EDR:

Tuesday, December 9, 2025 6:18 PM

What is EDR :

Endpoint Detection and Response (EDR) is a security solution that continuously monitors endpoint activity, detects suspicious or malicious behavior, and enables rapid response to contain and remediate threats.

How It Works :

At a high level, EDR works by:

1. **Deploying an agent on endpoints (workstations, servers, laptops).**
2. **Collecting detailed telemetry about system activity.**
3. **Analyzing behavior using rules, heuristics, and machine learning.**
4. **Alerting SOC analysts and enabling automated or manual response actions.**

Why EDR Is Critical in the Remote-Work Era :

With remote work, endpoints often operate outside the traditional network perimeter, making firewalls, IPS, and other network-centric controls insufficient on their own. EDR solves this by providing continuous protection directly on the endpoint, regardless of location.
Well-known EDR platforms include:

- **CrowdStrike Falcon**
- **SentinelOne ActiveEDR**
- **Microsoft Defender for Endpoint**
- **OpenEDR**
- **Broadcom Symantec EDR**

Although features vary, their core architecture and goals are similar.

The Three Pillars (Core Features) of EDR :

1 Visibility

Visibility is what truly differentiates EDR from traditional antivirus.
EDR collects deep telemetry such as:

- **Process modifications**
- **Registry changes**
- **File and folder activity**
- **User actions**
- **Network connections**
- **Parent–child process relationships**

This data is presented as:

- **Process trees**
- **Complete activity timelines**
- **Historical endpoint records**

This allows analysts to see exactly what happened, in what order, and why—giving full context for every detection.

2 Detection

EDR detection goes far beyond signatures by combining:

- **Signature-based detection**
- **Behavioral detection**
- **Machine-learning anomaly detection**
- **Fileless and in-memory attack detection**
- **Custom IOC ingestion**
- **MITRE ATT&CK mapping**

Each alert includes:

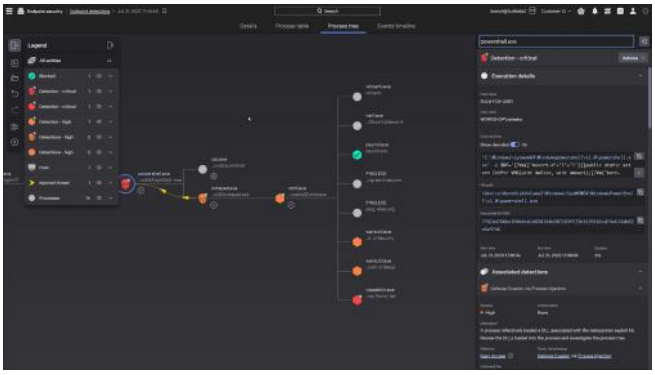
- **Severity**
- **Timestamp**
- **Affected host and user**
- **Triggering process/file**
- **ATT&CK tactic & technique**
- **Full execution context**

3 Response

EDR enables centralized, immediate response from a single console.
Common response actions:

- **Isolate the endpoint from the network**
- **Kill malicious processes**
- **Quarantine or delete files**
- **Run remote commands or scripts**

- Collect forensic artifacts



Why Is EDR Needed When AV Already Exists?

Traditional Antivirus (AV) and Endpoint Detection & Response (EDR) both aim to protect endpoints, but they operate at different levels of visibility and capability.

Antivirus (AV):

- Primarily relies on signature-based detection, hash comparisons, heuristic rules, and definition databases.
- Designed to detect known malware patterns.
- Limited telemetry collection.
- Reactive in nature.
- Does not typically monitor:
  - full process lineage
  - command-line arguments
  - memory injections
  - lateral movement techniques
  - behavioral anomalies

Endpoint Detection & Response (EDR)

- Provides continuous, real-time monitoring of endpoint activities.
- Detects threats using:
  - behavioral analytics
  - anomaly detection
  - machine learning
  - correlation across multiple endpoints
- Records rich telemetry:
  - process creation events
  - parent-child relationships
  - command-line execution
  - script interpreters activity (PowerShell, WMI, CMD)

In summary:

❌ AV detects known threats.
✔ EDR detects and responds to unknown, evasive, and multi-stage attacks.

Technical Scenario: AV vs EDR Response

Below is the technical breakdown of an advanced attack and how AV versus EDR handles each phase.

Attack Chain (Step-by-Step)

Step 1: Phishing email with malicious macro-enabled Word document

- AV:
  - No action if the file hash or macro signature is unknown.
- EDR:
  - Logs file download event.
  - Associates metadata (source URL, email attachment path, user initiating the download).

