

The EDR Revolution and Its Challenges

The shift from endpoint protection (EPP) to Endpoint Detection and Response (EDR) was prompted by the increasing sophistication of cyber threats and expanding attack surface. EDR solutions enable companies to detect and respond to complex attacks that EPP solutions could not prevent. However, EDR solutions pose their own challenges.

EDR solutions are simply not plug-and-play. They require a dedicated team to manage and perform tasks such as:

- Monitoring each low signal alert
- Enriching detection using telemetry from other solutions
- Defining response actions for each detection
- Investigating findings through related logs and alerts
- Optimising policies
- Reducing alert noise and prioritising what matters the most

Finding skilled EDR administrators or teams to handle such tasks is challenging. Therefore, it is advisable that organisations without access to such capabilities should continue using EPP. Investing in EDR solutions without the necessary resources would be a misuse of the cyber budget.

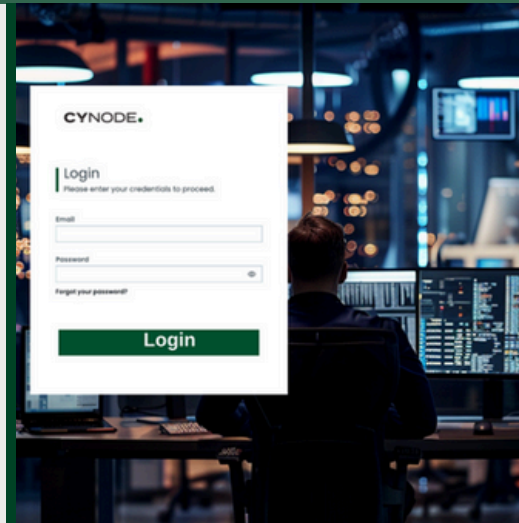
Cynode's MDR Service for Microsoft Defender: Journey to eXtended Detection and Response

Cynode's Detection and Response Service for Microsoft Defender enhances and extends the capabilities of our customers' existing Microsoft Defender investments. It provides unified pre and post breach detection and response against any threats impacting endpoint, identity, email, and application assets. The service not only tackles detection and response but also enhances the prevention capabilities of Microsoft Defender suite through policy guidance.

Cynode's Workspace Security Analytics and Ultima Threat Exposure Platforms play key roles in detecting, responding to, and validating and hardening EDR solutions. Cynode offers a customer portal within its Workspace platform to provide access to information such as the number of alerts and cases, the MITRE ATT&CK heat map, affected assets, and communication between key stakeholders.

Benefits

- Make sure that your Microsoft E5 License and Defender investment is not under utilised.
- Benefit from 24/7 endpoint security monitoring, threat detection, and incident response capabilities, ensuring constant vigilance and timely responses to emerging cyber threats and security incidents.
- Reduce cyber risk with comprehensive detection and response for threats targeting endpoints, identities, emails, and applications
- Proactively address cyber threats before they escalate into significant security incidents or data breaches, minimising the impact on business operations and reputation.
- Utilise a high-quality service delivered by experienced cyber security professionals using your OPEX budgets.
- Enhance your security posture by using insights from detected incidents.



Microsoft Defender at a Glance

Defender is Microsoft's enterprise defence suite that coordinates detection, prevention, investigation, and response across endpoints, identities, email, and applications to provide integrated protection against sophisticated attacks.

Microsoft Defender includes:

- Microsoft Defender for Endpoint
- Microsoft Entra ID Protection
- Microsoft Defender for Office 365
- Microsoft Defender for Cloud Apps

Microsoft Defender offers a variety of alert and incident types to identify (1) endpoint attacks, (2) mail attacks and (3) identity attacks.

Defender also identifies suspicious and abnormal activities occurring on SharePoint, OneDrive, Teams, and other Microsoft-related applications. Some indicators are:

- Suspicious sensitive data discovery.
- Large file review or downloads.
- Unusual or non-comply cloud applications usage.
- Excessive application consents.

How It Works

Onboarding Phase

Cynode's Managed Detection and Response for Microsoft Defender Service begins with a thorough on-boarding phase that includes:

- User posture analysis
- Device posture analysis
- Server posture analysis
- Policy benchmark
- Vulnerability Management
- Endpoint and server patch & posture update

The onboarding phase provides Cynode's security analysts with necessary insights into assets, policies, configurations, critical vulnerabilities, and misconfigurations across Microsoft Defender products. This phase aligns our technology and processes with each customer's environment, concluding with policy updates and a comprehensive remediation plan.

Detection Phase

Cynode's detection capabilities have been designed to bring out the synergies among endpoint, identity, email, and application components of Microsoft Defender. Consolidating alerts generated by Microsoft Defender into cases and identifying affected assets and threat entities, Cynode's Workspace Security Analytics engine applies detection rules and behaviour analysis to detect malicious behaviour and activities.

Combined capabilities allow Cynode to promptly investigate alerts accross endpoints, identities, emails, and applications and determine root cause, entry point, relevant breaches, and the scope of impact within the organisation. Each threat activity is reported by outlining the impact and displaying the targeted assets on the Workspace customer portal.

Each case is analysed encompassing all linked activities found in the relevant alerts and a full narrative of the attack is outlined. This not only helps in the response phase but also eliminates false positives.

