

EDR:

Endpoint Detection and Response (EDR) is a **security solution** designed to monitor, detect, and respond to advanced threats at the endpoint level. We will see how an **EDR** differs from a traditional antivirus and what data it collects from the endpoints.

To protect these devices, organizations implement several security measures, most of which are to protect the network on which they operate these digital devices.

however, the fast adoption of **Remote Work** has exposed these devices as they are **out of the perimeter protection** deployed on the organization's network.

To ensure these endpoint devices are protected **even out of the network**, we need a security solution that guards all devices in different areas and is capable of fighting advanced threats.

No matter where the endpoints are, the **EDR** will make sure they are monitored constantly and threats are detected.

EDR becomes a very powerful tool. **However, it's also important to remember that an **EDR** is a host-only security solution and does not detect network-level threats.**

Fileless malware is a type of malicious software that **doesn't write files to the hard drive**. Instead, it runs **in memory** and often uses legitimate system tools (like PowerShell or WMI) to carry out attacks, making it **harder to detect with traditional antivirus**. fileless malware **lives in RAM during execution**, sometimes with small tricks to come back after a reboot.

What is MITRE ATT&CK?

- MITRE ATT&CK stands for **Adversarial Tactics, Techniques, and Common Knowledge**.

- It's a **globally recognized knowledge base** of **attacker behaviors**, methods, and techniques used in real-world cyberattacks.
- It's used by **security teams** (SOC, threat intelligence, red teams) to **identify, detect, and defend against attacks**.
- Organized into **tactics** (the “why” of an attack) and **techniques** (the “how” attackers achieve that goal).

Features of EDR

There are **three** main features of an EDR,

Visibility:

A good analysis often depends on the available **level of visibility of the activity**. The level of **visibility EDR provides is impressive**. It collects detailed data from the endpoints, which includes **process modifications, registry modifications, file and folder modifications, user actions, and much more**. It presents this information in a very structured format to the analyst. The analyst can see the **whole process tree** with a complete **activity timeline of the sequence of actions**. The analyst can also access the **historical data** of any endpoint for threat hunting or any other purpose. Any detections in the EDR land with a whole context

Each **node** represents a **process**. The **lines** connecting them represents their **relationship**. If we click on the **b** given with each process, **we will be able to see all the network connections, registry changes, file changes etc. associated with that process**.

Detection:

It incorporates **signature-based detections** as well as **behavior-based detections**, such as unexpected user activities. With **modern machine learning capabilities**, it identifies any deviation from the **baseline behavior** and instantly flags it. It can also detect fileless malware that resides in memory. It also allows us to **feed custom IOCs for threat detections**.

Response:

EDR also empowers analysts to take **action on detected threats**. These actions can be taken at any endpoint within the **central EDR console**. As an analyst, you may decide to isolate a complete endpoint, terminate a process, or quarantine some files. You can also connect to the host remotely and execute actions independently. You can do this all from within the EDR console.

EDR detects automatically, but response is mostly manual, with optional automation for low-risk actions.

EDR vs antivirus:

Antivirus (AV) is like the **airport's immigration check**, catching only known threats, while EDR is like **security officers inside, continuously monitoring behavior and taking action on suspicious activity** that evades basic checks.

An **EDR provides deeper, behavior-based protection** beyond traditional antivirus, detecting **suspicious or unknown threats that evade basic signature checks**. It monitors activity continuously and can catch advanced attacks even if they're previously unknown.

The Antivirus (AV) may detect some basic threats, but to detect advanced threats that evade normal detections, we need an EDR. **An EDR also provides organization-wide visibility of any activity**. For example, if a **suspicious file is detected on one endpoint, the EDR will also check it across all the other endpoints**.

Some modern AVs may have more enhanced visibility and detection. However, an EDR is ahead as it levels up the detection and response in an endpoint.

How an EDR works?

Agents

We can **integrate multiple endpoints** with our EDR and **manage them through a centralized console**. There are EDR agents that **we have to deploy inside those endpoints**.

These agents are also sometimes referred to as **sensors**. They are the eyes and ears of the EDR. **The EDR agents can do some basic signature-based and behavior-based detections** by themselves and send them to the EDR console, which triggers alerts.

Console

All the detailed data sent by the EDR agents is correlated and analyzed through complex logic and machine learning algorithms. The threat intelligence information is matched with the collected data. The EDR is just like the brain connecting all the dots. These dots connect to form a detection, often called an alert.

What happens after Detection?

When a detection comes, it's a SOC analyst's responsibility to acknowledge the alert and prioritize it. The prioritization is made easy by the EDR itself. For the investigation, once the alert is clicked, the analyst can see all the details of the detection. This includes any files executed, processes executed, network connection attempts, registry modifications, and much more. The analyst's job is first to use their expertise to determine if the alert is a false positive or a true positive. In case of a true positive, the analyst can take actions from within the EDR console.

EDR with Other Tools

As a SOC Analyst, it is essential to understand that although a standalone EDR provides enough information to detect and respond to threats in an endpoint, it works alongside other security solutions to form a larger security ecosystem. Within a network, you will see Firewalls, DLPs, Email Security Gateways, IAMs, EDRs, and other security solutions protecting the different components of the network.

To minimize the effort and maximize the efficiency, all these security solutions are integrated with a SIEM solution that becomes the central point of investigation for the analysts.

