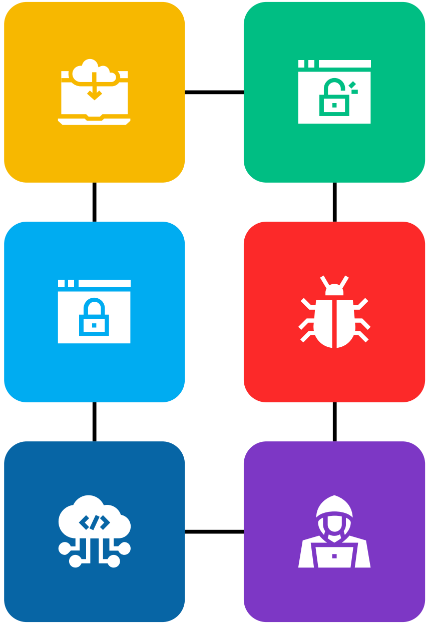
Endpoint Detection and Response (EDR)

MNU-2025



Dr. Ahmed Samy

Lecture 09

Module Contents

In this module, we will cover the below topics:

- What is EDR and how it works?
- EDR vs. Traditional Antivirus
- Forti EDR
- EDR in Action
- Popular EDR Tools
- EDR Challenge and Limitation

End Point Detection and Response (EDR)

What is Malware?

- **Malware (Malicious Software)** is any software intentionally designed to harm devices, steal data, or disrupt operations. It includes a wide range of threats, including viruses, ransomware, spyware, and more.

1. **Viruses**
    - Attach to clean files and spread when the file is executed. Requires user action (e.g., opening a file) to activate and spread.
    - *Example*: **Stuxnet Virus** (Disrupted physical equipment).
2. **Worms**
    - Self-replicating; spread without user interaction. Can consume bandwidth, crash systems, steal passwords, or deliver a payload.
    - *Example*: **ILOVEYOU Worm** (spread via email with the subject "ILOVEYOU").
3. **Trojans**
    - Hidden as legitimate software to trick users. Creates backdoors, steals information, or installs other malware.
    - *Example*: **Zeus** (steals banking credentials).

What is Malware?

4. **Ransomware**
   - Encrypts files and demands payment for decryption.
   - *Example*: **WannaCry, Locky** (targeted businesses via email attachments).

5. **Spyware**
   - Secretly monitors user activity and collect sensitive data like passwords, keystrokes, browsing habits
   - *Example:* **Pegasus** (spyware for mobile devices).

6. **Adware**
   - Displays unwanted ads, often bundled with free software.
   - *Example:* Pop-up ads redirecting to scam sites.

7. **Rootkits**
   - Grants attackers' remote control while hiding deep in systems.
   - *Example:* **Sony BMG Rootkit** (Installed by copy-protected music CDs from Sony BMG). made the system vulnerable to other malware.

What is EDR?

- **End Point Detection and Response (EDR)** is a software used by security operations teams to detect, contain, investigate and remediate cyberattacks.

- EDR tools are used to discover suspicious activities on hosts and endpoints that are connected to the network—such as mobile phones, desktops, laptops, and virtual machines.

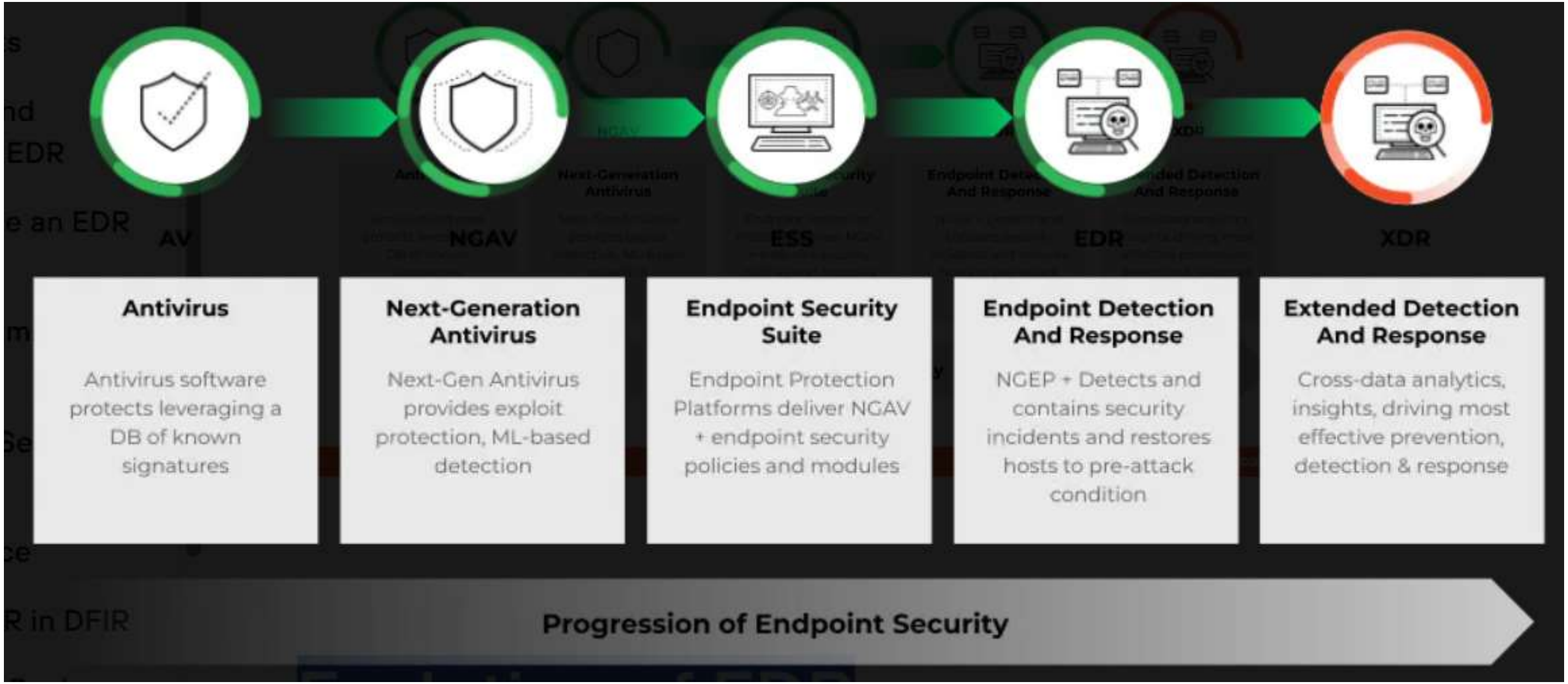
- EDR systems offer a proactive approach to threat management by:

