users to proactively respond to incidents

- Help frontline workers create and manage identity and access management requests, including ability to see current status and request specific approvals

- Empower frontline team to take control of the security of their identity

- Review Office 365 usage and gain insights through in-depth analysis

- Easily surface, and proactively respond to, Office 365 account issues, such as inappropriately shared files or storage limits

- Quickly discover recently accessed files across Office 365 applications

- Easily identify and collaborate with colleagues across many different communication channels

- Easily review and edit profile information

- Teams native app provides a seamless experience for end users

- Review M365 subscription and licensing information

THE RIGHT INFORMATION FOR THE RIGHT USERS

Define what type of information your frontline workers should see (*), according to characteristics such as:
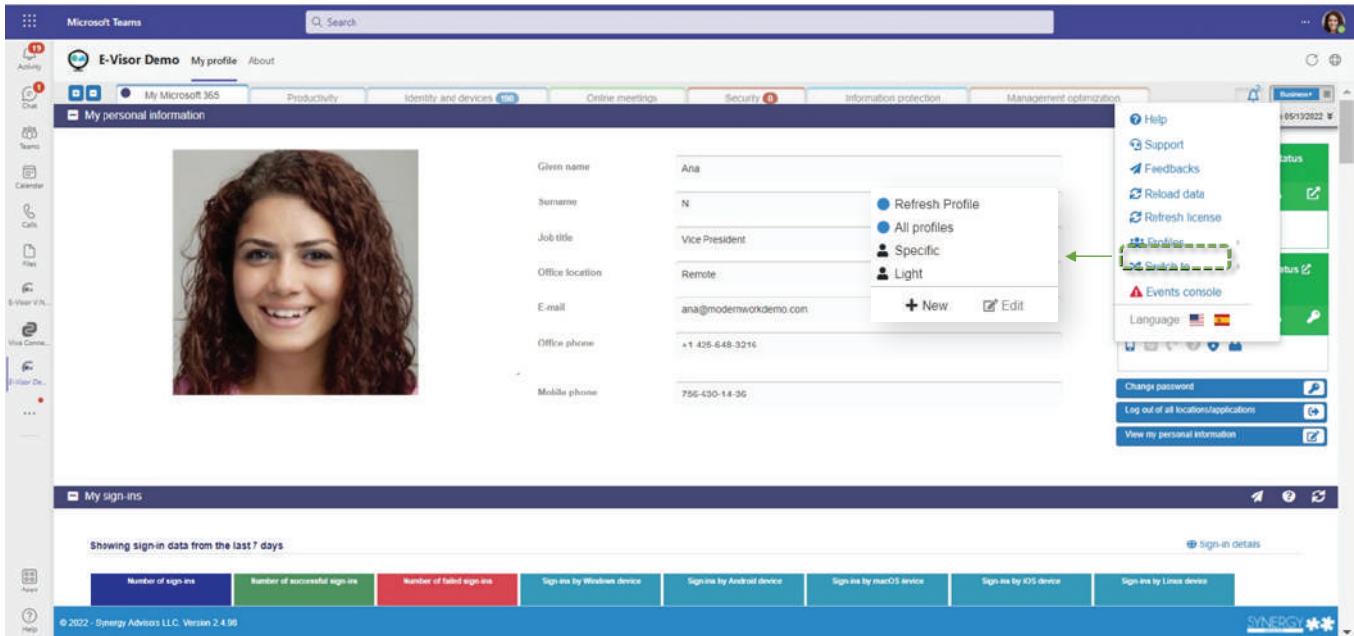
Role

Department

Permissions taxonomy

Application profile

≣ ▾	Name	Description	
4	Supervisor	External work team supervisor	
3	External Supervisor	Supervisor of off-site users	
2	User External	Users who are working off-site	
1	All Information		

*Only available on 'Business' and 'Business +' versions.