EDR Telemetry:

We learned about EDR agents, which collect different data from their endpoints and push it to the EDR console. This data is known as **Telemetry**. Telemetry is the data collected by EDR agents from endpoints and sent to the EDR console. It's like the "black box" of the device, containing all the information needed for **threat detection**,

investigation, and response. The more data is collected, the better judgments can be made. EDR collects detailed telemetry from the endpoints.

take a brief look at some of the telemetry that it collects:

Process Executions and Terminations

1. Tracks every **program that starts or stops on the device**.
2. Helps spot **suspicious parent-child process relationships** (e.g., a normal program launching **malware**).
Sometimes, malware hides by being launched by a **legitimate program**.
3. **Parent-child process relationship** = the program that started another program.
4. Example: If **Word (parent)** suddenly launches a **malware executable (child)**, that's suspicious.

Network Connections

- Monitors all network activity from the endpoint.
- Detects connections to **command-and-control (C2) servers**, unusual ports, data leaks, or internal movement by attackers.

Command Line Activity

- Records all commands run in **CMD, PowerShell, or terminal**.
- Detects **malicious or obfuscated commands** that antivirus might miss.

Files and Folders Modifications

- Tracks creation, deletion, or modification of files and folders.
- Detects **ransomware activity, data staging, or malware dropping files**.

Registry Modifications

- Monitors changes in the **Windows registry**, which stores system configurations.
- Detects **malicious changes made by malware to maintain persistence or alter settings**.

The **Windows registry** is like a configuration database for the system and programs.

Malware often changes the registry to:

- **Stay hidden after a reboot** (persistence)
- **Disable security features**
- **Change system behavior** for malicious purposes
-
-

So, EDR **does not analyze all network traffic**, but it **does care about network behavior of the endpoint** to detect malware or C2 communications.

In short:

EDR doesn't replace a network security solution, but it **monitors the network activity of its own endpoints** to catch suspicious connections.

EDR collects much more than this data from an endpoint. While individual actions may appear harmless, detailed telemetry reveals malicious patterns, helping EDR detect threats and enabling analysts to **investigate, identify the root cause, and reconstruct the full attack timeline.**

Detection And Response Capabilities:

some advanced detection techniques are applied to this data. Some of these techniques include:

Behavioral Detection:

Instead of just **matching the signatures with known threats**, it observes the complete **behavior of a file**.

Example: A process winword.exe spawning PowerShell.exe will be flagged by the EDR due to the behavior. A **Word document** spawning a PowerShell is an **unusual parent-child relationship**.

Anomaly Detection:

With time, EDR understands the **baseline behavior of the endpoints**. Any activity that deviates from this behavior will be **flagged**. During any malicious activity, the endpoint's behavior deviates from normal. EDR picks it up.

Example: On one of the endpoints, a process **modifies an auto-start registry key**, which is **not a common behavior on the endpoint**.

IOC matching:

EDRs have some strong **threat intelligence field** integrations. Except for zero-day attacks, most of the attacks have **indicators published in the threat intelligence feeds**.

Example: A user downloads a file that drops an executable. The executable is often used in a **specific attack**. The hash of this executable will **get matched with the threat intelligence feed and instantly flagged by the EDR**.

Machine Learning Algorithms

Advanced threat actors try to evade defenses **as much as possible**, and their activities may sometimes **bypass advanced detection techniques**. Modern EDRs have **machine learning models trained by a large dataset of normal and malicious behaviors**. This can detect complex patterns of an attack.

Example: Attacks in which the individual actions are not inherently malicious, but the **ML algorithm identifies the whole chain of activities as malicious**. Fileless attacks and multi-staged intrusions are often detected through this.

MITRE ATT&CK Mapping in EDR

- When EDR detects suspicious or malicious activity, it **tags it with a corresponding MITRE ATT&CK tactic and technique**.
- **Tactic** = the goal of the attacker at that stage (the “why”).
- **Technique** = the method used to achieve that goal (the “how”).

Example:

- Activity: EDR detects creation of a scheduled task on the endpoint.
- MITRE Mapping:
 - **Tactic:** Persistence (attacker wants to stay on the system even after reboot)
 - **Technique:** Scheduled Task/Job (the method used to maintain persistence)

Response

EDR offers both **automated and manual responses**. You can make policies to block known malicious behaviors automatically. However, manual response gives you a wide range of response capabilities.

Isolate Host

Disconnects a **compromised endpoint from the network** to stop malware from spreading.

Most attacks start from a **single endpoint and move laterally to other endpoints** to compromise the whole network.

Terminate Process

Some hosts run the **core business operations, and isolating them** can cause more **loss than the malicious activity**. Stops a malicious process without isolating the whole host, useful for critical business machines.

Quarantine

Moves malicious **files to a safe location where they cannot execute**, allowing review or deletion.

Remote Access:

This is often done when the **EDR's built-in response is not enough to take action on a specific activity**. Through remote access, analysts can gain deeper visibility into the **system or take custom actions within the endpoints**

Analysts can remotely access the endpoint, run commands, scripts, or custom investigations when built-in responses aren't enough.

Artefacts Collection:

Analysts can **extract important artefacts from the endpoints without physically accessing the device**. The most commonly extracted artefacts include:

- Memory Dump
- Event Logs
- Specific Folder Contents
- Registry Hives

Extracts data for forensic or legal investigation without physically touching the device.

Common artefacts: **memory dumps, event logs, folder contents, registry hives**.