  1. Collecting and analyzing vast amounts of data from endpoints to uncover suspicious behavior, often using machine learning and behavioral analysis techniques.
  2. Providing detailed visibility into endpoint activities, allowing for rapid detection of anomalies and rapid response to incidents.
  3. Integrating with other security tools to enhance an organization's overall security posture (SIEM, Firewalls, ….).
  4. Ensuring comprehensive protection against sophisticated cyberthreats.

Why is EDR Important?

- The key reason is to detect and mitigate damage from cyberthreats and prevent data leakage to bad actors.
- **Real-Time Threat Detection:** EDR continuously monitors endpoint activity to detect suspicious behavior or known threat patterns.
- **Incident Response:** It enables security teams to investigate incidents quickly by providing tools to isolate infected devices or remove threats.
- **Improved Visibility:** EDR provides deep visibility into endpoint behavior, helping detect and respond to attacks that would otherwise go unnoticed.
- **Forensics and Root Cause Analysis:** EDR tools retain historical data that can be used to trace how an attack happened, determine what systems were affected, and prevent future incidents.
- **Automation and Threat Hunting:** Many EDR systems include automation features and allow proactive threat hunting, helping organizations stay ahead of evolving threats.

Evolution of EDR



Antivirus

Antivirus software protects leveraging a DB of known signatures

Next-Generation Antivirus

Next-Gen Antivirus provides exploit protection, ML-based detection

Endpoint Security Suite

Endpoint Protection Platforms deliver NGAV + endpoint security policies and modules

Endpoint Detection And Response

NGEP + Detects and contains security incidents and restores hosts to pre-attack condition

Extended Detection And Response

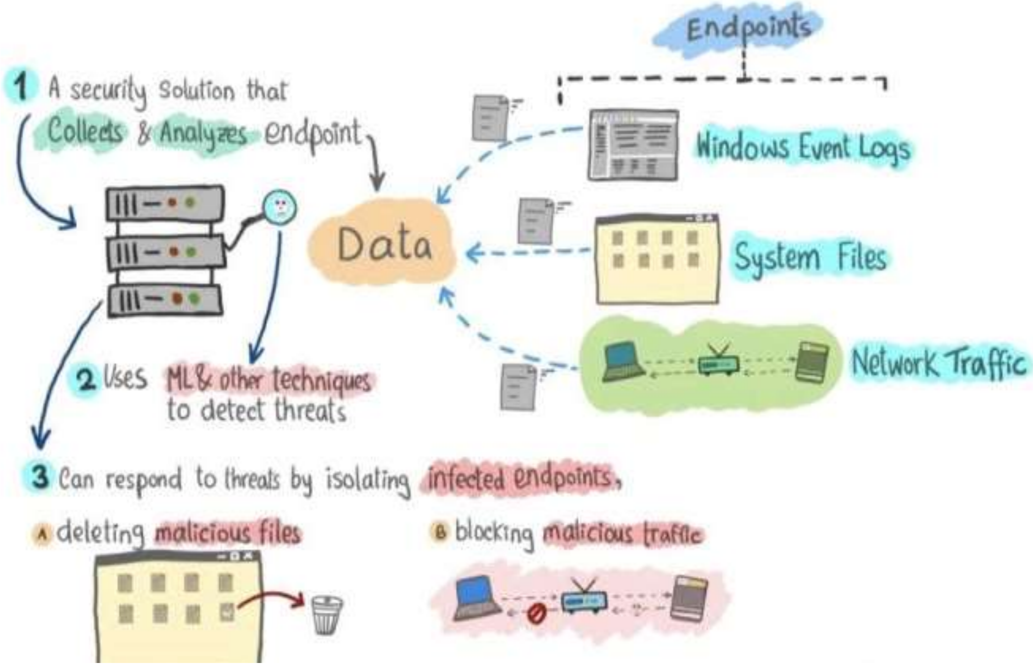
Cross-data analytics, insights, driving most effective prevention, detection & response

Progression of Endpoint Security

How EDR Works?

