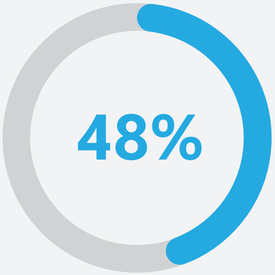
SYNERGY ADVISORS

E-Vigilant

Advanced security **incident management** and **analytics**

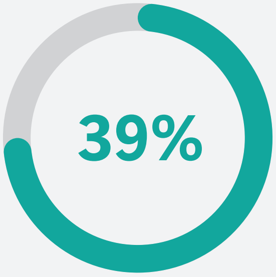
Proactively manage security incidents with advanced alerts, notifications, and workflows.

Organizations are spending more on cybersecurity resources to improve their defenses and working harder than ever to integrate security through design. Despite the high attention to cyber incidents in recent years, many organizations worldwide still struggle to understand and manage emerging cyber risks in an increasingly complex digital society.



of companies do not have training programs for employees on information security threats.

Global State of Information.
EY



... of organizations have been affected by a cyber incident in the past two years, and other 6% do not know.

Global Cybersecurity Outlook 2022.
WEF

... is the average first response time to a ticket, for an average of 1500 tickets per month, resulting in reduced productivity.

The Zendesk Benchmark.
Zendesk

Primary Concerns of Organizations

- Malware
  Malware and security threats
- Poor device management
- Non-compliance with internal policies
- Unconnected security and IT efforts
- E-mail Security

What is E-Vigilant and how does it help mitigate security risks?

E-Vigilant is an advanced analytics and alerting solution that uses Microsoft solutions to COLLECT information from different sources (workloads), ALERT different audiences to different types of incidents, provide a comprehensive VIEW OF THE CYBERSECURITY ecosystem, and facilitate more EFFECTIVE MANAGEMENT.

E-VIGILANT EXTENDS MICROSOFT SOLUTION CAPABILITIES

Identities
Microsoft Defender
for identity

Endpoints
Microsoft Defender
for endpoint

Apps & Clouds Apps
Microsoft Defender
for cloud apps

E-mail & Docs
Microsoft Defender
for Office 365

Microsoft Purview Information Protection

Microsoft Entra ID

Microsoft Intune

Common security issues

- Lack of communication between the IT and security teams.

- Loss of productivity and high costs from incident management of the IT department.

- High number of false positives.

- Many unattended incidents, due to lack of alerting and reporting.

How E-Vigiliant solves them

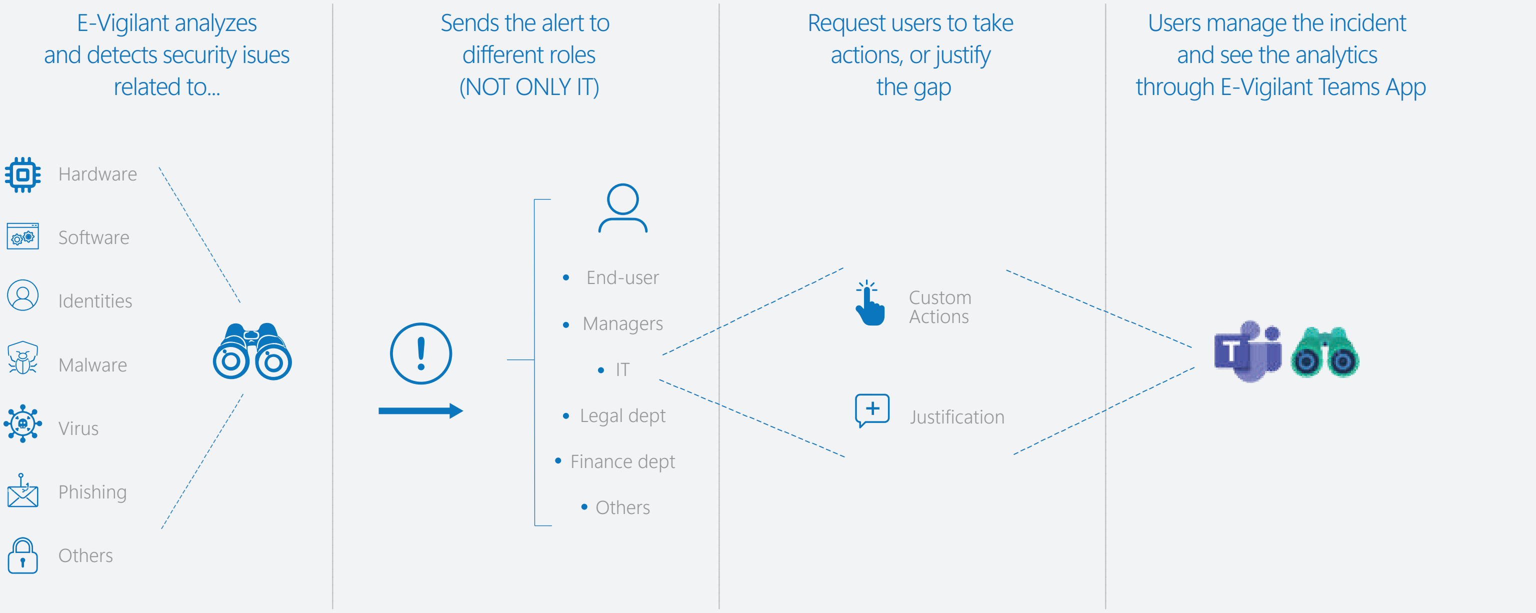
- E-Vigilant provides a single and complete view of the cybersecurity ecosystem, connecting IT and security efforts in a single console.

