CYNODE.

# Microsoft Defender XDR Engineering

Make the most of your Microsoft Defender Security Suite

Datasheet

## Overview

The Cynode Microsoft Defender XDR Service delivers unified protection across **endpoints**, **identities**, **email**, and **cloud applications** — connecting security signals into one coordinated defense. Built natively into Microsoft 365, it empowers organisations to detect, investigate, and respond to threats faster with AI-driven correlation and automated response actions.

Defender XDR integrates seamlessly with existing Microsoft and third-party tools, ensuring broad coverage without added complexity. Its intelligent policies, shared telemetry, and automation workflows turn fragmented tools into a connected, proactive security framework.

- Up to 242% ROI*
- Lower operational overhead through consolidation
- Significant reduction in breach-related costs and downtime

***Forrester Total Economic Impact (TEI) (2025)***

Cynode's Managed Defender XDR service ensure Defender XDR is designed, deployed, and operated for measurable impact — aligning architecture, detection, and response with your operational objectives while driving continuous optimisation, efficiency, and resilience.

Microsoft Defender

CYNODE.

## Benefits of Cynode's Managed Microsoft Defender XDR

**1. Faster Time-to-Protection**
Rapid onboarding delivers full Defender XDR coverage and visibility across endpoints, identities, and email.

**2. Integrated Operations**
Unified incident management and analytics streamline investigations and strengthen cross-domain correlation accuracy.

**3. Operational Efficiency**
Automated triage, containment, and remediation reduce analyst workload and improve MTTD and MTTR.

**4. Cost & License Optimisation**
Continuous entitlement and telemetry reviews maximise Microsoft 365 investment and reduce total ownership costs.

**5. Sustained Risk Reduction**
Ongoing tuning and compliance alignment minimise exposure and maintain consistent security readiness.

**6. Business Continuity**
Faster detection and containment reduce disruption, protecting operations, revenue, and customer trust.

With Cynode, Microsoft Defender XDR becomes more than a protection suite — it evolves into an integrated defense fabric that delivers proactive detection, automation, and measurable resilience across your entire estate.

