XDR - Synergy Advisors for Managed Services SOC

Synergy Advisors

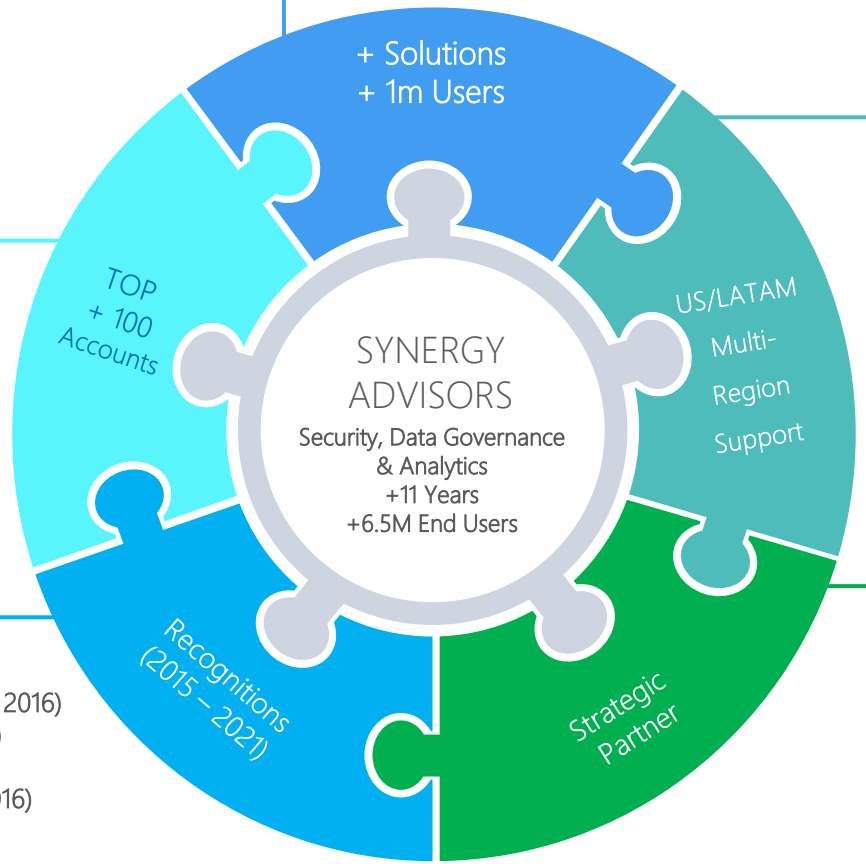
Overview

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

CONSULTING

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



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

E-Suite
SYNERGY ADVISORS

E-Visor

Enterprise-wide analytics

- Adoption and security correlated insights
- Configuration best practices
- Licensing usage and activity

E-Cryptor

- Document lifecycle management
- Self-service document access request
- Advanced collaboration
- Application integration

E-Inspector

- Data at rest content inventory and inspection
- Business and compliance driven data labeling and protection
- General alerts

E-Vigilant

- Advanced security and usage alerts and notifications
- Workflow based + E-Bot
- Business and technical incident management

E-Migrator

- Assess, discover, and analyze past and future meetings
- Zoom to Teams [Z2T] phased migration