Step 2: User opens the Word document

- AV:
  - winword.exe is legitimate → allowed.
- EDR:
  - Records process execution telemetry (winword.exe).
  - Starts tracking child processes spawned by winword.exe

Outcome Comparison

Capability	Traditional AV	EDR
Detection method	Signature-based, static analysis	Behavioral, telemetry-rich, real-time monitoring
Visibility	Low	High (system-wide telemetry)
Process lineage tracking	No	Yes

Script-based attack detection	Weak	Strong
Memory injection detection	No	Yes
Network behavior monitoring	Minimal	Full context-aware visibility
Response actions	Limited to quarantine/block	Kill process, isolate host, investigate timeline, rollback (if supported)
Kill chain reconstruction	No	Yes

How EDR Works :

What makes EDR powerful?
EDR gives deep visibility into endpoint activity, detects advanced threats, and allows quick response actions—things traditional AV cannot do

How EDR Works:
A. EDR Agents (Sensors) – "Eyes & Ears" :

- **Installed on endpoints (PCs, servers).**
- **Continuously monitor activity:**
  - **process creation**
  - **command-line usage**
  - **PowerShell/WMI activity**
  - **file changes**
  - **registry changes**
  - **memory injections**
  - **network connections**
- **Sends all telemetry to the EDR console in real time.**
- **Can do basic local detections**

➡ **Agent collects raw data + performs lightweight detection.**

B. EDR Console – "Brain" :

- **Receives all telemetry from agents.**
- **Correlates events and checks with Threat Intelligence.**
- **Uses behavioral analytics & ML to detect suspicious patterns.**
- **Generates alerts with severity levels (Critical to Informational).**

➡ **Console analyzes data, correlates patterns, and generates alerts.**

What Happens After a Detection?

- **SOC Analyst reviews the alert → checks process tree, scripts, network traffic, etc.**
- **Determines False Positive or True Positive.**
- **If malicious → analyst takes action directly from console.**

Response actions EDR can perform:

- **Kill process**
- **Quarantine file**
- **Isolate the host**
- **Block hash**
- **Collect forensic data**

EDR Telemetry :

What is Telemetry?

- **Telemetry is the detailed data collected from an endpoint by the EDR agent.**
- **It acts like a black box that records everything happening on a system.**
- **This data is sent to the EDR console for detection, analysis, and investigation.**

Types of Telemetry Collected by EDR

Process Executions & Terminations

- **Tracks all running and stopped processes**
- **Captures parent–child process relationships**
- **Helps identify suspicious behavior (e.g., winword.exe spawning powershell.exe)**

Network Connections

- **Monitors inbound and outbound connections**
- **Detects:**
  - **Command-and-Control (C2) traffic**
  - **Unusual ports or protocols**
  - **Lateral movement**
  - **Data exfiltration attempts**

Command-Line Activity

- Logs commands executed via:
  - CMD
  - PowerShell
  - Scripting engines
- Critical for detecting:
  - Obfuscated commands
  - Malicious PowerShell usage
  - Living-off-the-land techniques

🗂 File & Folder Modifications

- Tracks file creation, deletion, and modification
- Useful for detecting:
  - Malware drops
  - Ransomware encryption behavior
  - Data staging prior to exfiltration

🗃 Registry Modifications

- Monitors registry changes used for:
  - Persistence
  - Privilege escalation
  - Security control tampering

The Windows Registry is a goldmine for attackers—and defenders.

Detection and Response Capabilities of EDR:

Advanced Detection Techniques :

1️⃣ Behavioral Detection

This detection method focuses on how a process behaves, not just what it is.

- Identifies suspicious parent–child relationships
- Detects misuse of legitimate tools (LOLBins)
- Effective against obfuscated and fileless attacks

Example:
winword.exe spawning powershell.exe → flagged due to unusual behavior.
➡️ This is especially useful for detecting known malicious behaviors, even if the file hash is unknown.

2️⃣ Anomaly Detection

EDR learns the baseline behavior of an endpoint over time.

- Flags deviations from normal behavior
- Useful for detecting insider threats and misconfigurations
- May generate false positives, but full telemetry helps analysts validate

Example:
A rarely used process modifying an auto-start registry key.

3️⃣ IOC Matching

EDR integrates with threat intelligence feeds.

- Matches hashes, IPs, domains, filenames, etc.
- Enables fast detection of known threats
- Limited against true zero-day attacks

Example:
A downloaded executable hash matches a known ransomware IOC.

4️⃣ MITRE ATT&CK Mapping

Each detection is mapped to:

- Tactic (Why)
- Technique (How)

This helps analysts:

- Understand attack stages
- Prioritize alerts
- Communicate clearly in reports

5️⃣ Machine Learning Algorithms

EDR applies ML models trained on massive datasets.

- Detects multi-stage and fileless attacks
- Identifies malicious chains of activity
- Effective against advanced evasion techniques

Response Capabilities :

🔒 Isolate Host :

- Disconnects endpoint from the network
- Prevents lateral movement

- One of the fastest containment actions

❌ **Terminate Process :**
- Stops a malicious process without isolating the host
- Useful for business-critical systems

📦 **Quarantine :**
- Moves malicious files to a safe, non-executable location
- Allows later review or removal

💻 **Remote Access (RTR) :**
- Analysts can open a remote shell
- Run commands and scripts
- Collect forensic data
- Perform custom remediation

📄 **Artefact Collection :**
- Memory dumps
- Event logs
- Registry hives
- Folder contents

All without physical access to the device.

FOR UNDERSTANDING DASHBOARD SEE THIS VEDIO:

https://screenrec.com/share/qgnzXECRPT