Skillmine
Technology • Consulting • Services

infosec
Miners

Endpoint Detection and Response (EDR)

March 2025

Imarc Group reports USD 3.7 billion in 2024 as the initial value of the global endpoint detection and response market, which will expand to USD 16.0 billion by 2033 while achieving a 17.6% growth rate (CAGR) between 2025 and 2033.

The cybersecurity solution Endpoint Detection and Response operates by providing real-time tracking alongside identification capabilities together with response features to defend endpoint devices against cyber threats. The purpose of EDR systems includes identifying unusual endpoint activities and responding to attacks while extracting endpoint intelligence for security breach mitigation.

EDR Life Cycle?

An EDR solution operates through multiple main functions to create complete endpoint protection.

The continuous functionality of EDR solutions tracks endpoint activities by observing all file operations and process executions as well as network connections. Each endpoint action gets recorded by these systems so they can spot potential threats as they happen.

Example: User actions become traceable when they open unsuspicious email attachments because EDR monitors the attachment's attempts to run malicious code through tracking mechanisms.

Endpoints undergo threat detection through current algorithms and signature-based detection techniques as well as machine learning detection methods provided by EDR systems. A combination of known and unknown threat detection follows from recognizing abnormal system activities.

Example: The warning alarms would become active when any endpoint starts conducting connections to external IP addresses which belong to ransomware networks.

An EDR system offers security teams instant threat response abilities through its built-in incident response functionality. The security system grants operators possession to defend devices by preventing unauthorized access and stopping execution of threats and shutting down internet connectivity. Attack confinement becomes possible through implementation of security protocols.

Example: The EDR tool of a manufacturing firm detects suspicious computer actions when a user connects to an unverified server. The security team isolates devices then eliminates potentially dangerous operations and cancels network transmission. Through prompt reaction, the system protects both itself and the network from further damage caused by malware.

The activity information from endpoints becomes available through EDR Solutions during forensic and investigational activities. These historical reports help security teams track down the origin of attacks and their initiation points along with determining their effects on company business operations.

Example: A security investigation becomes more efficient using EDR solutions because the system generates an attack timeline showing which files were accessed and what processes ran together with enumerated network connections thus enabling investigators to reconstruct the entire attack route.

The automatic threat remediation capabilities of EDR solutions enable them to remove malicious files and stop malicious processes together with performing vulnerability patching to secure systems.

Example: The EDR solution will either automatically remove suspicious files or stop malicious process execution.

Importance of EDR:

Traditional anti-virus solutions remain unable to defend against advanced threats as ransomware and file-less malware along with refinement cyberattacks cannot be detected by their methods. Traditional security approaches are outmatched by EDR systems because these systems continuously track and detect harmful operations which standard systems cannot identify.

By detecting security threats in real time EDR solutions minimize both the time needed to detect security incidents and the time required to stop dangerous threats.

End-point monitoring in real-time through EDR systems makes organizations more secure by finding and fixing their security weaknesses. The system informs operators about all prevention of unauthorized activities and unusual user actions to protect against system vulnerabilities.

Security capabilities of EDR solutions persist because they produce complete procedural reports that assist official checks and reviews.

The End-point Detection and Response solutions give organizations complete capabilities to investigate security incidents. Security teams generate attack information through endpoint data collection that produces incident avoidance knowledge for upcoming attacks.

Traditional Antivirus Vs EDR:

Feature	Traditional Antivirus	EDR Solutions
Detection Method	Signature-based detection	Behavioural analysis & anomaly detection
Threat Coverage	Known viruses and malware	Known and unknown threats
Response Time	Slow, relies on signature updates	Real-time detection and response
Adaptability	Rule-based, struggles with evolving threats	Continuously learns attack patterns
File-less Malware Detection	Ineffective	Effective through behavioural monitoring
Incident Response	Requires manual intervention	Automatic or near-automatic response
Monitoring Scope	Scans files periodically	Continuously tracks endpoint behaviour

Some of the Popular EDR solutions:

In 2024, Gartner for Endpoint Protection Platforms (EPP) evaluates various vendors in the EPP market based on their ability to execute and completeness of vision.

- **CrowdStrike Falcon** – A cloud-based cybersecurity tool using data patterns to detect threats across devices and cloud storage.
- **Microsoft Defender for Endpoint** – Leverages Microsoft tools for threat detection and automated response.
- **SentinelOne** – An autonomous defense solution with real-time attack remediation.
- **Palo Alto Cortex XDR** – Uses AI analytics for continuous endpoint, network, and cloud monitoring.
- **Sophos Intercept X** – Combines basic protection with advanced threat detection and proactive security protocols.

SKILLMINE CYBER SECURITY TEAM

For more information
Contact: info@skill-mine.com

Skillmine Technology • Consulting • Services
India | KSA | UK | USA

Stay Connected