The Cynode Workspace Platform provides case enrichment by pulling in evidence from all data sources within Microsoft Defender:

Identities with Microsoft Entra ID Protection:

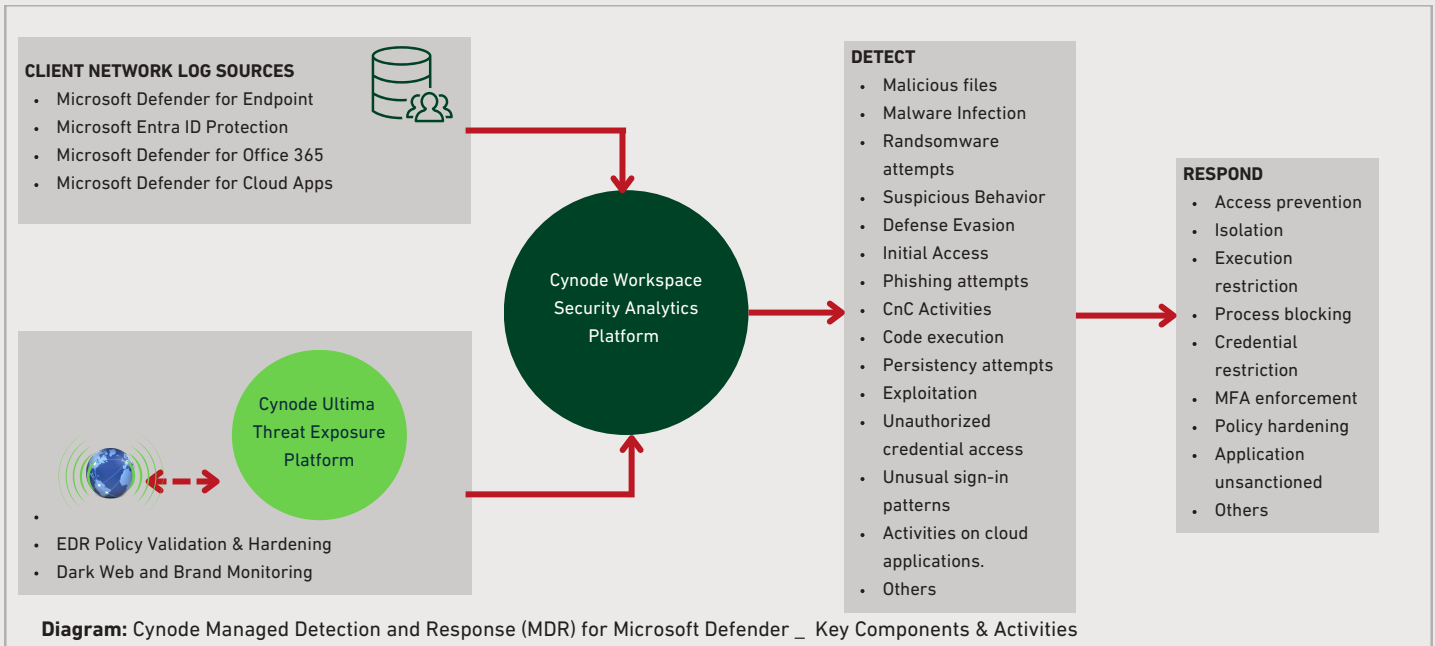
- Investigate the relevant user application and device suspicious logins to determine the unfamiliar sign-in properties.
- Identify the tactics and techniques used by the threat actor to impersonate or compromise the user account.
- Evaluate the devices involved in the incidents and identify any suspicious sign-in activity or unfamiliar processes.
-

Email and collaboration with Defender for Office 365 :

- Examine any malicious codes delivered in attachments or URLs that may potentially initiate a chained attack.
- Assess the scope of the incident instigated by malicious email activity that provided initial access.

Applications with Microsoft Defender for Cloud Apps (CASB):

- Identify any suspicious, anomalous, or extensive user behaviour on cloud applications, including Sharepoint, Onedrive and Teams.



Response Phase


Cynode coordinates incident response efforts across IT and security teams to ensure a unified and timely response to the security attacks. A response plan is agreed with a customer and Cynode Workspace Platform automates all the actions that can be automated. Some of the response actions are:


- Isolate the relevant endpoints.
- Block and limit sign-in of incident related users.
- Stop or block malicious services, processes or command line execution.
- Block and restrict the Indicators of Compromise (IOCs) identified from the relevant cases.
- Offer remediation plan such as applying patches, updating software.
- Unsanctioned non-compliant and risky cloud applications.


Cynode Workspace notifies the stakeholders with enhanced and verified content, providing guidance and support on list of mitigation actions.


Cynode Ultima Threat Exposure Platform’s EDR Policy Validation and Hardening service conducts a post-incident analysis to evaluate the effectiveness of response actions, identify lessons learned, and implement improvements to endpoint detection and response capabilities.


OTHER CYNODE MDR SERVICES


 Managed Detection and Response for Endpoint


 Managed Business Email Compromise Detection and Response

 Managed WebApp Exposure Monitoring

 Managed Detection and Response for Cloud

 Managed Phishing Detection and Response

 Managed Detection and Response for Identity Protection

 Managed Shadow IT Monitoring