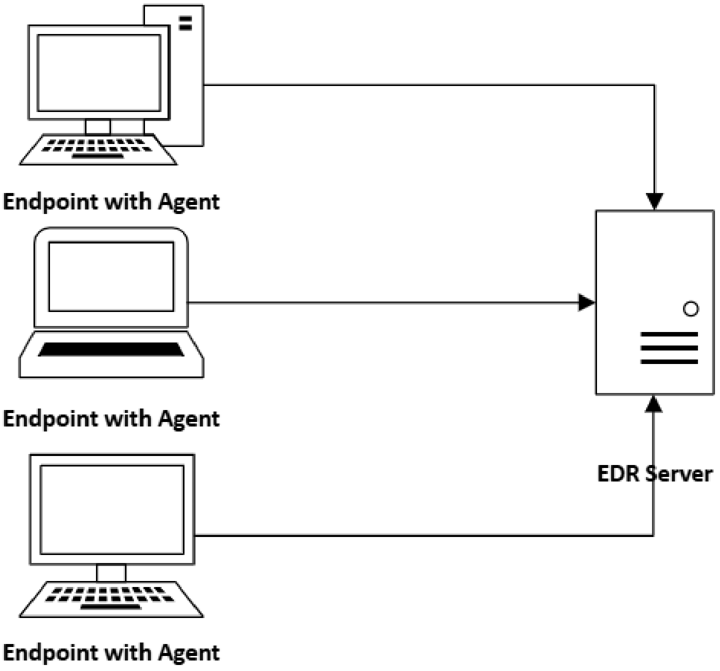
How EDR Works?

1. **Data Collection:** Logs processes, network connections, file changes.
2. **Behavioral Analysis:** Detects anomalies (e.g., unusual file encryption).
3. **Threat Detection:** Uses AI, ML, and threat intelligence.
4. **Alerting & Investigation:** Security teams analyze alerts.
5. **Response:** Isolate endpoints, kill malicious processes, roll back changes.


Endpoints
1 A security solution that Collects & Analyzes endpoint
Data
Windows Event Logs
System Files
Network Traffic
2 Uses ML & other techniques to detect threats
3 Can respond to threats by isolating infected endpoints,
A deleting malicious files
B blocking malicious traffic

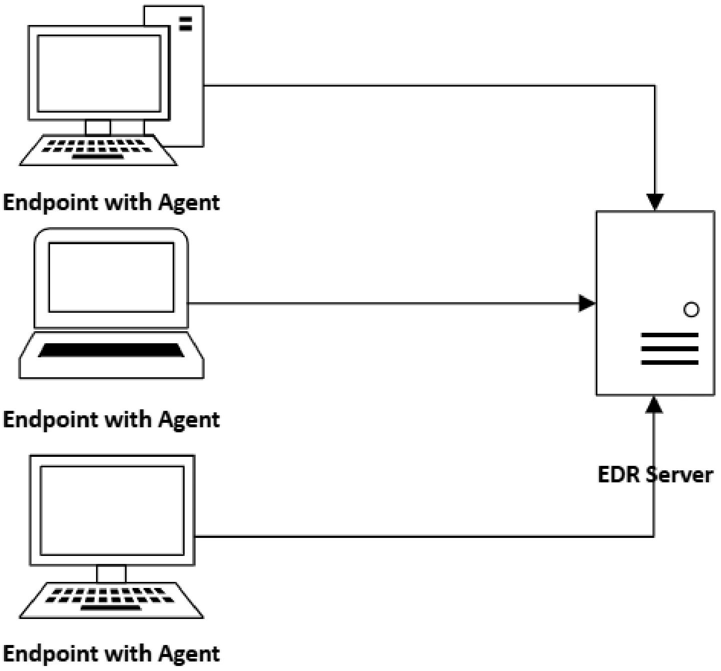
1. Data Collection

- EDR agents installed on endpoints and gather vast amounts of data from endpoints, capturing every action and event.
- This data includes file changes, process executions, network connections, and user activities.
- Logs are sent to a centralized dashboard for analysis.
- By collecting this information continuously, EDR solutions create a comprehensive timeline of endpoint behavior.



2. Behavioral Analysis

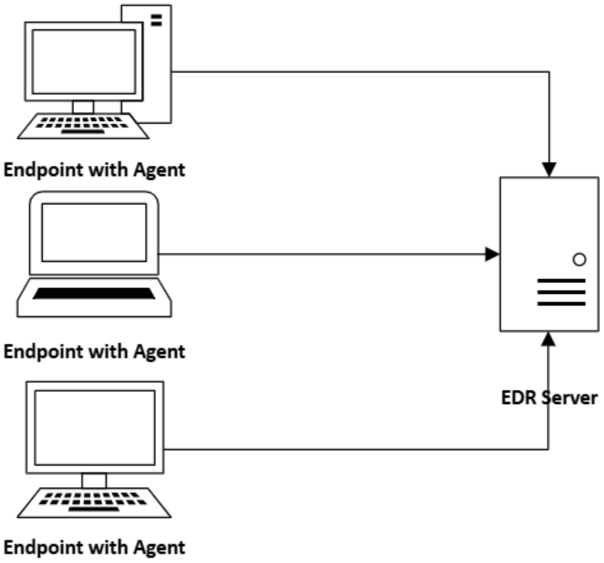
- Instead of just checking for known malware (like antivirus), EDR analyzes behavior.
- Uses AI/ML models to detect anomalies (e.g., a program suddenly encrypting files).
- Catches zero-day attacks (previously unknown threats).
- **Example:** Detects ransomware based on file encryption patterns.



