XDR - Synergy Advisors for Managed Security Services

SYNERGY ADVISORS

eXtended Detection and Response

Cyberattacks have become one of the most important challenges that organizations face with many fronts to defend. Individuals or organizations conduct cyberattacks with business, political, criminal, or personal intent to destroy or gain access to systems and classified information.

U.S. Office of Personnel Management

$21.5 Million

... it cost the organization under investigation, due to the theft of 5.6 million fingerprints. "One of the most significant data breaches in U.S. history".

Equifax

147.9 Million

... customers in the US, UK, and Canada had credit card and social security numbers stolen due to an unpatched vulnerability.

Russian Cyberattacks

+58%

... of all cyberattacks observed by Microsoft have been attributed to hackers in Russia, at stealing data from other countries with a 32% success rate in 2021.

Most common cyberattacks

- Malware
- Distributed Denial of Service (DDoS)
- Phishing
- SQL Injection Attacks
- Cross-Site Scripting (XSS)
- Botnet networks
- Ransomware

What is eXtended Detection and Response (XDR) and how does it help mitigate cyberattacks?

XDR is a solution based on MICROSOFT 365 DEFENDER that automatically collects, correlates, and analyzes signal, threat, and alert data from across the Microsoft 365 environment, endpoints, servers and multiple loads in Azure. It leverages artificial intelligence (AI) and automation to automatically stop attacks and remediate affected assets to a safe state.

XDR is the next step in security, unifying protection:

- Endpoint
- E-mail
- Applications
- Identities

How to take advantage of the capabilities and benefits of XDR?

Synergy Advisors' Managed Security Services

Synergy Advisors provides managed services using comprehensive and robust tooling built into the Azure platform for managing customer tenant activity across identities, endpoints, applications, information, network, and more, with a multi-tenant methodology that enables scalability, higher automation, and enhanced governance.

Extended, Detection, and Response strategy that provides 24/7/365 Managed SOC Services, across Microsoft unified SecOps stack.

Monitoring, hunting, and response

Customer
• Detection • Response • Remediation

Synergy Advisors' SOC Services > Protect organization against cyberattacks

Investigation of potential incidents

- □ Alerts Optimization
- □ SOC Analysis
- □ Incident Investigations

Triage, prioritization and detection of incidents

- □ Incident Triaged
- □ Incident Prioritized
- □ Incident Optimized

Coordination of incident response

- □ Microsoft Tools and Technologies
- □ Identification and Remediation

Maintenance of relevance

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

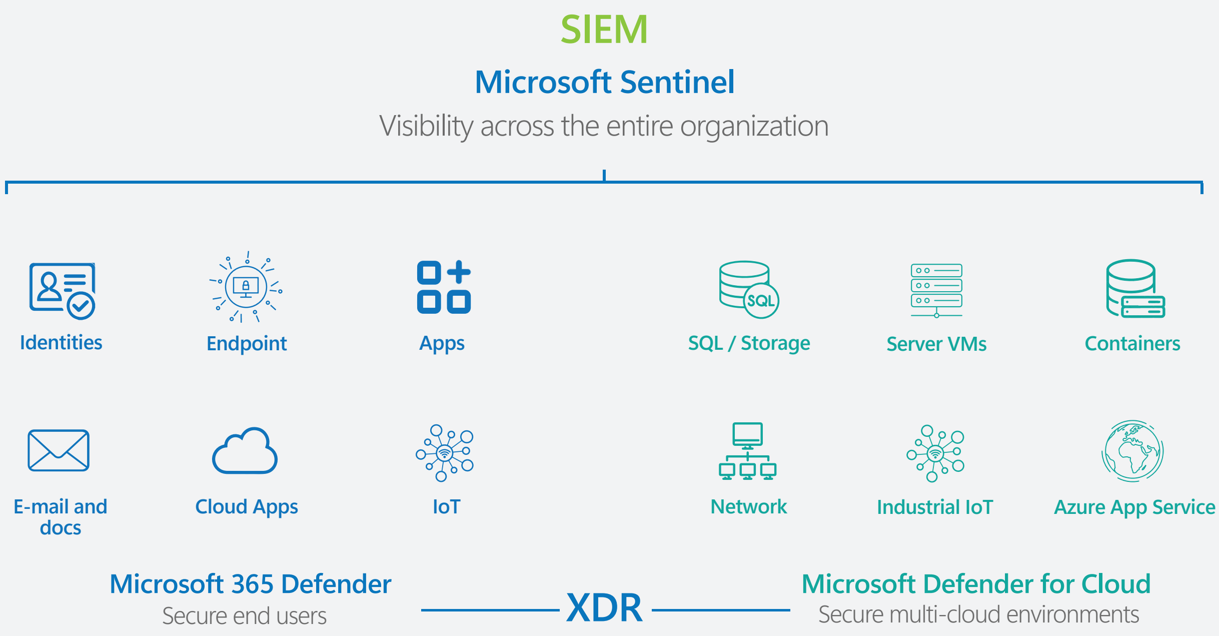
Patching of vulnerable systems

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

Infrastructure management

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

Leveraging Microsoft technologies and capabilities



SIEM

Microsoft Sentinel

Visibility across the entire organization

Identities

Endpoint

Apps

SQL / Storage

Server VMs

Containers

E-mail and docs

Cloud Apps

IoT

Network

Industrial IoT

Azure App Service

Microsoft 365 Defender

Secure end users

XDR

Microsoft Defender for Cloud

Secure multi-cloud environments

What can you get from our Managed Security Services + XDR?

