



XDR - Synergy Advisors for Managed Services  
SOC



# Synergy Advisors

Overview

## CONSULTING

- Architecture Design Sessions [ADS]
- PoC in a Box
- Production Pilot
- End-to-end Deployment
- Adoption and Change Management
- Workshops and Training

## SOLUTIONS

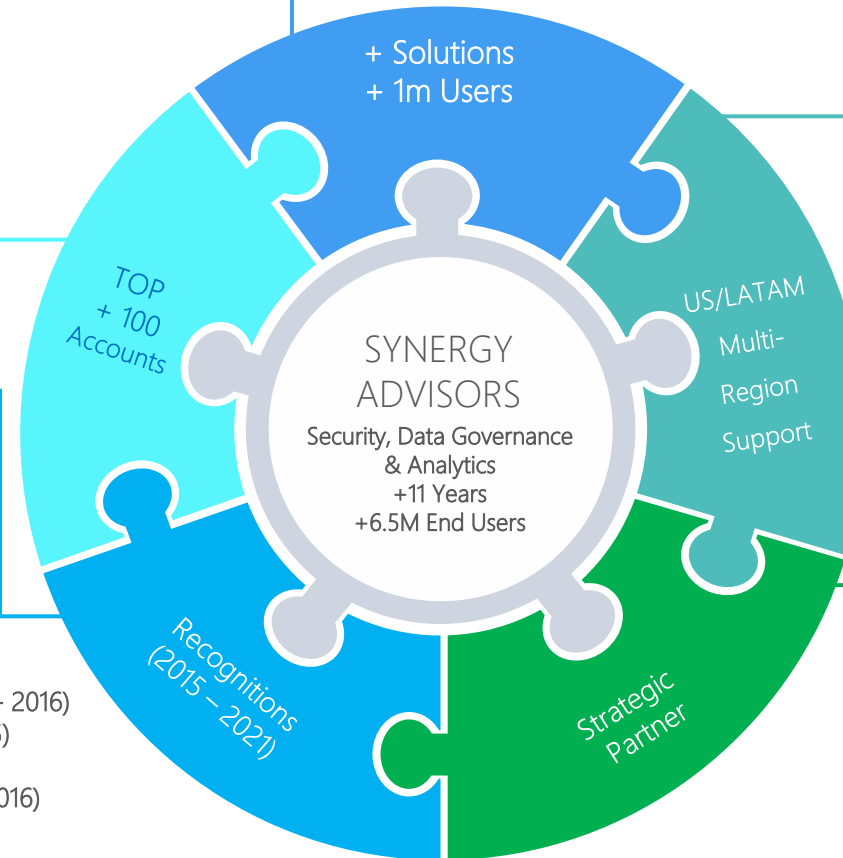
- E-Suite: E-Visor, E-Inspector, E-Cryptor, E-Vigilant, E-Migrator, E-Visor Teams App (Available in the Azure Marketplace):
  - Information Governance and Compliance solutions
  - Enterprise Analytics
  - Next Gen Operations, Alerting, Monitoring and Support

## MANAGED SERVICES

- End-to-end Secure Productivity
- Cyber Security
- Productivity
- IT automation
- Continuous optimization
- Modern business and IT operations framework