3. Threat Detection & Alerting

- **Continuous file analysis detects threats** by examining each file that interacts with the endpoint. Files that present a threat are flagged.
- In many cases, a file appears safe, at first. However, if it starts to exhibit threatening behavior, your EDR can send an alert to let the IT team and other stakeholders know.

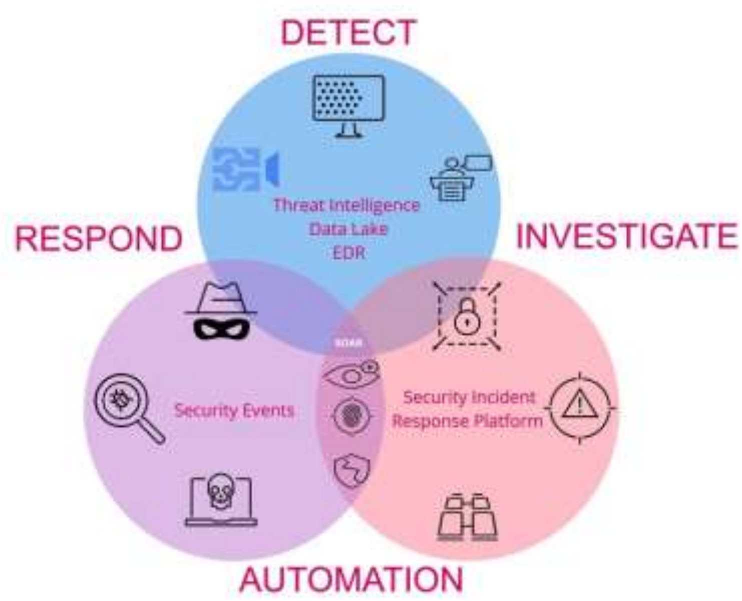
- **Global cyber threat intelligence** analyzes information collected from artificial intelligence (AI) and large data storehouses of existing and constantly evolving cyber threats to detect threats that are targeting endpoints.



4. Investigation & Forensics

- SOC analysts review alerts, check timelines, and investigate.

- EDR provides forensic data (e.g., which files were accessed, which user executed the malware).



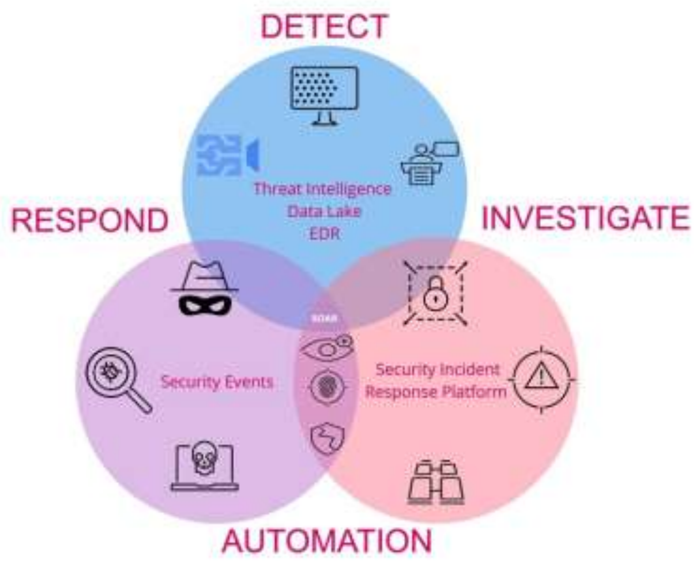
5. Incident Response

- **Automated incident response** transforms how EDR systems handle threats by enabling fast, decisive actions without human intervention.

- When an EDR system detects a potential threat, it can automatically isolate the affected endpoint, preventing lateral movement across the network.

- Sophisticated EDR solutions can execute predefined response playbooks, such as terminating malicious processes, deleting harmful files, or rolling back changes made by ransomware.

- **Automated actions:** Quarantine device, kill malicious process, roll back changes.
- **Manual actions:** SOC may isolate the network, patch vulnerabilities.

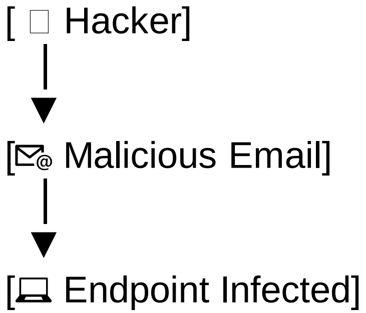


EDR in Action

EDR in Action – Stopping a Malware Attack

- **Step 1: Hacker Deploys Malware**
- An employee clicks on a phishing email (e.g., a fake invoice PDF).
- The PDF contains a malicious script that downloads ransomware.
- **What Happens Behind the Scenes?**
- The malware executes and tries to:

  1. Disable the device’s antivirus.
  2. Start encrypting files (e.g., documents, databases).
  3. Spread to other devices on the network.