NEXT GENERATION CYBERSECURITY

E - Visor Teams App provides strong capabilities to secure sensitive information and resources in your environment, supported by advanced Microsoft solutions. From the security tab, the user can easily see, and take action on, the security of their identity, devices, and cloud apps.

Microsoft Defender for Endpoint - MDE
Identify if the devices have been compromised and view device data:
- Name, ID, and health status of the devices
- Severity, type, and category of security events
- Status and classification
- Actions to take (anti-virus scan, isolate machine)

Microsoft Defender for Identity - MDI
Identify if your identity has been compromised by an external attack:
- User and IP adress
- Number of impacted users and devices
- Severity of risk
- Actions to take (quick or full scan, selective or full machine isolation)

Microsoft Defender for Cloud Apps - MDCA
Identify infractions when using or accessing cloud applications :
- Type of infraction
- Date of the event
- Applications involved

Microsoft Defender for Offices 365 - MDO
Validate the status of the Office services:
- Compromised Office apps
- Type of compromise
- Actions to take (communicate to IT administrator)

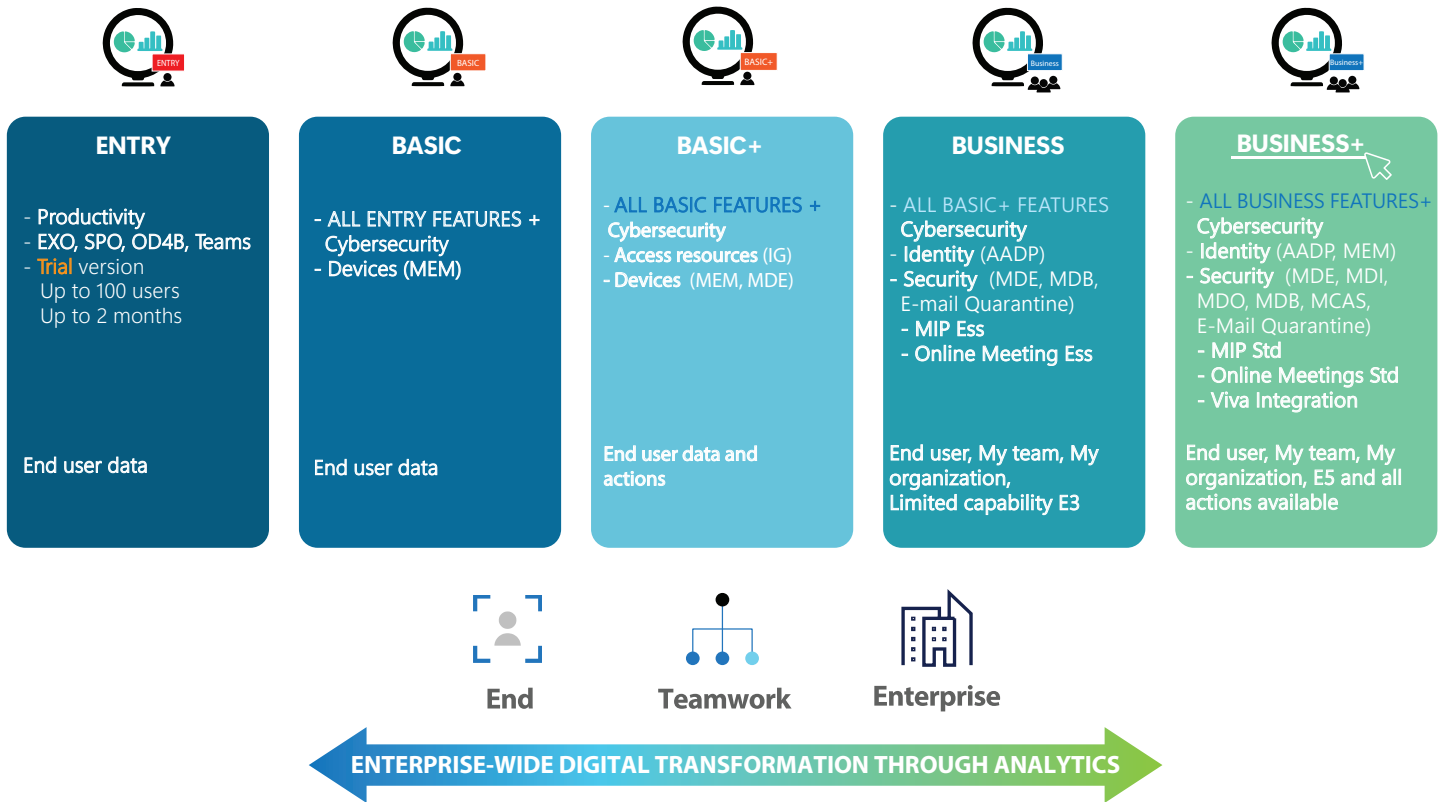**E-mail Quarantine - MDO + EXO (Exchange Online)**
Identify the status of the expected and outgoing e-mails:
- Number of e-mails blocked
- Policies applied
- E-mail addresses
- Quarantine reason
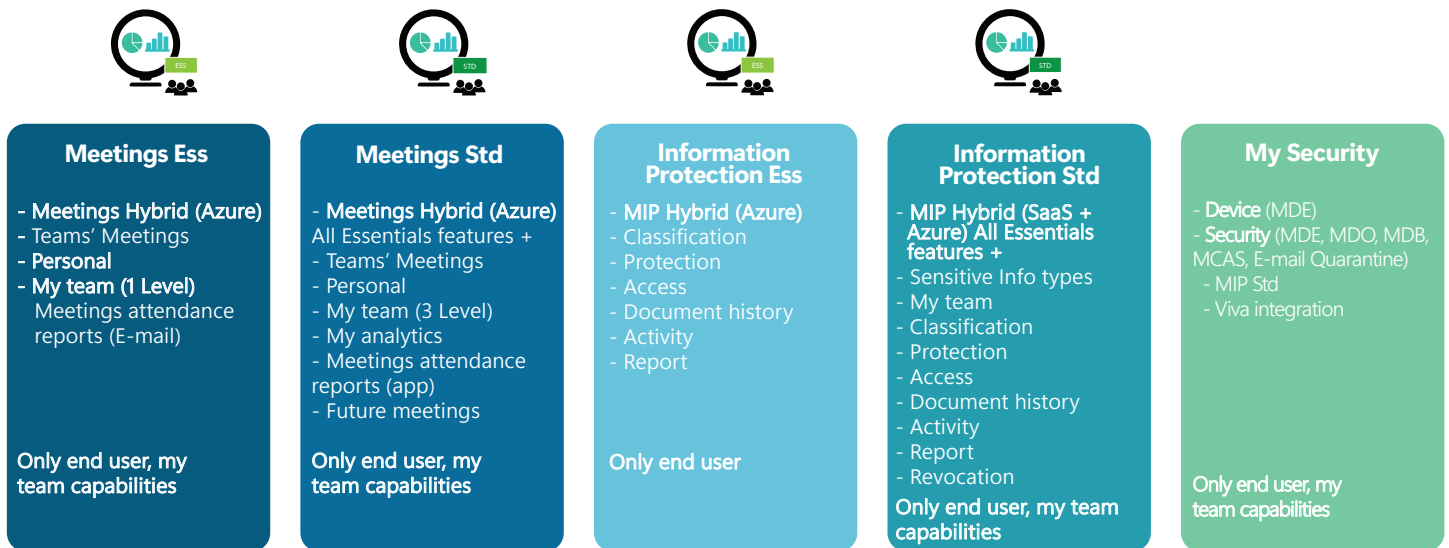- Actions to take (realease e-mail, delete from quarantine, block sender)

Microsoft Defender

E-VISOR TEAMS APP VERSIONS

ENTRY

- Productivity
- EXO, SPO, OD4B, Teams
- Trial version
  Up to 100 users
  Up to 2 months