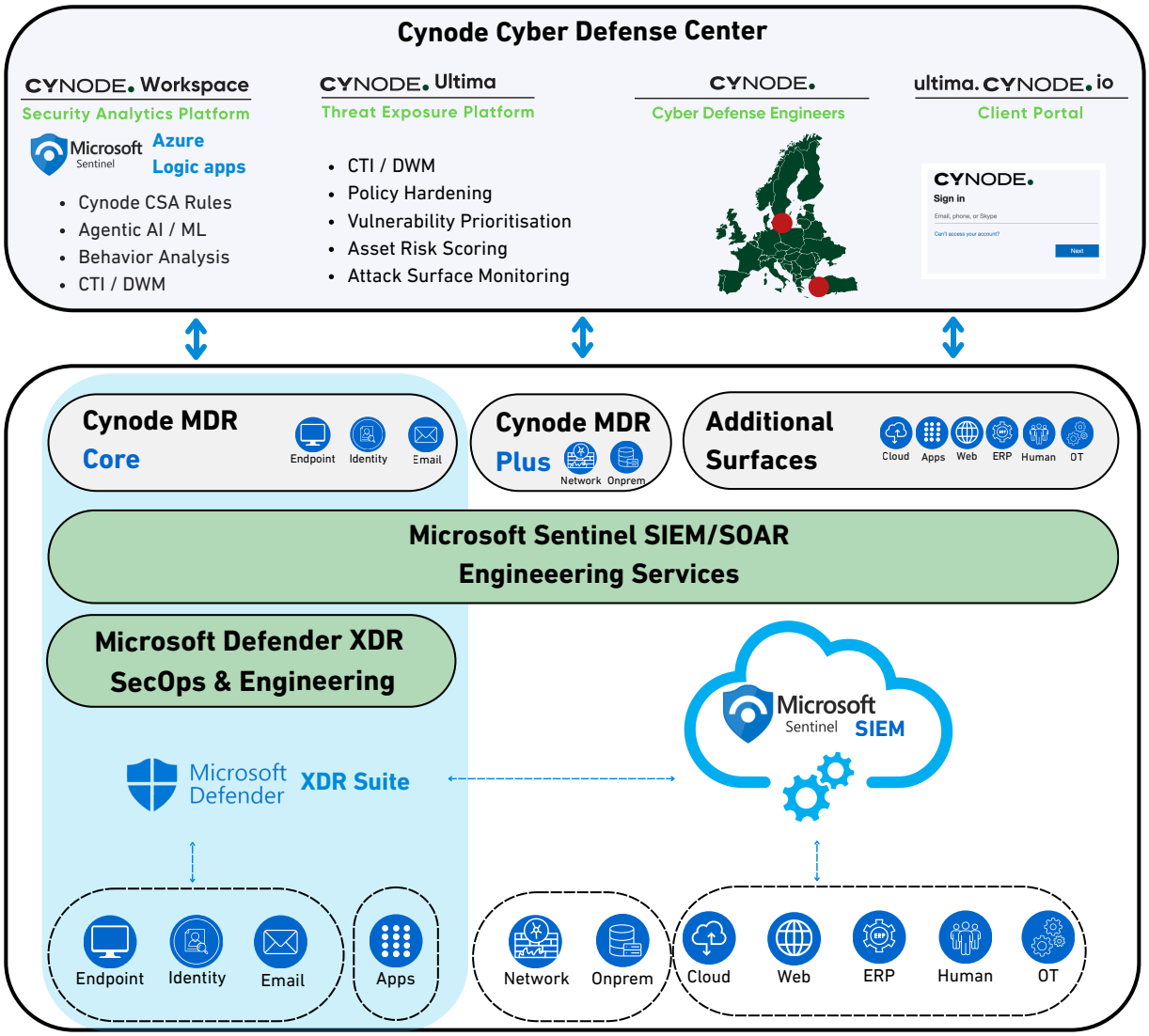
## The Cynode Methodology

**1 Design**
Build a Defender XDR architecture aligned with your real operational model, security priorities, and available response capabilities.

**2 Deploy**
Implement, configure, and validate the Defender XDR stack across your environment — integrated and ready for incident response.

**3 Optimise**
Tune Defender configuration, detection scope, and response pathways over time to stay aligned with changing risk and operational needs.

**4 Empower**
Empower your team — or your provider — with the knowledge, structure, and documentation to run Defender XDR securely and efficiently.



## Summary of the Scope

| Category | Outputs |
|---|---|
| **1. Architecture & Deployment Design** | End-to-end Defender XDR architecture design covering Endpoint, Identity, Office 365, and Cloud Apps. Entra ID tenant alignment, role-based access (RBAC/PIM), and coexistence planning with third-party tools ensure a scalable and conflict-free deployment. |
| **2. Policy & Control Optimisation** | Standardised policy baselines (AV, ASR, Safe Links, Safe Attachments, MCAS) segmented by business unit, geography, or risk level. Continuous tuning and segmentation maintain balance between protection and operational stability. |
| **3. Automation & Response Engineering** | Custom Logic App playbooks and Action Center workflows deliver automated isolation, remediation, and user notification. Semi-automated approval flows streamline containment while maintaining control and auditability. |
| **4. Telemetry & Integration Framework** | Flexible telemetry routing to Microsoft Sentinel or third-party SIEM/SOAR platforms. Connector configuration ensures high-quality signal ingestion, correlation fidelity, and reliable data flow across environments. |
| **5. Detection Tuning & Alert Precision** | Continuous refinement of suppression logic, threshold calibration, and contextual enrichment to eliminate noise and focus on high-fidelity detections. Enhanced correlation across Defender components reduces alert fatigue. |
| **6. Governance & Access Control** | Defined role scopes for analysts, admins, and responders, with least-privilege and just-in-time access enforced through PIM. Clear delegation boundaries support collaboration with MSSPs or external partners. |
| **7. Performance & Licensing Optimisation** | Regular assessment of Defender usage, policy impact, and license utilisation to ensure optimal coverage at minimum cost. Adjustments align feature sets with evolving business and compliance needs. |
| **8. Enablement & Operational Maturity** | Knowledge transfer, runbooks, SOPs, and asset inventories equip internal SOC or MDR teams for long-term sustainability. Power BI dashboards provide insight into alert trends, response performance, and platform health. |

## Service Delivery

- Delivered as an **annual service** following Cynode's design → deploy → optimise → empower methodology.
- Ongoing delivery through regular reviews, tuning cycles, and updates to policies, detections, and integrations.
- Collaboration with your team via documentation, knowledge transfer, and guided operational practices.