[□ Hacker]

↓

[📧 Malicious Email]

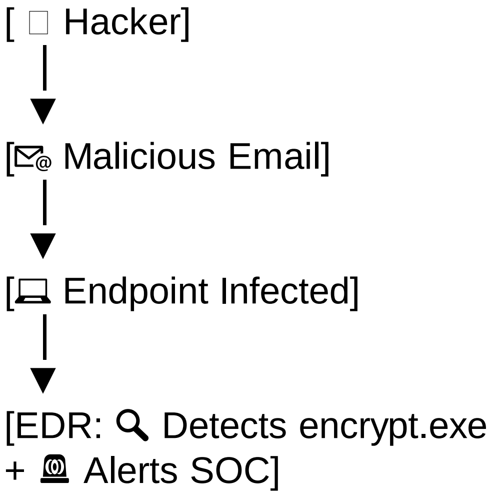
↓

[💻 Endpoint Infected]

EDR in Action – Stopping a Malware Attack

- **Step 2: EDR Detects Unusual Behavior**

1. **Process Monitoring:**
   - EDR sees a rare process (e.g., encrypt.exe) spawning suddenly.
   - Flags it because the user never runs this program.
2. **Behavioral Analysis:**
   - The malware tries to modify hundreds of files in seconds (unlike normal user activity).
   - Matches a known ransomware pattern (e.g., rapid file encryption).
3. **Threat Intelligence Check:**
   - EDR compares the process against a threat database (e.g., MITRE ATT&CK T1486 – Data Encrypted for Impact).



[□ Hacker]

▼

[📧 Malicious Email]

▼

[💻 Endpoint Infected]

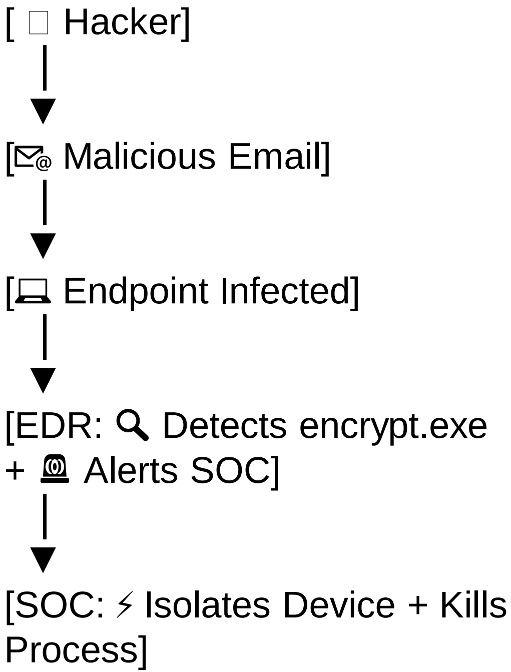
▼

[EDR: 🔍 Detects encrypt.exe + 🚨 Alerts SOC]

EDR in Action – Stopping a Malware Attack

- **Step 3: SOC Team Investigates & Isolates the Device**

1. **Alert Analysis:**
   - Receives an alert: "Suspicious file encryption activity on Device-A."
   - Checks process tree: invoice.pdf → powershell.exe → encrypt.exe
2. **Forensic Data:**
   - EDR provides:
     - ➢ Which files were altered.
     - ➢ Network connections made (e.g., malware calling a C2 server).
     - ➢ User account involved.
3. **Containment Action:**
   - Clicks "Isolate Device" in the EDR tool:
     - ➢ Blocks all network traffic from the infected device.
     - ➢ Suspends the malicious process.



[□ Hacker]

↓

[📧 Malicious Email]

↓

[💻 Endpoint Infected]

↓

[EDR: 🔍 Detects encrypt.exe + 🚨 Alerts SOC]

↓

[SOC: ⚡ Isolates Device + Kills Process]

EDR in Action – Stopping a Malware Attack

- **Step 4: Threat Contained – Minimal Damage**

- The ransomware **only encrypted 10 files** before being stopped.
- IT restores files from **backups** (no ransom paid).
- Post-incident:
  - EDR logs help identify the **phishing email source**.
  - Company updates **security training** to prevent repeats.

[□ Hacker]
|
▼
[📧 Malicious Email]
|
▼
[💻 Endpoint Infected]
|
▼
[EDR: 🔍 Detects encrypt.exe + 🚨 Alerts SOC]
|
▼
[SOC: ⚡ Isolates Device + Kills Process]
|
▼
[✅ Threat Stopped]

EDR vs Traditional Antivirus

- EDR and traditional Antivirus software protect computers and networks from malware and other threats, but they provide different levels of defense.