End user data

BASIC

- ALL ENTRY FEATURES +
  Cybersecurity
- Devices (MEM)

End user data

BASIC+

- ALL BASIC FEATURES +
  Cybersecurity
- Access resources (IG)
- Devices (MEM, MDE)

End user data and
actions

BUSINESS

- ALL BASIC+ FEATURES
  Cybersecurity
- Identity (AADP)
- Security (MDE, MDB,
  E-mail Quarantine)
  - MIP Ess
  - Online Meeting Ess

End user, My team, My
organization,
Limited capability E3

BUSINESS+

- ALL BUSINESS FEATURES+
  Cybersecurity
- Identity (AADP, MEM)
- Security (MDE, MDI,
  MDO, MDB, MCAS,
  E-Mail Quarantine)
  - MIP Std
  - Online Meetings Std
  - Viva Integration

End user, My team, My
organization, E5 and all
actions available

End **Teamwork** **Enterprise**

ENTERPRISE-WIDE DIGITAL TRANSFORMATION THROUGH ANALYTICS

ADD-ON FEATURES

Synergy Advisors offers additional features that are part of the Business+ version and can be added to the Basic and Basic+ versions.

Meetings Ess

- Meetings Hybrid (Azure)
- Teams' Meetings
- Personal
- My team (1 Level)
  Meetings attendance
  reports (E-mail)

Only end user, my
team capabilities

Meetings Std

- Meetings Hybrid (Azure)
All Essentials features +
- Teams' Meetings
- Personal
- My team (3 Level)
- My analytics
- Meetings attendance
reports (app)
- Future meetings

Only end user, my
team capabilities

Information Protection Ess

- MIP Hybrid (Azure)
- Classification
- Protection
- Access
- Document history
- Activity
- Report

Only end user

Information Protection Std

- MIP Hybrid (SaaS +
  Azure) All Essentials
  features +
- Sensitive Info types
- My team
- Classification
- Protection
- Access
- Document history
- Activity
- Report
- Revocation

Only end user, my team
capabilities

My Security

- Device (MDE)
- Security (MDE, MDO, MDB,
MCAS, E-mail Quarantine)
  - MIP Std
  - Viva integration

Only end user, my
team capabilities

IT ADVANCED EXPERIENCE:
NEW PROCESS OPTIMIZATION CAPABILITIES

MANAGEMENT OPTIMIZATION

New tab that gathers information through different platforms, summarizing changes in a specific time frame, helping the organization understand how their administrative portals are working.
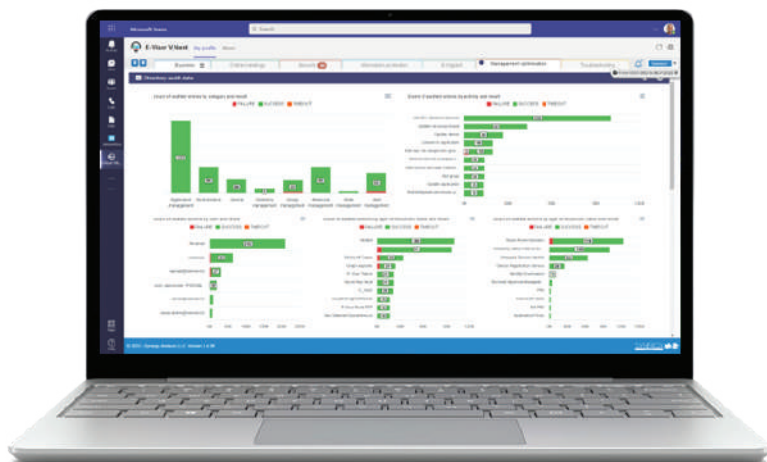
Service Status History:

Enables the organization to know the service status of its administration platforms, and their functionality history.

Directory Audit Data:

Provides a summary and behavior of the organization's Active Directory, status, and activities.