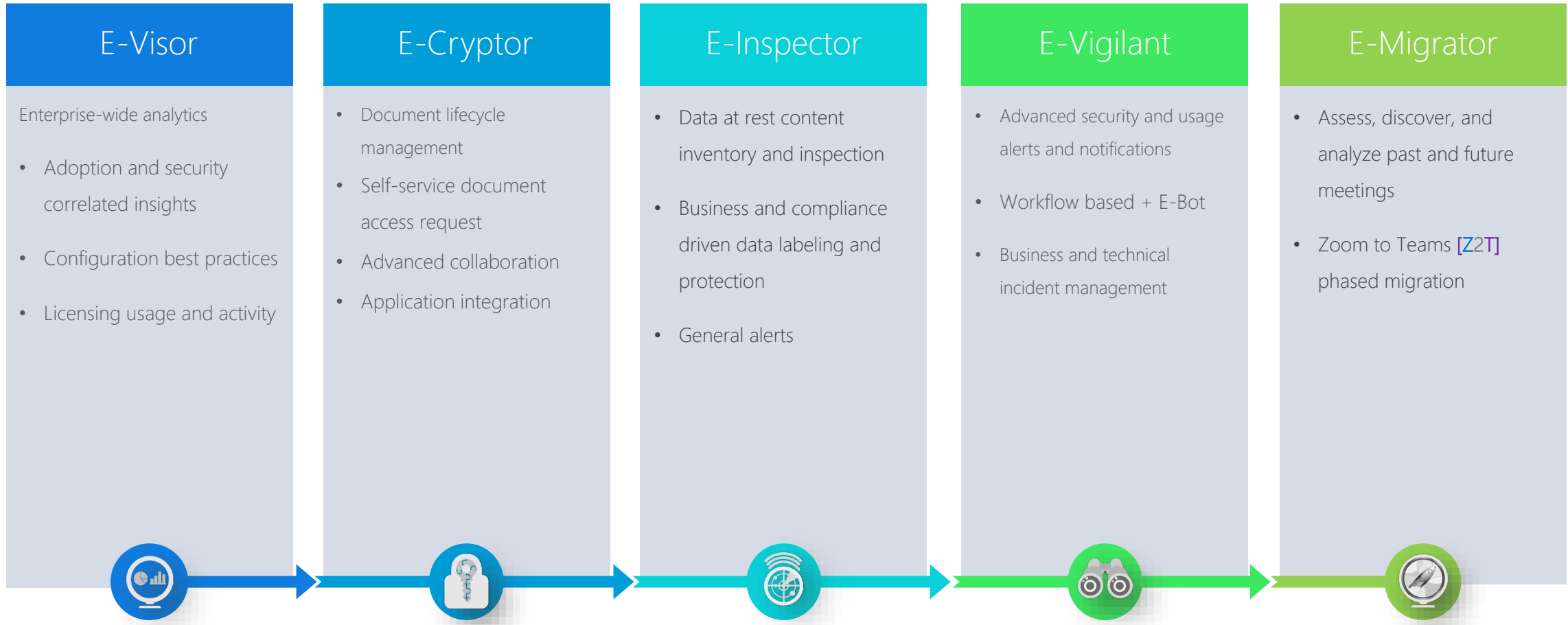
## AWARDS AND NOMINATIONS

- Microsoft MISA (Member 2020)
- Guardians of Productivity (Member 2020)
- Security & Manageability Elite Partners (Member since 2015)
- Identity Advisors (Member since 2015)
- Security Workshop – Partner of the Year (Finalist 2021)
- Security Workshop – Partner of the Year (Winner 2020)
- US EPG Partner of the Year [West Coast] (Finalist 2017)
- WW Microsoft Partner Case Study – Cloud Adoption (Winner - 2016)
- WW EMS Partner of the Year (Finalist 2016, Nominated 2015)
- Alliance Partner of the year (Nominated FY 2015 & 2016)
- National Solution Partner of the Year (Nominated FY 2015 & 2016)
- Compete Partner of the Year (Nominated FY 2015 & 2016)
- Cloud Partner of the Year (Nominated FY 2015 & 2016)
- Specialty Partner Apps and IP (Nominated FY 2015 & 2016)



## ADDITIONAL PRODUCTS AND TECHNOLOGIES

- Yubico
- Thales
- Secude
- Entrust



# Solutions



## 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 baseline
- Threats
- Data Leak Mitigation

## Information Protection and Compliance

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

## Threat Protection

- Users (internal / external)
- Devices
- Identities
- Endpoints
- Cloud
- Monitoring
- Infrastructure
- Security baseline

## Platform Protection

- Monitoring / Services analysis/ Alerts and notifications
- Security baseline



# XDR - Synergy Advisors for Managed Services SOC



# XDR - Synergy Advisors for Managed Security Services

Extended, Detection and Response strategy that provides 24/7/365 Managed SOC Services.