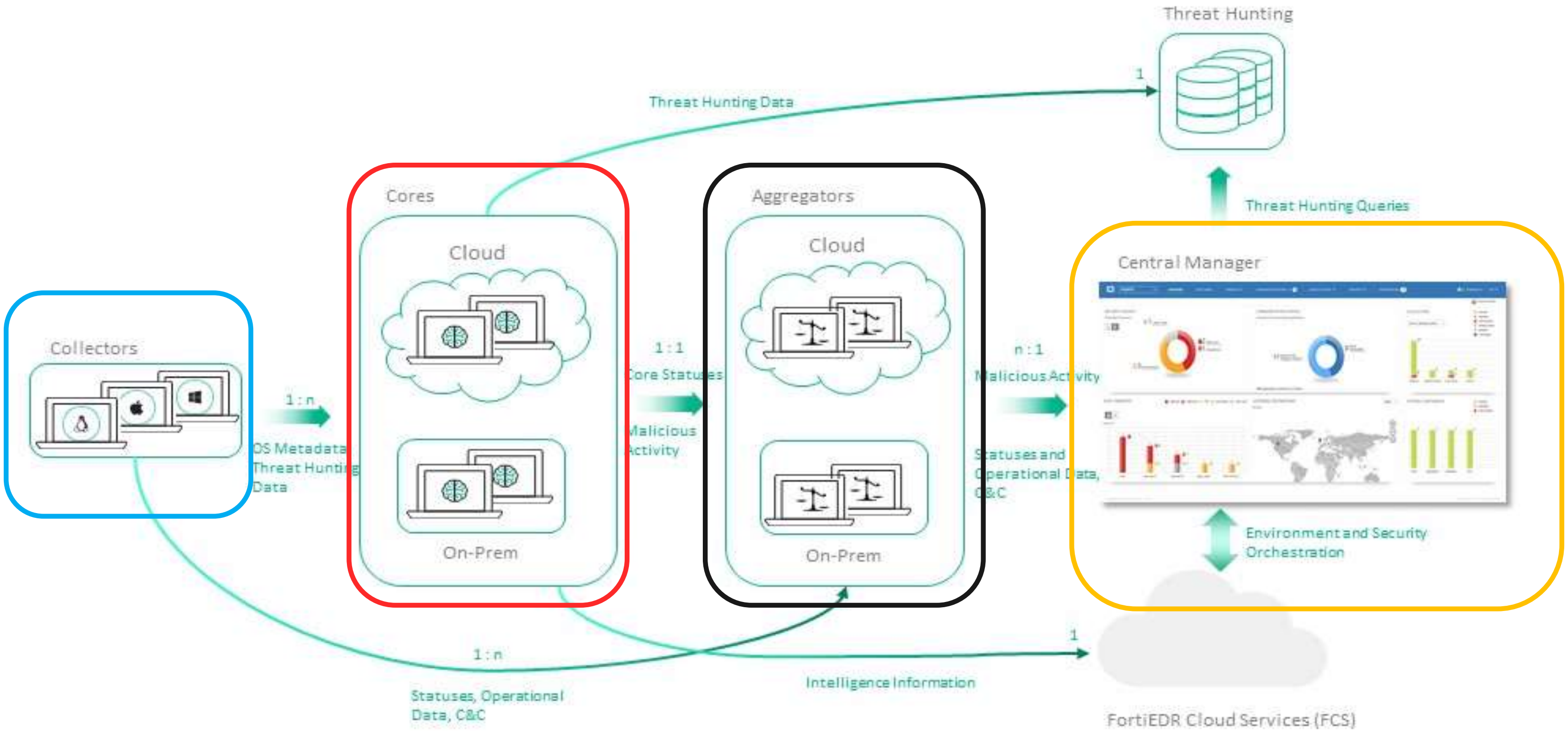
	EDR	Antivirus
Purpose	Monitors, detects, and responds to a broader range of threats, including sophisticated attacks.	Targets known malware using signature-based detection
Detection Methods	Uses behavioral patterns and anomaly detection for identifying advanced threats.	Relies on signatures to identify threats
Response Capabilities	Includes real-time containment and detailed investigation tools.	Focuses on block or removing malware
Scope of Protection	Offers broader protection with forensic tools and network-wide analysis.	Limited to file and program integrity.
required Knowledge	Requires skilled personnel for effective management and response.	Minimal; operates automatically

Popular EDR Tools

Popular EDR Tools

1. CrowdStrike Falcon
2. Microsoft Defender for Endpoint
3. Kaspersky EDR
4. Symantec EDR
5. FortiEDR

Fortinet EDR Components



FortiEDR Collector

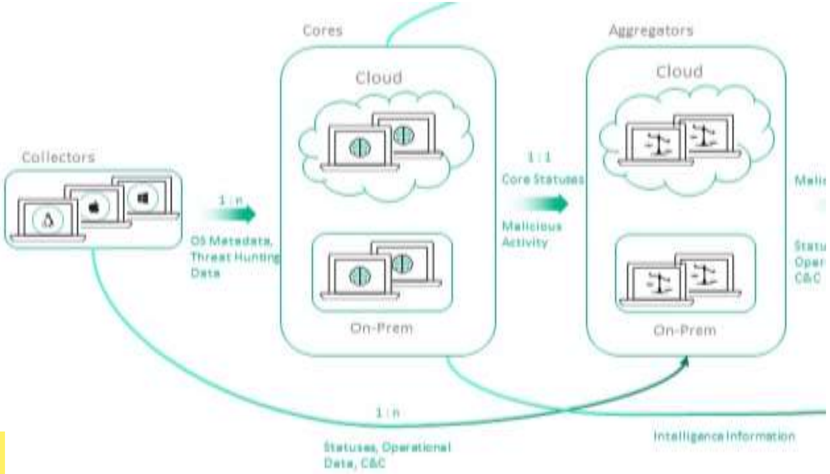
- The **FortiEDR Collector** is an agent that resides on every communicating device in your enterprise, including desktops, laptops and servers.

- Upon every attempt made by the communicating device to establish a network connection or change a file, the Collector collects all required metadata and analyzes it to determine whether the process performing the action is legitimate.

- You can configure the Collector to use a Core for the metadata analysis, in which case the Collector holds the establishment of the connection until authorization is received from the Core.

- The FortiEDR Collector initially sends registration information to the FortiEDR Aggregator via SSL and then it sends ongoing health, status information, and security events.

- The FortiEDR Collector receives its configuration from the FortiEDR Aggregator.



