

# Anti-Ransomware Vs Malware Protection Vs Endpoint Detection & Response

This document outlines the key differences between the security add-ons available in Endpoint Central: Anti-Ransomware, Malware Protection, and Endpoint Detection and Response (EDR). This intended to help sales and partner teams identify the right add-on for the right customer.



## Anti-Ransomware

Detects ransomware attacks at an early stage using ML-based behavioural detection. Quarantine compromised endpoints, terminates malicious processes, and offers single-click recovery of encrypted enterprise data.



## Malware Protection

Offers protection beyond ransomware, covering a broad range of malware threats across endpoints. Powered by multi-layered detection leveraging behavioural analysis, advanced memory scanning, and intelligent triggers, it quarantines infected endpoints and restores systems to their pre-attack state.



## Endpoint Detection and Response (EDR)

One-stop solution for complete breach prevention, covering ransomware, malware, and beyond. When threats slip past prevention, EDR equips security teams with deep endpoint visibility, AI-driven threat hunting, and swift incident investigation, and effective response.

Our flagship EDR add-on, combining the full capabilities of Anti-Ransomware and Malware Protection with a complete detection and response layer.

| Category                       | Anti-Ransomware (ARW) | Malware Protection (MP)                         | Endpoint Detection and Response (EDR) |
|--------------------------------|-----------------------|-------------------------------------------------|---------------------------------------|
| Product segment                | Ransomware protection | Next-Generation Antivirus (NGAV) / Anti-malware | Endpoint Detection and Response (EDR) |
| Deployment                     | On-premises and cloud | On-premises and cloud                           | Cloud                                 |
| Ransomware protection          | ✓                     | ✓                                               | ✓                                     |
| Data exfiltration prevention   | ✓                     | ✓                                               | ✓                                     |
| MITRE Attack framework mapping | ✓                     | ✓                                               | ✓                                     |
| Single click data recovery     | ✓                     | ✓                                               | ✓                                     |
| Network quarantine             | ✓                     | ✓                                               | ✓                                     |
| Malware protection             | ✗                     | ✓                                               | ✓                                     |
| Advanced memory scanning       | ✗                     | ✓                                               | ✓                                     |
| Zia AI alert triage            | ✗                     | ✓                                               | ✓                                     |
| ML based behavioural detection | ✗                     | ✓                                               | ✓                                     |
| Threat hunting                 | ✗                     | ✗                                               | ✓                                     |
| Zia AI guided investigation    | ✗                     | ✗                                               | ✓                                     |
| Telemetry collection           | ✗                     | ✗                                               | ✓                                     |
| Threat Intelligence database   | ✗                     | ✗                                               | ✓                                     |

## Note

1. All three add-ons are available across all editions of Endpoint Central.
2. EDR add-on support for on-premises environments will be available soon.