Advanced Hunting



Customer

- Detection
- Response
- Remediation



*NOTE: All this across Microsoft unified SecOps stack*

## What do we offer?

### Monitor, Hunt, and Respond

- 24x7x365 incident monitoring across Microsoft Security Solutions
- End to end Incident Management & Resolution (It includes resolving incidents and alerts)
- Advanced hunting using SIEM solutions and Latest Microsoft Technologies
- Defender's built-in response capabilities (Preventive actions, live response, block files, suspend user(s), delete email or block emails)

## What do we do?

### Integration

- Synergy Advisors integrates incident data that includes management and control of devices using Microsoft Security solution like MEM, MDE, identity (MDI), email (MDO), cloud apps (MDA) among others.
- In addition, we enhance advanced hunting investigation performed with proprietary and SIEM solutions.
- Custom detection can be customized based on customer's needs for custom hunting and detection queries leveraging M365 operations
- Perform manual/automatic response actions by leveraging M365D portals using APIs and Synergy Advisors solutions

### Onboarding and posture Management

- Synergy Advisors aids onboarding and adopt of invested Microsoft Solutions to strength security posture.
- Set and manage right security configurations based on customer needs, requirements and best practices of the industry to ensure the best protection level for customers.





## Synergy's SOC Services > Protect Organization's Against Cyberattacks

Overview of the services provided

### Investigating Potential Incidents

- Alerts Optimization
- SOC Analysis
- Incident Investigations

### Triaging & Prioritizing Detected Incidents

- Incident Triage
- Incident Prioritized
- Incident Optimized

### Coordination of Incident Response

- Microsoft Tools and Technologies
- Identification and Remediation

Other SOC roles and responsibilities

### Maintaining Relevance

- Manage Threats
- New & Trending Attacks
- Update of Set of Rules

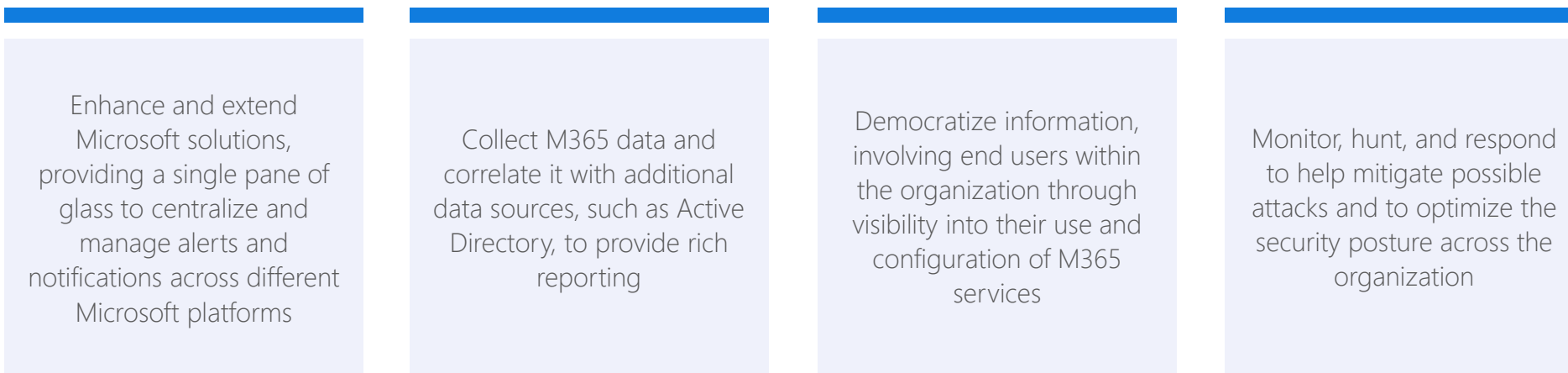
### Patching Vulnerable Systems

- Identify, Apply & Testing
- Vulnerability Environments
- System, Hardware & Software

### Infrastructure Management

- Onboarding and Adoption
- New Security Solutions
- Managed and Optimization

Synergy Advisors has developed a comprehensive offering that extends across the Microsoft unified SecOps stack and includes different integration levels in a holistic combination of consulting services, and implementation of Microsoft security solutions, augmented with the power of E-Visor Teams App.