Service Messages:

Offers the organization IT incidents status, analytics, and recommendations

TROUBLESHOOTING

New tab for fast problem solving while enhancing time optimization.

Group Membership: Groups of the Active Directory which the user, and teams belong to.

Teams Membership: Microsoft Teams' channels and groups the user, and teams belong to.

Role Membership: Shows the role of the user within the group.

E-Suite Collection Membership: Type of E-Suite collection users have assigned.

Conditional Access Rule Membership: Users, and teams' conditional access rules applied to.

Office 365 DLP Rule Membership: Rules within Office 365 DLP applied to the users, and teams.

Information Protection: Shows the permissions the user has assigned at information protection level.
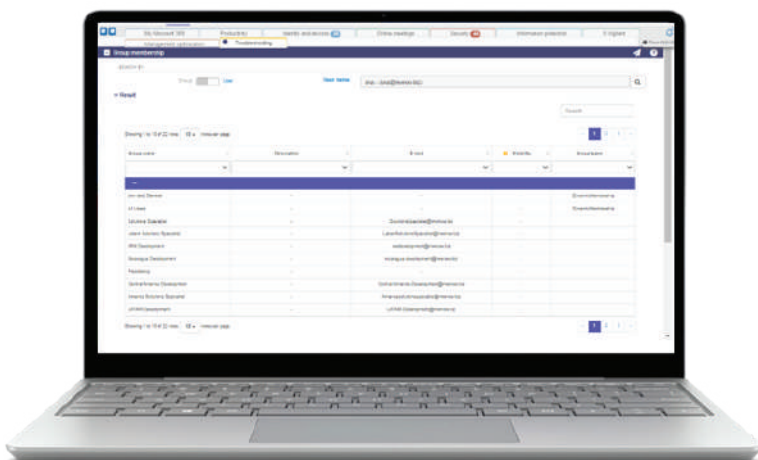
BENEFITS FOR FRONTLINE WORKERS

- Consolidated view of end user information in one unique console

- Single application natively integrated with Microsoft Teams

- Easy deployment and management for end users, team leaders, and administrators

- Save time and money by using a single location to submit, track, and manage information access

- Full E-Visor for Teams App experience – visibility and secure productivity

- Robust tracking and reporting

- Automated features and capabilities provisioning and deprovisioning

- Built for Microsoft Teams

WHAT ORGANIZATION IS THIS SOLUTION FOR?

Any organization looking to:

- Reduce administrative task and costs

- Connect employees with the tools they need to perform at their best

- Consolidate administrative views

- Simplify processes through automation and personalized actions

- Track the frontline staff activity

- Securely provision access

- Improve productivity and motivation of frontline workers

ABOUT US

Synergy Advisors is a premier Microsoft Certified Partner that specializes in Microsoft 365, Identity, Azure B2C and B2B Collaboration, Security, Management, and Cloud technologies. We help you digitally transform and implement a more secure collaborative infrastructure, reduce your IT costs, and meet your regulatory requirements through our comprehensive portfolio and experience in consulting and managed services.

Secure E-mail

- Users
- Apps
- Services
- Hygiene
- Threats
- Data Leak Mitigation

Secure Collaboration

- Users (internal / external)
- Apps
- Services
- Hygiene
- Threats
- Data Leak Mitigation

Device Protection

- Applications security
- O.S. security
- Security base line
- Threats
- Data Leak Mitigation

Information Protection

- Data in use
- Data at rest
- Data in transit
- Application integration
- Data Leak Mitigation
- Structured and unstructured data protection

Platform Protection

- Monitoring / Services analysis/ Alerts and notifications
- Security base line

Contact us for more information: HERE
Or e-mail us at: ww-sales@synergyadvisors.biz

LET'S START!

SYNERGY
ADVISORS

Synergy Advisors LLC

Synergy Advisors

@Synergyadvisors

Synergy Advisors

@SynergySEC