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

SYNERGY ADVISORS

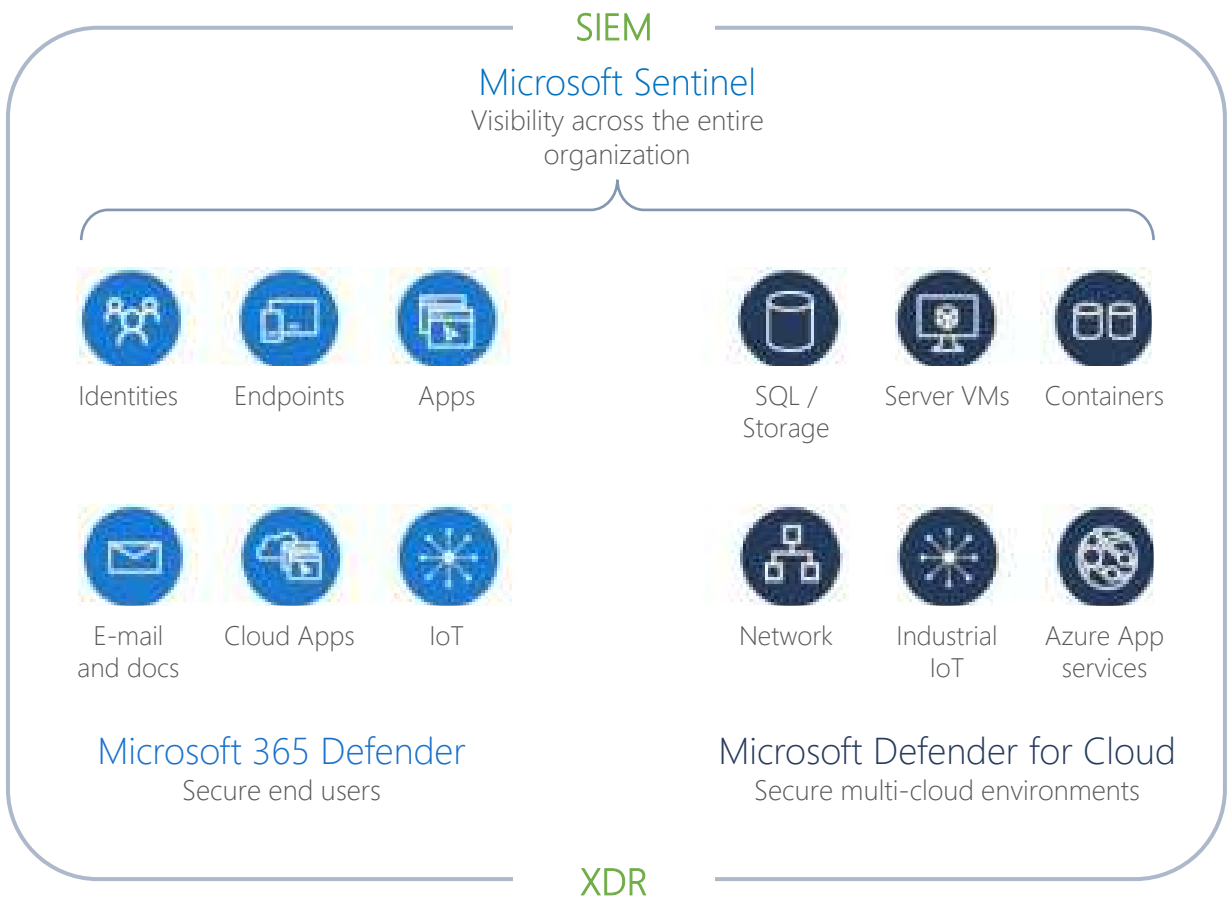
XDR - Synergy Advisors for Managed Security Services

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 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 Triaged
- ☐ 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.

Enhance and extend Microsoft solutions, providing a single pane of glass to centralize and manage alerts and notifications across different Microsoft platforms

Collect M365 data and correlate it with additional data sources, such as Active Directory, to provide rich reporting

Democratize information, involving end users within the organization through visibility into their use and configuration of M365 services

Monitor, hunt, and respond to help mitigate possible attacks and to optimize the security posture across the organization

ONBOARDING AND ADOPTION OF MICROSOFT SECURITY CAPABILITIES AND SOLUTIONS

Identities
Microsoft Defender for Identity

Endpoint
Microsoft Defender for Endpoint

Apps and cloud apps
Microsoft Defender for Cloud Apps

E-mail and docs
Microsoft Defender for Office 365

SIEM
Microsoft Sentinel

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

XDR + E-Visor Teams App for Managed SOC Services

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.