- Cost and time reduction by optimizing and automating incident management.

- Provides traceability of incidents to manage them effectively and focus on what is really important. Not everything is a threat!

- Optimizes and automates alerts that extend beyond the IT department, to accelerate response.

How does E-Vigilant work



E-Vigilant analyzes and detects security isues related to...

Sends the alert to different roles (NOT ONLY IT)

Request users to take actions, or justify the gap

Users manage the incident and see the analytics through E-Vigilant Teams App

Find out about

- Malware and virus threats
- Identity theft risks
- Successful and unsuccessful access to protected documentation
- Detect the misuse of sensitive information
- Quarantined e-mails

Benefits

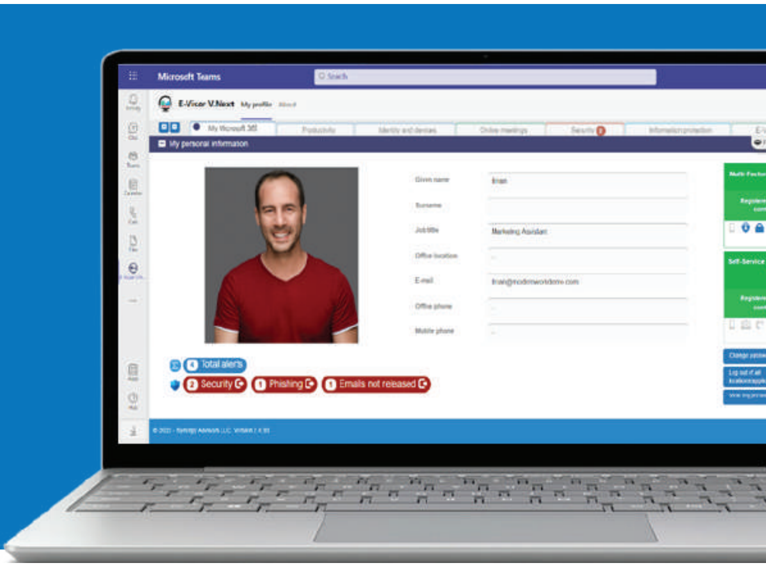
- Advanced alerts and notifications
- Incident management
- Mitigate security risks
- Optimized alert management process
- Homogenization process

Main features

- Automation with flows
- Risk mitigation
- Real-time alerts
- BOT interaction
- Integration with Microsoft Teams
- Integration with other platforms, such as Service Now and Dynamics 365

Built into Teams, E-Vigilant enables **users to play a part** in security incident management by providing them with the necessary **context to easily surfaces real incidents** while clearly **flagging false positives, reducing time and costs** in an optimized and **automated process**.

Workflow-based notifications and actions = Security + Modern Work



Microsoft Teams

E-Vicor V.Next My profile

My Microsoft 365

My personal information

Given name: Brian
Surname:
Job title: Marketing Assistant
Office location: -
E-mail: brian@modernworkdemo.com
Office phone: -
Mobile phone: -

4 Total alerts
2 Security
1 Phishing
1 Emails not released

E-Vigilant Coverage Workloads

Identity

- Identity theft risks
- Risky sign-ins
- MFA configuration
- Access packages [Identity governance]

Devices

- Devices out of compliance
- Uncompliant devices
- Unhealthy devices
- Device with risks

Security

- E-mail reported by users as malware or phishing attempts
- OD4B - malware detection
- Unusual volume of file deletion
- User and IP address reconnaissance (SMB)