← ONBOARDING AND ADOPTION OF MICROSOFT SECURITY CAPABILITIES AND SOLUTIONS →



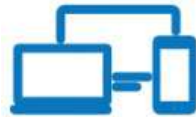
## SOC – Capabilities and solutions managed



### Identities

Microsoft Defender for Identity

- Monitor users, entity behavior, and activities with learning-based analytics
- Protect user identities and credentials stored in Active Directory
- Identify and investigate suspicious user activities and advanced attacks throughout the kill chain
- Provide clear incident information on a simple timeline for fast triage



### Endpoint

Microsoft Defender for Endpoint

- Core Defender Vulnerability Management
- Attack surface reduction
- Next-generation protection
- Endpoint detection and response
- Automated investigation and remediation
- Microsoft Secure Score for Devices
- Microsoft Threat Experts



### Apps and cloud apps

Microsoft Defender for Cloud Apps

- Discover and control the use of shadow IT
- Protect your sensitive information anywhere in the cloud
- Enable secure remote work, protect against threats
- Help secure your organization with real-time controls
- Manage your cloud app security posture
- Gain insight into your Microsoft 365 app behaviors



### E-mail and docs

Microsoft Defender for Office 365

- Configuration, protection, and detection capabilities:
- Safe Attachments
- Safe Links
- Safe Attachments for SharePoint, OneDrive, and Microsoft Teams
- Anti-phishing protection in Defender for Office 365
- Real-time detections



### SIEM

Microsoft Sentinel

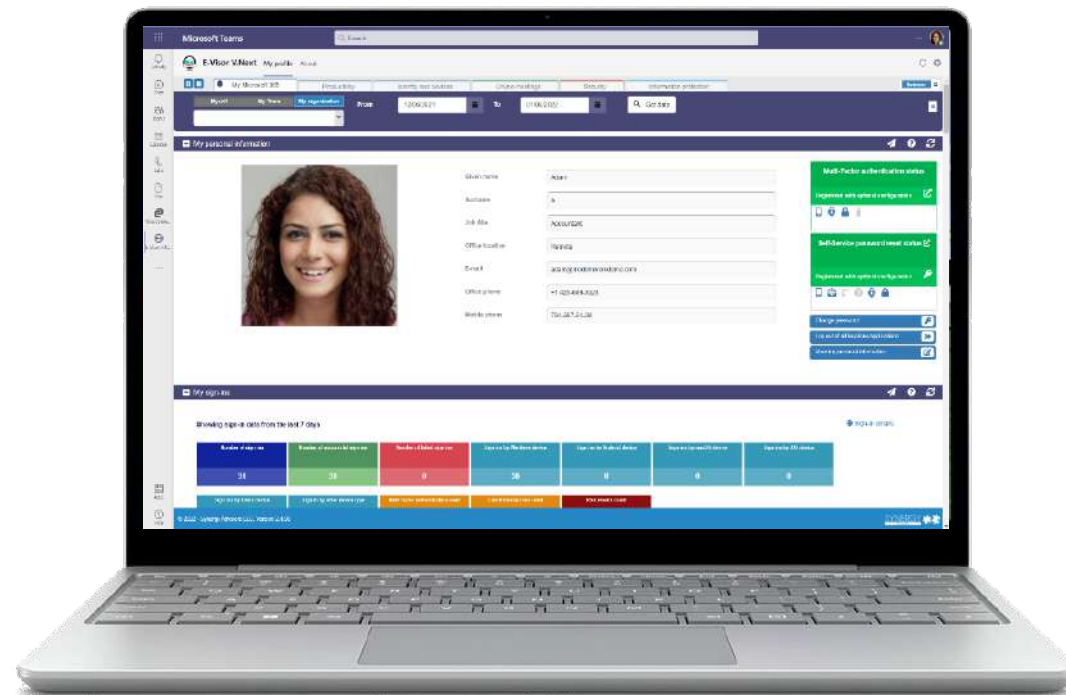
- Collect data at cloud scale across all users, devices, applications, and infrastructure
- Detect previously uncovered threats and minimize false positives using analytics
- Investigate threats with AI and hunt suspicious activities at scale, tapping into decades of cybersecurity
- Respond to incidents rapidly with built-in orchestration and automation