- Security
- Productivity
- Identity Governance
- Threat Protection

- 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 + Teams

End User – Manager – IT Experience

XDR Services & Solutions = Security + Modern Work

Additional info: Link

Offering overview: Link

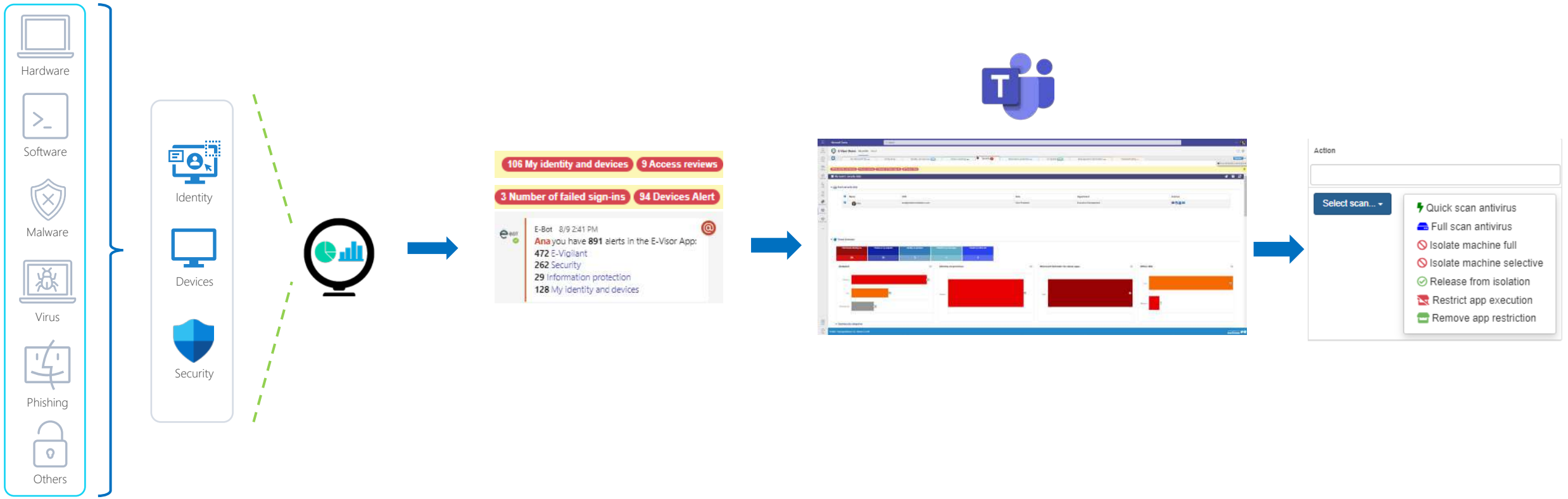
How does 'XDR + E-Visor Teams App' work?

