CYNODE.

Managed Detection and Response (MDR) for Endpoint

Data sheet

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 a team of skilled EDR administrators is very challenging and organisations without this capability internally could continue using EPP. As investing in EDR solutions without the necessary resources could be considered a misallocation of the cyber security budget.

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

Cynode's Detection and Response Service for Endpoint enhances and extends the capabilities of our customers' EDR investments. The service provides unified pre and post breach detection and response against any threats impacting endpoint assets.

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 Workspace 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.

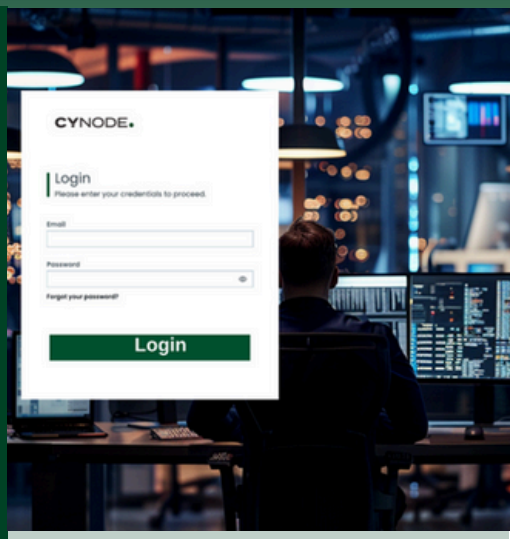
Customers have the option to add-on identity, email, and application-based analyses. If chosen, Cynode will gather alerts, incidents, and logs from these solutions and incorporate them into the service:

- Sign-in and access logs of IAM.
- Abnormal activity detection related to users and applications from the CASB solutions.
- Detection of malicious delivery and phishing attempts by Email Protection.

The service includes Cynode Ultima EDR Policy Validation and Hardening. This measures the readiness of an Endpoint Detection and Response (EDR) solution against real-world threats and attack scenarios. Furthermore, Ultima delivers vendor-specific detection content for optimised protection.

Supported EDR Technologies

Crowdstrike, Trellix, SentinelOne, Trend Micro, Cisco, VMWare Carbon Black, Broadcom. To enquire about other solutions, please get in touch with us at hello@cynode.com.



Benefits

- Make sure that your EDR 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.
- Minimise cyber risk with a holistic detection of and response to cyber 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 cybersecurity professionals using your OPEX budgets.
- Enhance your security posture using insights from detected incidents.

How It Works

Onboarding Phase

Cynode's Managed Detection and Response for Microsoft Defender Service begins with a thorough onboarding 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 on our customers' EDR technologies. This phase aligns our technology and processes with each customer's environment, concluding with policy updates and a comprehensive remediation plan.

Detection Phase

Cynode utilise endpoint detection and response (EDR) solutions to continuously monitor endpoint devices for suspicious activities, indicators of compromise (IOCs), and anomalous behaviour. Alerts are correlated into cases based on threat entities or targeted assets. Cases are prioritised according to severity, impact, and relevance to your organisation's security posture. The service utilises Workspace Platform's detection rules which are based on MITRE tactics and incorporate various techniques.

Cynode consolidates the threat signals received by EDR solution. It determines the full scope and impact, including how it entered the environment, the areas it affected, and its current impact on the organisation. These details can be accessed through 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 response phase but also eliminates false positives.

Cynode performs manual or automated review to incorporates additional evidence to elaborate a case that is triggered by one of the products:

- **Identity and Access Management (IAM)**
  - Investigate the relevant user application and device suspicious logins to determine the unfamiliar sign-in properties.
- **Identity Monitoring and Protection**
  - 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 Protection**
  - 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.
- **Cloud Access Security Broker (CASB)**
  - Identify any suspicious, anomalous, or extensive user behaviour on cloud applications, including email, collaboration, instant messaging, and file storage and sharing platforms.

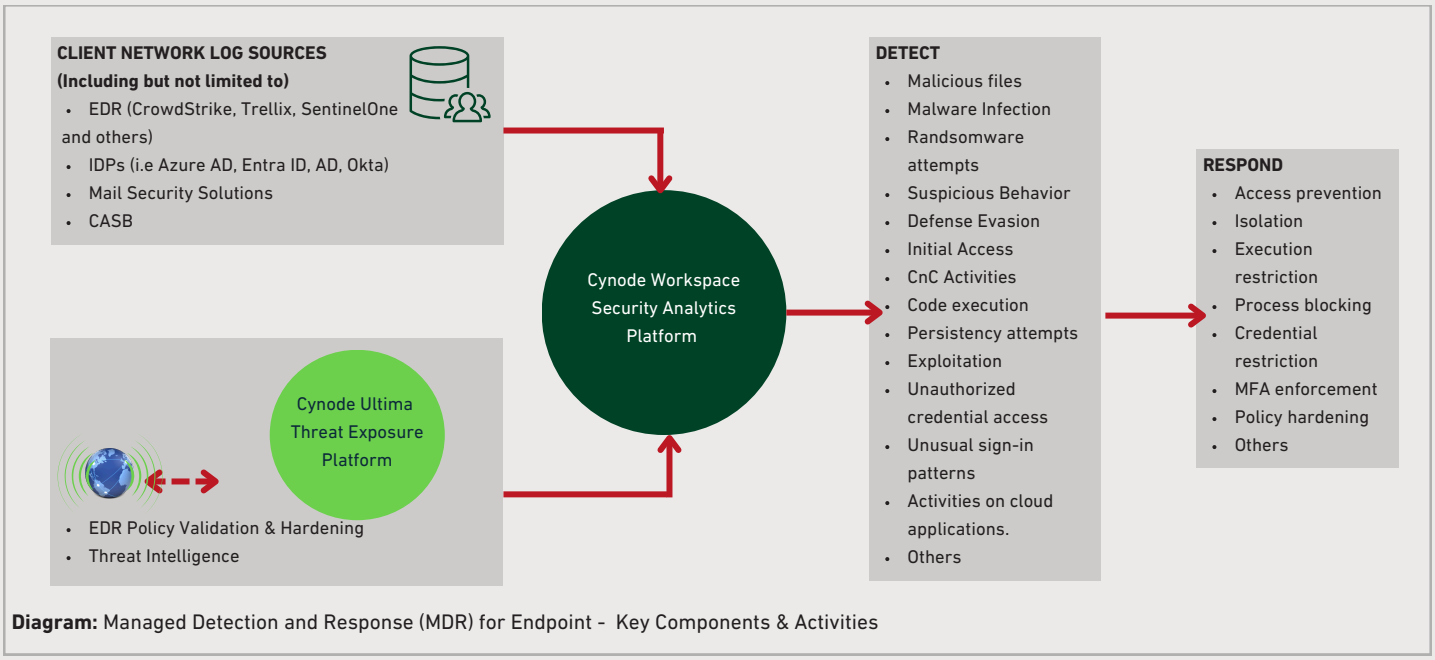


Diagram: Managed Detection and Response (MDR) for Endpoint - Key Components & Activities

Response Phase

Cynode coordinates incident response efforts across IT and security teams to ensure a unified and timely response to the security attacks. Cynode Workspace Platform provides response plan with customer negotiated automated actions that include the following Workspace playbooks:

- 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 incident.
- Offer remediation plan such as applying patches, updating software.
- Unsanction 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 Microsoft Defender
- Managed Detection and Response for Cloud
- Managed Business Email Compromise Detection and Response
- Managed Phishing Detection and Response
- Managed Shadow IT Monitoring
- Managed WebApp Exposure Monitoring
- Managed Detection and Response for Identity Protection