## E-Visor Teams App

Centralized place aimed to empower end users to manage Microsoft solutions, leveraging data from Microsoft 365, Azure Active Directory, MDE, MDI, MDA, MDO, and optimizing Sentinel - all inside Microsoft Teams.



- Ingest Microsoft Defender, MEM, and identity information and health, including device (MDE), identity (MDI), e-mail (MDO), cloud apps (MDCA), and cloud infra.
- Alert information via bots or API integration
- Advanced hunting investigation performed in a single pane of glass, utilizing Microsoft Graph APIs
- Custom detection creation: customized depending on customer needs and scenarios; It can include advanced hunting custom detection queries and custom indicators added to the system through M365D portals or APIs
- Perform manual/automatic response actions
- Training/readiness, setup, onboarding, adoption and ongoing monitoring, response, and management service



E-Visor Teams App +



End User – Manager – IT Experience



Additional info: [Link](#)

Offering overview: [Link](#)



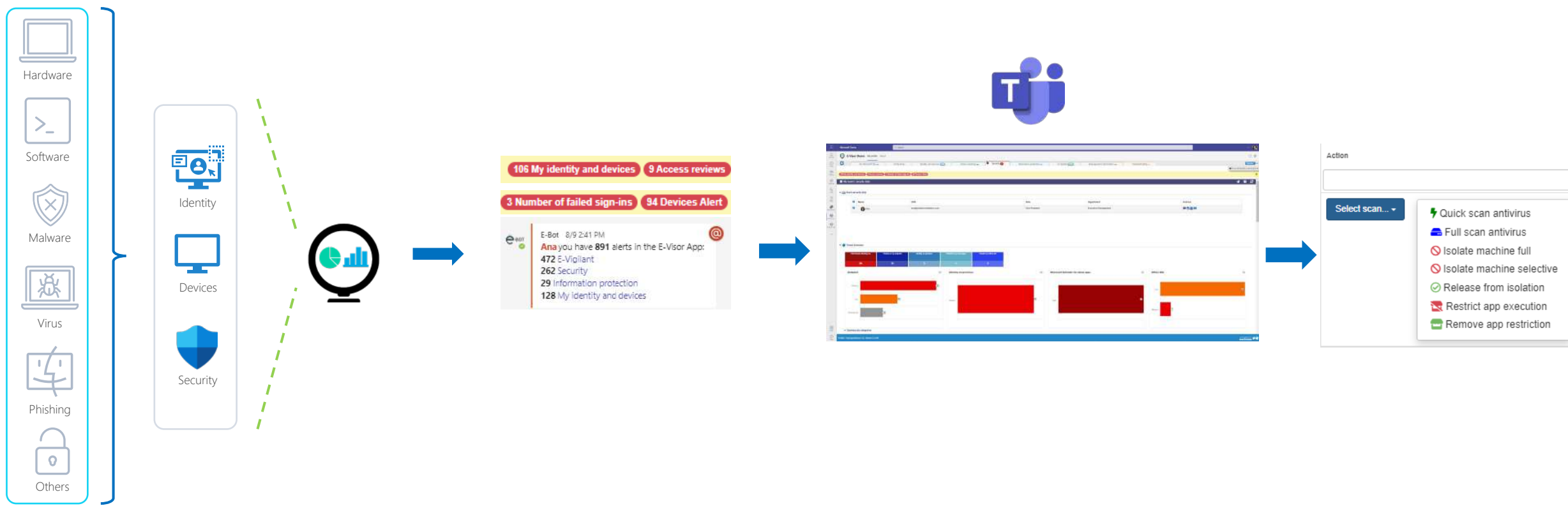
## How does 'XDR + E-Visor Teams App' work?

