Endpoint Detection Response

Threat detection and response lifecycle with speed, automation and unrivaled visibility

At a Glance

Endpoint detection, also known as endpoint detection and response (EDR), is a cybersecurity technique used to identify and respond to potential security threats on endpoints within a network. Endpoints refer to devices such as desktop computers, laptops, servers, and mobile devices that are connected to a network.

When an endpoint detection system identifies a suspicious activity or potential threat, it generates an alert or triggers an automated response.

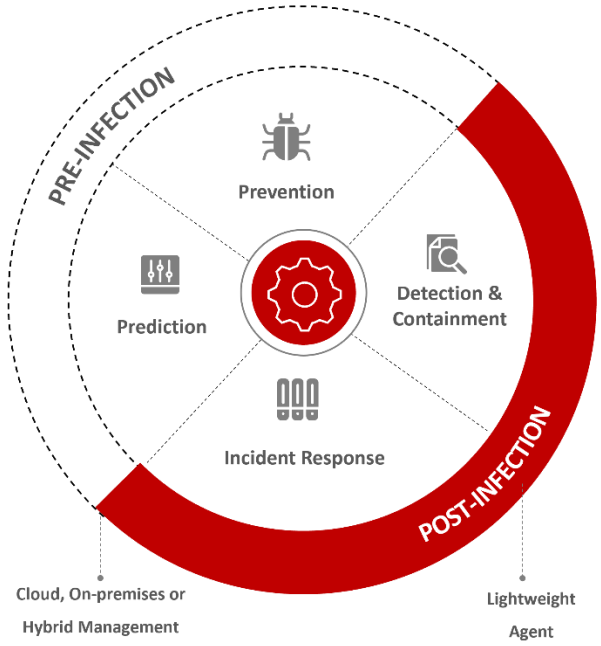
Key Features

- Ransomware & Malware Protection
- Realtime Analytics & Insights
- Zero Endpoint Impact
- Application tracking and ratings
- real-time threat intelligence
- Leverage OS-centric detection
- Pre-infection Protection
- Post-infection Protection
- Cloud Managed Platform
- Machine Learning
- Offline Protection
- Offline Protection
- Auto Threat Defusal

Product Overview

Garaj EDR continuously monitors all endpoint activity and analyzes the data in real time to automatically identify threat activity, enabling it to both detect and prevent advanced threats as they happen. Security teams can rapidly investigate incidents, respond to alerts and proactively hunt for new threats.

Garaj EDR works across multiple protected devices including workstations, servers, and cloud workloads with current and legacy operating systems, as well as manufacturing and OT systems. Garaj EDR features native integrations with the Garaj Security Fabric along with numerous third-party solutions.



The Garaj Advantage

Local Support	Managed Services	Dedicated Account Manager
Flexible Packages	Local Currency Billing	Onshore Data Residency

Find Out More

For information or to purchase Garaj products, call our 24/7 helpline 0304 1110365 or email us at cloud.support@jazz.com.pk

For detailed product specifications and system requirements visit our website garajcloud.com.