Monitoring, hunting, and response

- 24x7x365 incident monitoring across Microsoft Security Solutions
- End to end incident management and resolution (it includes solving 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 users, and delete or block e-mails)

Security-driven integrations

- Incident data for management and control of devices using Microsoft Security solutions such as MEM, MDE, MDI, MDO, MDCA), and others.
- Advanced hunting investigation performed with proprietary, and SIEM solutions.
- Customized detection based on customer's needs for hunting and detection queries leveraging Microsoft 365 operations
- Manual and/or automatic response actions by leveraging Microsoft 365 Defender portals, using APIs and Synergy Advisors solutions

Onboarding and posture management

- Synergy Advisors supports onboarding and adopt of invested Microsoft solutions to strengthen the 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

Go beyond with E-Visor Teams App for Managed Security Services + XDR!

E-Visor Teams App is a reporting and analytics app that **helps end users 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 and take actions on security incidents.

Synergy Advisors extends across the Microsoft unified SecOps stack and includes different integration 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 Microsoft 365 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 Microsoft 365 services

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

ENHANCE THE SECURITY POSTURE WITH MICROSOFT SECURITY SOLUTIONS

Identities

Microsoft Defender for Identity

Endpoint

Microsoft Defender for Endpoint

Apps and cloud apps

Microsoft Defender for Cloud apps

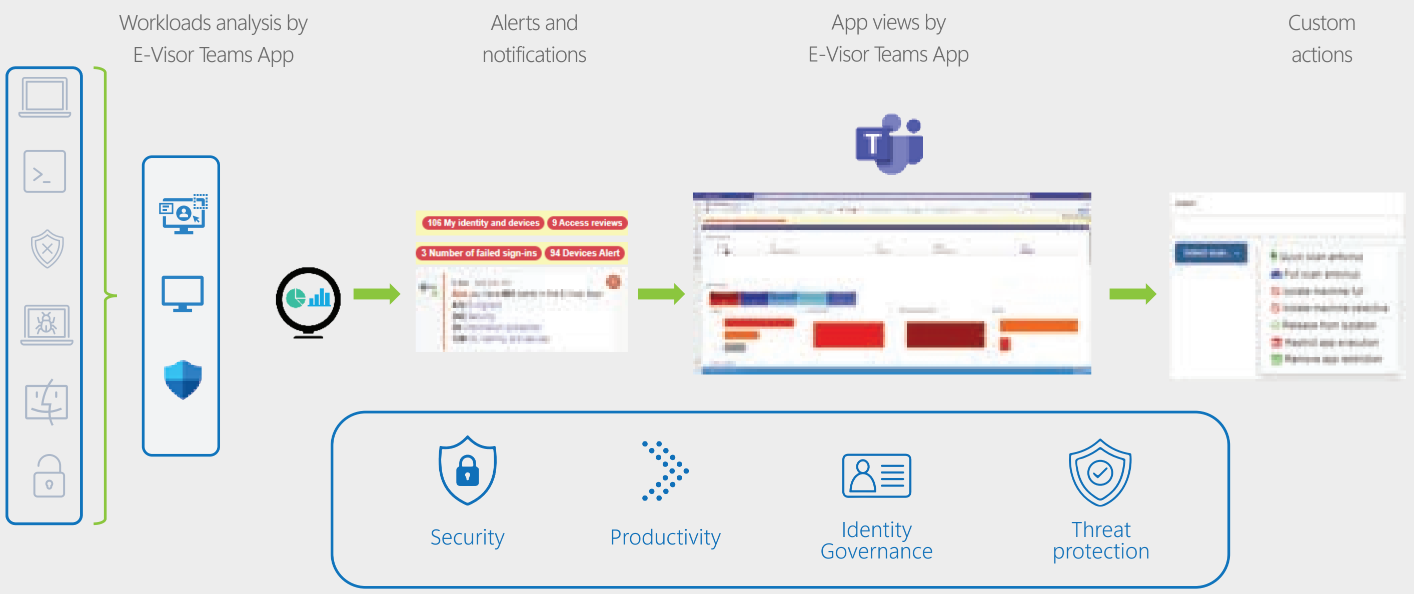
E-mail and docs

Microsoft Defender for Office 356

SIEM

Microsoft Sentinel

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



Highlighted features

- 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: individualized depending on customer needs and scenarios; it can include advanced hunting custom detection queries and custom indicators added to the system through Microsoft 365 portals or APIs
- Perform manual & automatic response actions
- Training/readiness, setup, onboarding, adoption and ongoing monitoring, response, and management services

E-Visor Teams App

XDR services and solutions = Security X + Modern work X

Contact us to get a quote for your organization's needs HERE

E-mail us and get a free consulting session:
ww-marketing@synergyadvisors.biz

SYNERGY ADVISORS