Workloads analysis by E-Visor Teams App

Alerts and notifications

App views by E-Visor Teams App

Custom actions



## Centralized events collected by Defender platforms

The screenshot displays the E-Visor Teams App interface within a Microsoft Teams environment. The top navigation bar includes tabs for 'My Microsoft 365', 'Productivity', 'Identify and devices' (108), 'Online meetings', 'Security' (0), 'Information protection', 'E-Vigilant' (738), 'Management optimization', and 'Troubleshooting'. A yellow notification banner at the top indicates: '108 My identify and devices', '3 Access reviews', '3 Number of failed sign-ins', and '34 Devices Alert'.

The main content area is titled 'My team's security data' and shows 'Ana's security data' in a table:

Name	UPN	Role	Department	Actions
Ana	ana@modernworkdemo.com	Vice President	Executive Management	[Chat] [Share] [Email]

Below the table is a 'Threat Summary' section with a dashboard of charts:

- Total threats affecting me:** 26
- Threats on my endpoint:** 11
- Identity on-premises:** 5
- Threats to my cloud apps:** 1
- Threats my Office 365:** 9

The charts are categorized as follows:

- Endpoint:** Medium (47), Low (23), Informational (14)
- Identity on-premises:** Medium (3)
- Microsoft defender for cloud apps:** High (1)
- Office 365:** Low (8), Medium (1)

At the bottom, there is a 'Summary by categories' section and a footer with the text '© 2022 - Synergy Advisors LLC. Version 2.4.106' and the SYNERGY logo.

## Incidents information such as users, impacted machines, and more

The screenshot displays the E-Visor Teams App interface within a Microsoft Teams environment. The interface is divided into several sections:

- Microsoft defender for cloud apps:** Shows a 'Suspicious activity' count of 1.
- Office 365:** A summary table with the following data:
 

Initial access	Suspicious activity	Total Spams	Total SPoilers	Total malware	Total high confidence phishing	Total Transport rules
8	1	339	1	3	6	1
- My known incidents:** A table listing various security incidents with columns for ID, Name, Severity, Categories, Impact, Impact on devices, Status, Assigned to, Service source, Detection source, Classification, Determination, Auto remediated, First activity, and Last activity.

The 'My known incidents' table contains the following data:

ID	Name	Severity	Categories	Impact	Impact on devices	Status	Assigned to	Service source	Detection source	Classification	Determination	Auto remediated	First activity	Last activity
311	Multi-stage incident involving initial access & Discovery on multiple endpoints	High	Persistence, Execution, Discovery, Initial access, Collection, Defense evasion, Malware, Unwanted software	1 impacted device 1 impacted user	1 impacted device 1 impacted user	Active	Service desk	Microsoft defender for endpoint	Windows defender av	Unknown	Not Available	-	Mar 29 2022, 20:03:48	May 20 2022, 13:05:31
341	Email reported by user as malware or phish	Low	Initial access			Resolved	Service desk	Microsoft defender for office 365	Office x ip	Unknown	Not Available	-	Apr 05 2022, 16:54:50	Apr 05 2022, 16:04:57
350	'Rundll32bin' malware in a command line was prevented from executing on one endpoint	Informational	Malware	1 impacted device 1 impacted user	1 impacted device 1 impacted user	Resolved	Service desk	Microsoft defender for endpoint	Windows defender av	Unknown	Not Available	-	Apr 07 2022, 15:04:56	Apr 07 2022, 18:34:54
352	Unauthorized cloud app access was blocked on one endpoint	Informational	Suspicious activity	1 impacted device	1 impacted device	Resolved	Service desk	Microsoft defender for endpoint	Customer i	Unknown	Not Available	-	Apr 07 2022, 16:04:23	Apr 07 2022, 17:34:36
365	DLP-Cred	Medium	Suspicious activity			Active	Service desk	Microsoft defender for office 365	Office x ip	Unknown	Not Available	-	Apr 13 2022, 15:04:54	Apr 13 2022, 15:04:55
368	Suspicious activity incident on one endpoint	Medium	Persistence, Execution, Initial access, Discovery, Collection	1 impacted device 1 impacted user	1 impacted device 1 impacted user	Active	Service desk	Microsoft defender for endpoint	Windows defender av	Unknown	Not Available	-	Apr 26 2022, 19:04:59	Apr 26 2022, 22:04:15
373	User and IP address reconnaissance (GME) on one endpoint	Medium	Discovery	1 impacted device 1 impacted user	1 impacted device 1 impacted user	Active	Service desk	Microsoft defender for identity	Azure x ip	Unknown	Not Available	-	May 09 2022, 16:04:70	May 20 2022, 13:05:14
430	[Teal.Alert] Suspicious Powershell commandline on one endpoint	High	Discovery, Suspicious activity, Malware, Execution	2 impacted device 2 impacted user	1 impacted device 1 impacted user, server	Active	Service desk	Microsoft defender for endpoint	NT ip	Unknown	Not Available	-	May 10 2022, 14:05:59	Jun 03 2022, 16:04:61