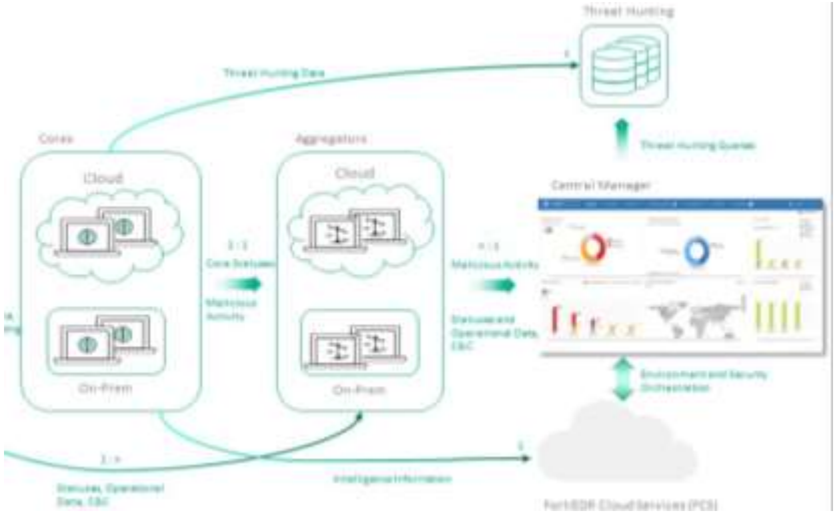
FortiEDR Core

- The FortiEDR Core is the security policy enforcer and decision-maker. It determines whether a connection establishment request is legitimate or represents a malicious exfiltration attempt that must therefore be blocked.

- The core may run on-premises, in the cloud, or a combination of both.

- If the collector is offline, it uses built-in policies at the collector level, to operate in autonomous mode.

- That means if the collector can't connect to the core, the device is still protected at the collector level.

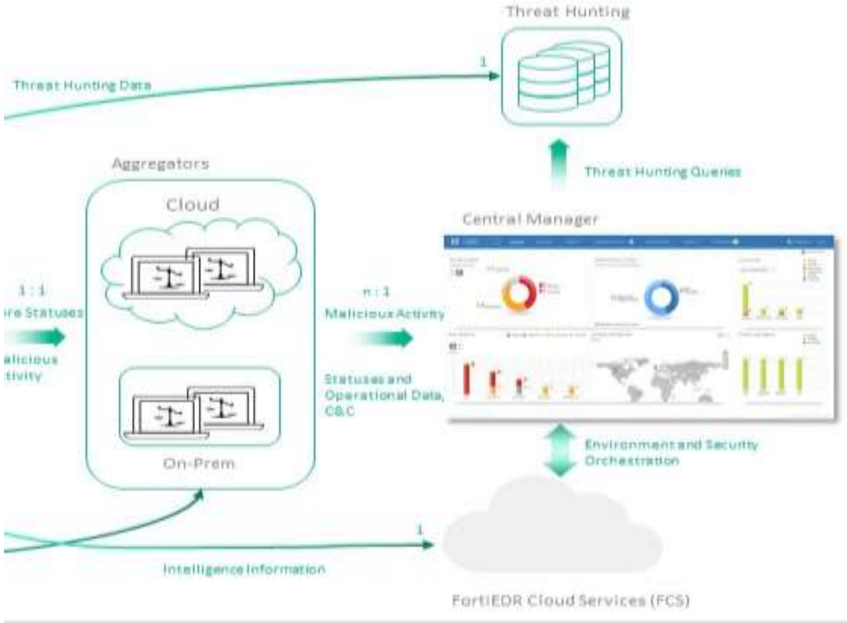


FortiEDR Aggregators

- The **FortiEDR Aggregator** is a software-only entity that acts as a proxy for the FortiEDR Central Manager and provides processing load handling services.

- All FortiEDR Collectors and FortiEDR Cores interact with the Aggregator for registration, configuration and monitoring purposes.

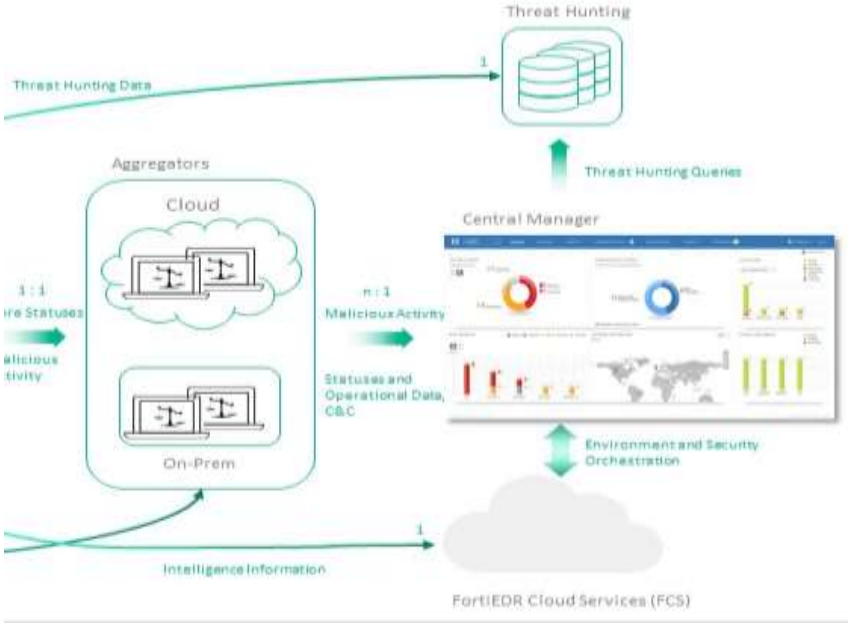
- The FortiEDR Aggregator aggregates this information for the FortiEDR Central Manager and distributes the configurations defined in the FortiEDR Central Manager (such as exceptions, policies, and rules) to the FortiEDR Collectors and FortiEDR Cores.