Information Protection DLP

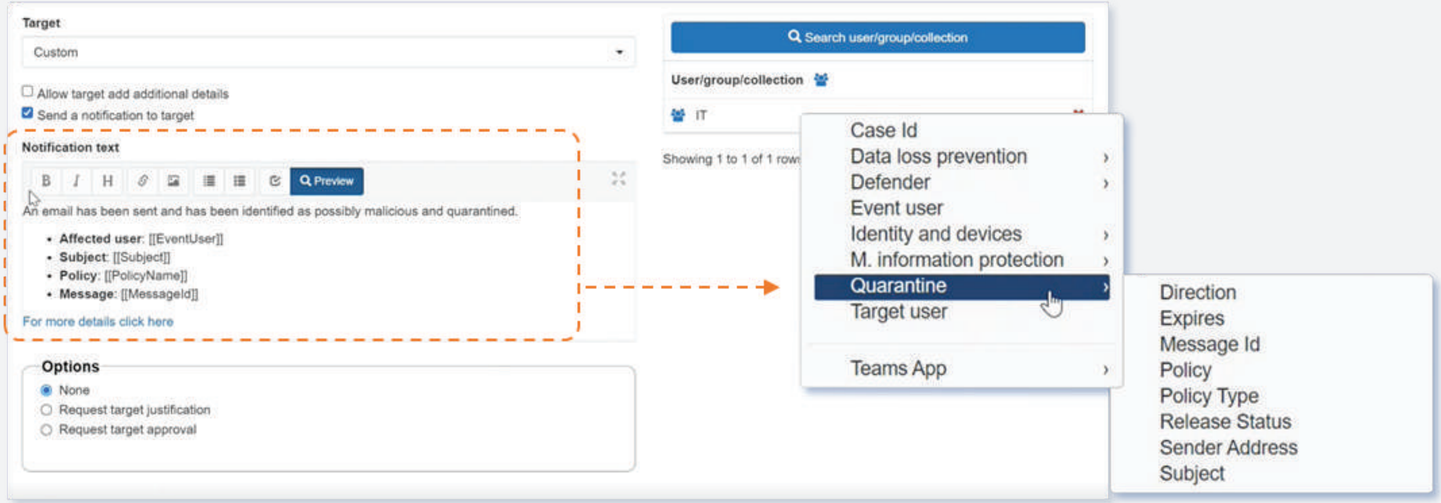
- Access time control
- Block access
- Notification of DLP violations
- Policy override
- Protection policy match
- Subscription errors

Information Protection Documents

- Classify documents
- Discover sensitive information
- File change protection
- File classification removed
- File was classified

Alerts and notification

Customizable notification messages



Target

Custom

□ Allow target add additional details

☑ Send a notification to target

Notification text

An email has been sent and has been identified as possibly malicious and quarantined.

- **Affected user**: [[EventUser]]
- **Subject**: [[Subject]]
- **Policy**: [[PolicyName]]
- **Message**: [[MessageId]]

For more details click here

Options

● None

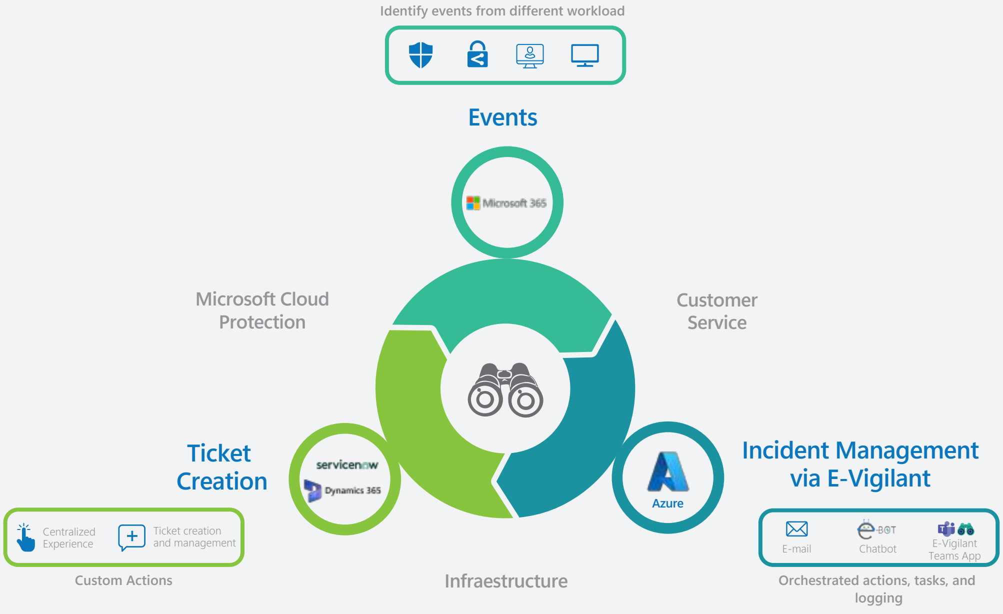
○ Request target justification

○ Request target approval

Orchestrated actions, tasks, and logging from different channels

E-Vigilant integrations with Dynamics 365 and ServiceNow ticket platforms

Centralized incident and support management for Microsoft 365


Identify events from different workload

Events

Microsoft 365

Microsoft Cloud Protection

Customer Service

Ticket Creation

servicenow

Dynamics 365

Azure

Incident Management via E-Vigilant

Centralized Experience

Ticket creation and management

Custom Actions

Infraestructure

E-mail

BOT Chatbot

E-Vigilant Teams App

Orchestrated actions, tasks, and logging

E-Vigilant in action!

Business-driven notification

- Notify the right people
- People involved in the incident
    - End user
    - Management/Upper Management
    - Technology and business

Business-driven actions

- Workflow-based alerts and notifications
- SLAs
- Actions to be performed based on impact
- Enforcement
- Escalations

Seamless user experience

- Centralized user notifications via Teams
- Centralized administrator view via E-Visor/E-Visor for Teams*
- Viva Connections - Sharepoint

About Synergy Advisors

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

Threat Protection

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

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