## Custom actions for end-user, managers, and IT admin experience

The screenshot displays the E-Visor Teams App interface within a Microsoft Teams environment. The main window shows a list of 'My known incidents' with columns for Id, Name, and Severity. An incident with Id 549 is highlighted, showing a 'High' severity level and a description: 'An active 'Rundll0lBin' malware in a command line was prevented from executing on one endpoint'.

An 'Impacted devices' modal window is open, displaying a table of devices affected by the incident. The table includes columns for Device name, Risk score, Health status, Defender status, Onboarding status, First seen, Platform, Build, Version, and Action. A custom actions menu is visible over the table, listing several options:

- Select scan...
  - Quick scan antivirus
  - Full scan antivirus
  - Isolate machine full
  - Isolate machine selectiv
  - Release from Isolation
  - Restrict app execution
  - Remove app restriction

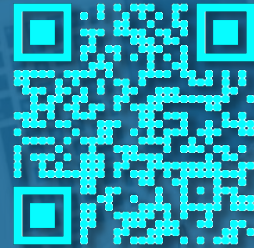
The interface also shows a 'Security' tab with 17 alerts and a 'Business' tab. The bottom of the screen displays the copyright information: © 2022 - Synergy Advisors LLC. Version 2.4.105.



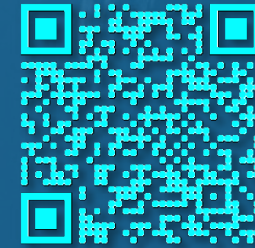
# Learn more about us



Consulting services



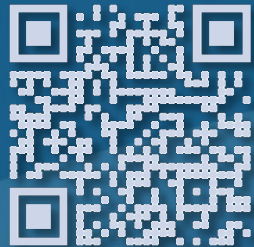
E-Suite solutions



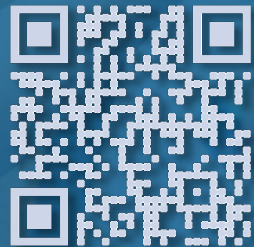
Managed services



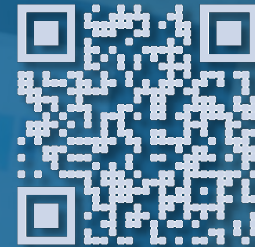
E-Visor



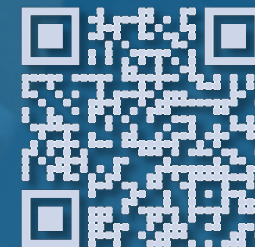
E-Visor Teams App



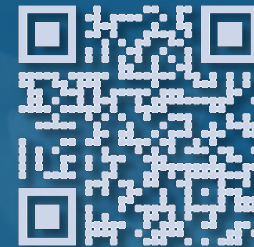
E-Inspector



E-Cryptor



E-Migrator



E-Vigilant

Thanks!



Follow us...



Synergy Advisors



Synergy Advisors



Synergy Advisors LLC



@SynergySEC



@Synergyadvisors