# **Endpoint Detection and Response**

Microsoft Defender Managed Services is your managed cloudbased security solution that leverages enterprise various security platforms (including Sentinel, Defender for Endpoint & Defender for Cloud) designed to help enterprise networks prevent, detect, investigate, and respond to advanced threats.

## What We Offer

We enhance security with integrated services leveraging Microsoft Defender for Endpoint, Cloud and Sentinel.

Endpoint behavioral sensors: Collect and process behavioral signals.

**Cloud security analytics:** Translate signals into insights, detections, and recommended responses.

**Threat intelligence:** Identifies attacker tools, techniques, and procedures. Extended Defender Managed Services offer setup review, policy configuration, threat analysis, and attack response, reducing the security burden on IT and security teams.

Additionally, integration with Eviden MDR enhances risk response, reducing error rates by up to 40% with shorter MTTD and MTTR.





# **Endpoint Detection and Response**

## **How it Works**

Extended Defender Managed Services is a full cloud service. The cloud infrastructure is based on software and technology innovations that improve the environment. The main considerations are a strong carbon footprint reduction versus the onpremises infrastructure and efficient energy usage. The solution is composed of endpoint, cloud security and Sentinel that can be additionally enhanced with Eviden MDR.

## **Execution Strategies and Solutions**

#### First line of defense

Traditional endpoint protection cleans known malware before seen in EDR Service

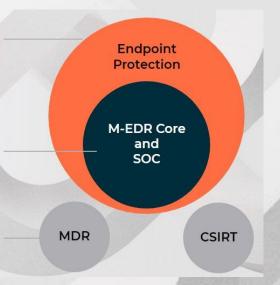
#### Second line of defense

- Core provides new generation of prevention features filling the gap left by legacy antivirus solutions that primarily focus on malware
- Triage of alerts generated by the managed endpoint detection core with a goal to identify true positives and provide analysis and mitigation recommendations

#### Kernel

MDR (threat intelligence and hunting) and CSIRT based on M-EDR information

More focused investigations thanks to layered approach



# **Endpoint Detection and Response**

## **Customer Outcomes**

Auto investigation and remediation

Attack surface reduction

Protect endpoints & cloud in the organization

## **Customer Success**

Company: The Government sector in the Netherlands

#### Solution:

- Threat protection
- Microsoft Defender for Endpoint (Microsoft Defender Antivirus and Microsoft Defender Endpoint Detection and Response EDR)
- Security Management
- Monitoring, reacting & reporting

### Impact:

- Strengthen and maintain the security posture of Azure cloud servers
- Configure antivirus protection for servers against antimalware threats
- Defender for Linux as a new, rapidly developing antimalware solution for Linux



Eviden is your preferred digital, cloud, data, and security partner to help you realize your digital future. Together, Microsoft and Eviden are expanding the possibilities of data and technology, now and for generations to come.