Workloads analysis by E-Visor Teams App

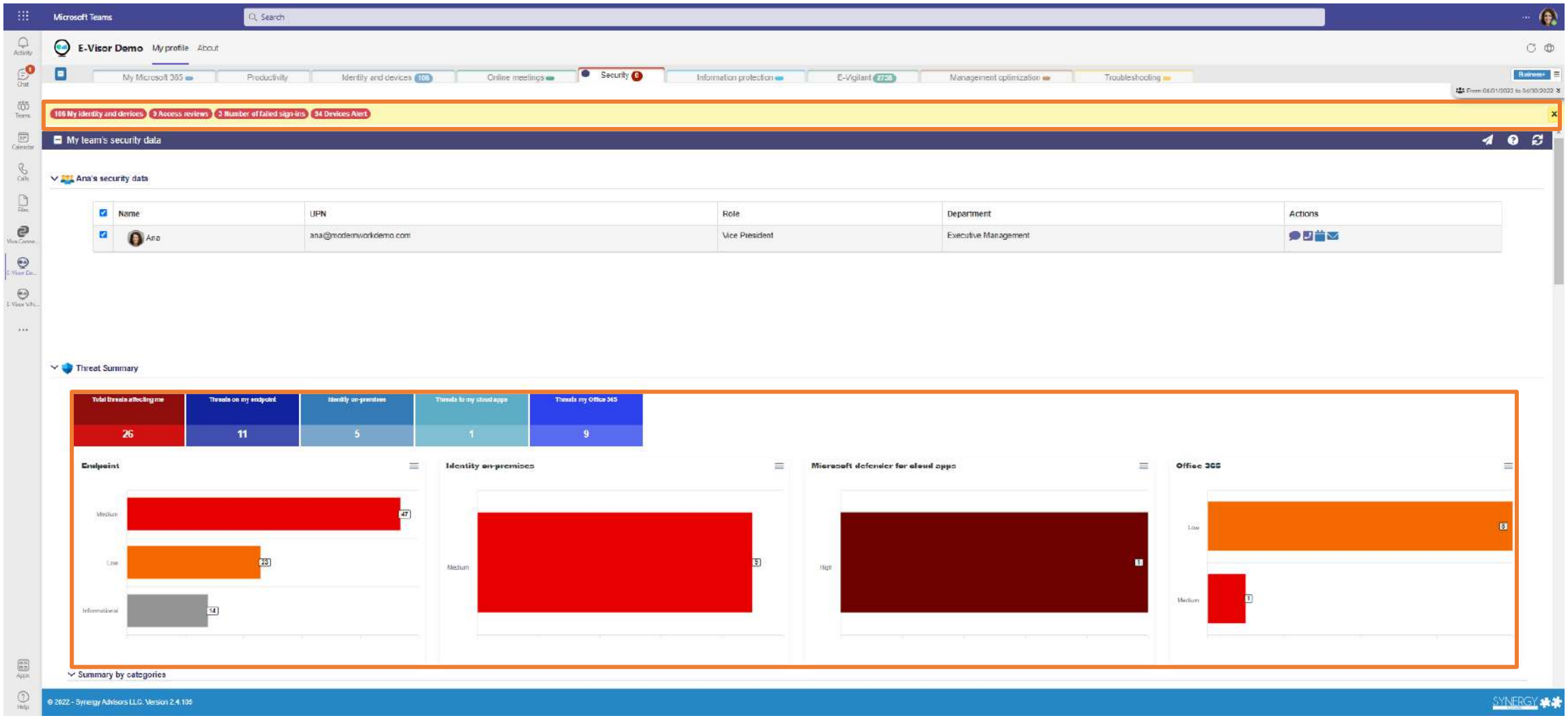
Alerts and notifications

App views by E-Visor Teams App

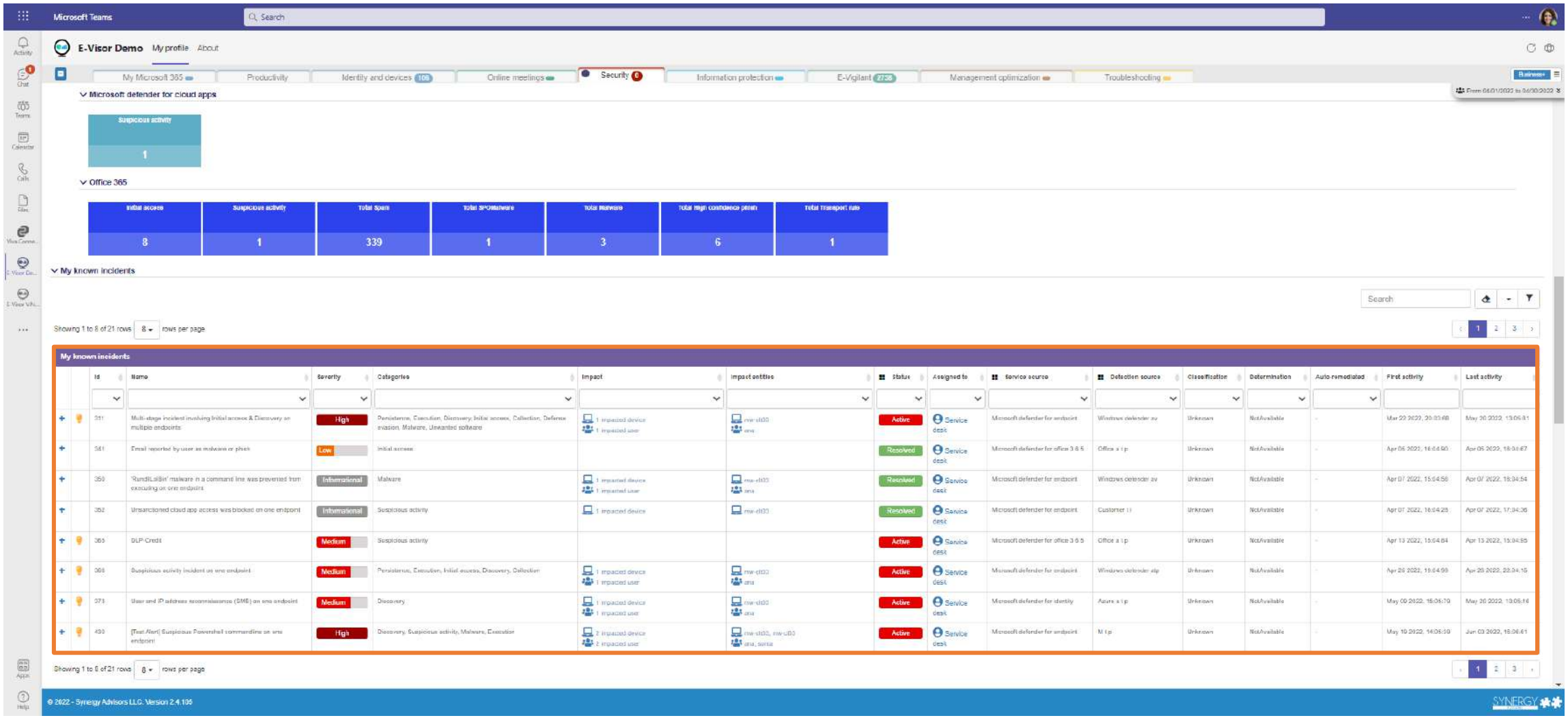
Custom actions



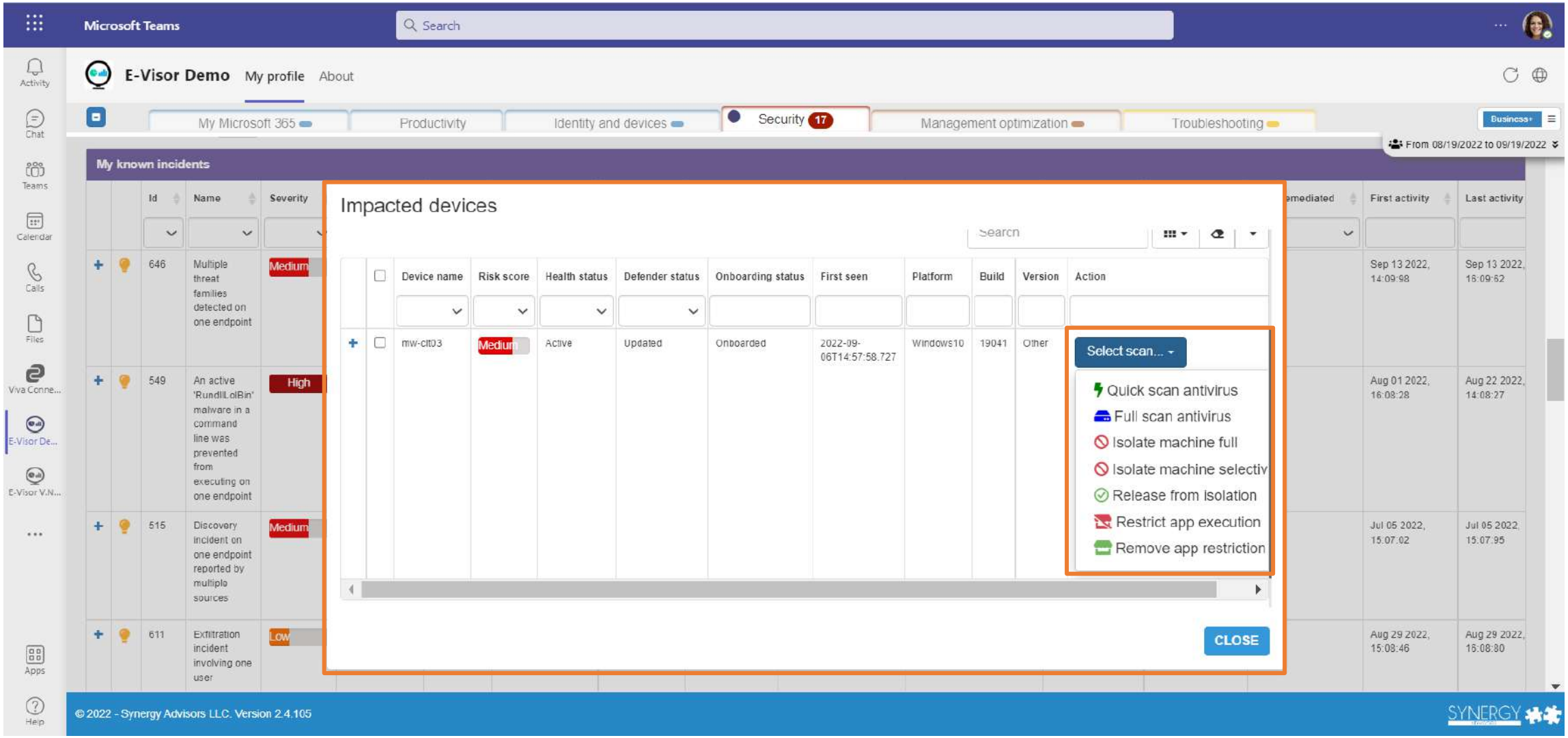
Centralized events collected by Defender platforms



Incidents information such as users, impacted machines, and more



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



SYNERGY ADVISORS

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!

SYNERGY ADVISORS

Follow us...

Synergy Advisors

Synergy Advisors

Synergy Advisors LLC

@SynergySEC

@Synergyadvisors