FortiEDR Central Manager

- The **FortiEDR Central Manager** is a software-only central web user interface and backend server for viewing and analyzing events and configuring the system.

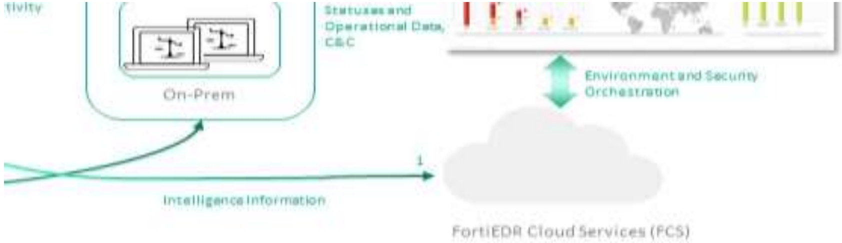
- The FortiEDR Central Manager is the only component that has a user interface. It enables you to:
  - Control and configure FortiEDR system behavior.
  - Monitor and handle FortiEDR events.
  - Perform deep forensic analysis of security issues.
  - Monitor system status and health.



FortiEDR Cloud Service

- **The FortiEDR Cloud Service (FCS)** enriches and enhances system security by performing deep, thorough analysis and investigation about the classification of a security event.

- The FCS is a cloud-based, software-only service that determines the exact classification of security events and acts accordingly based on that classification – all with a high degree of accuracy.


tivity
On-Prem
Statuses and Operational Data, C&C
Environment and Security Orchestration
1
Intelligence Information
FortiEDR Cloud Services (FCS)

How does FortiEDR work?

- **The FortiEDR Collector collects OS metadata**: A FortiEDR Collector runs on each communicating device in the organization and transparently collects OS metadata on the computing device.

- **Communicating device makes a connection establishment request**: the FortiEDR Collector sends a snapshot of the OS connection establishment to the FortiEDR Core, enriched with the collected OS metadata.

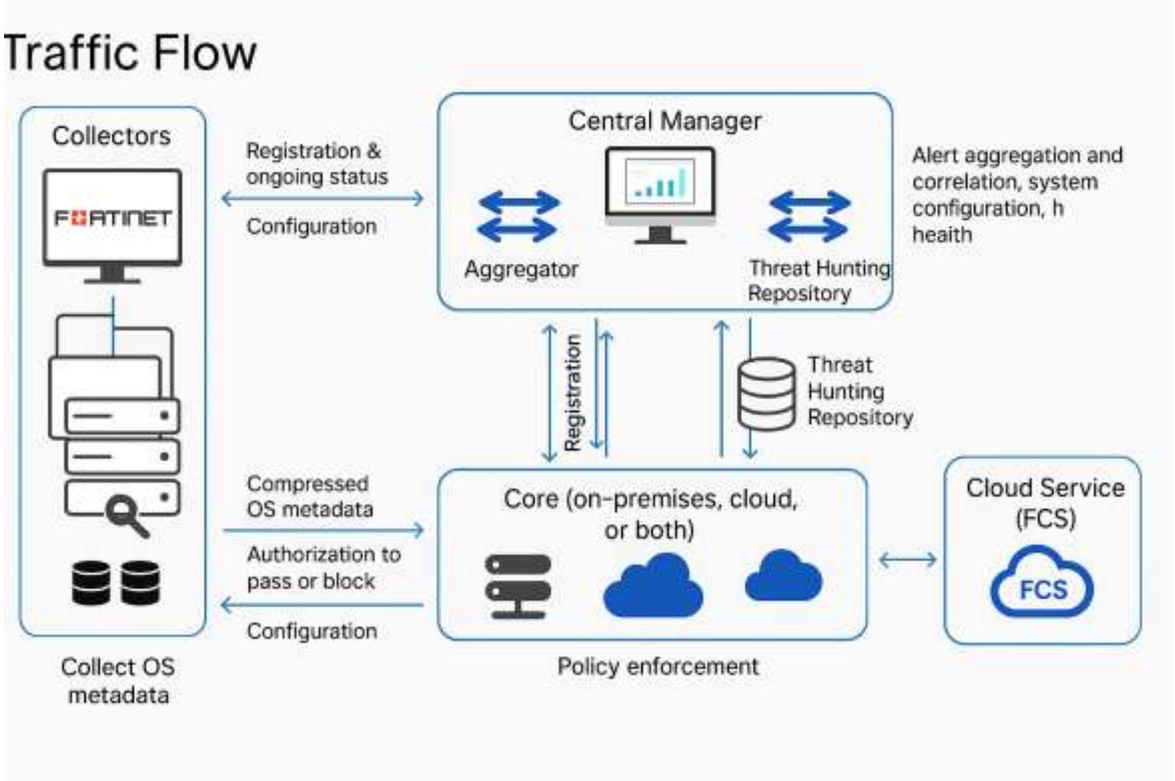
- **The FortiEDR Core identifies malicious requests:** the FortiEDR Core analyzes the collected OS metadata and enforces the policies.

- **Pass or block:** Only legitimate connections are allowed outbound communication.

- **Event Generation:** Each FortiEDR policy violation generates a realtime security event (alert). This security event is triggered by the FortiEDR Core and is viewable in the FortiEDR Central Manager console.

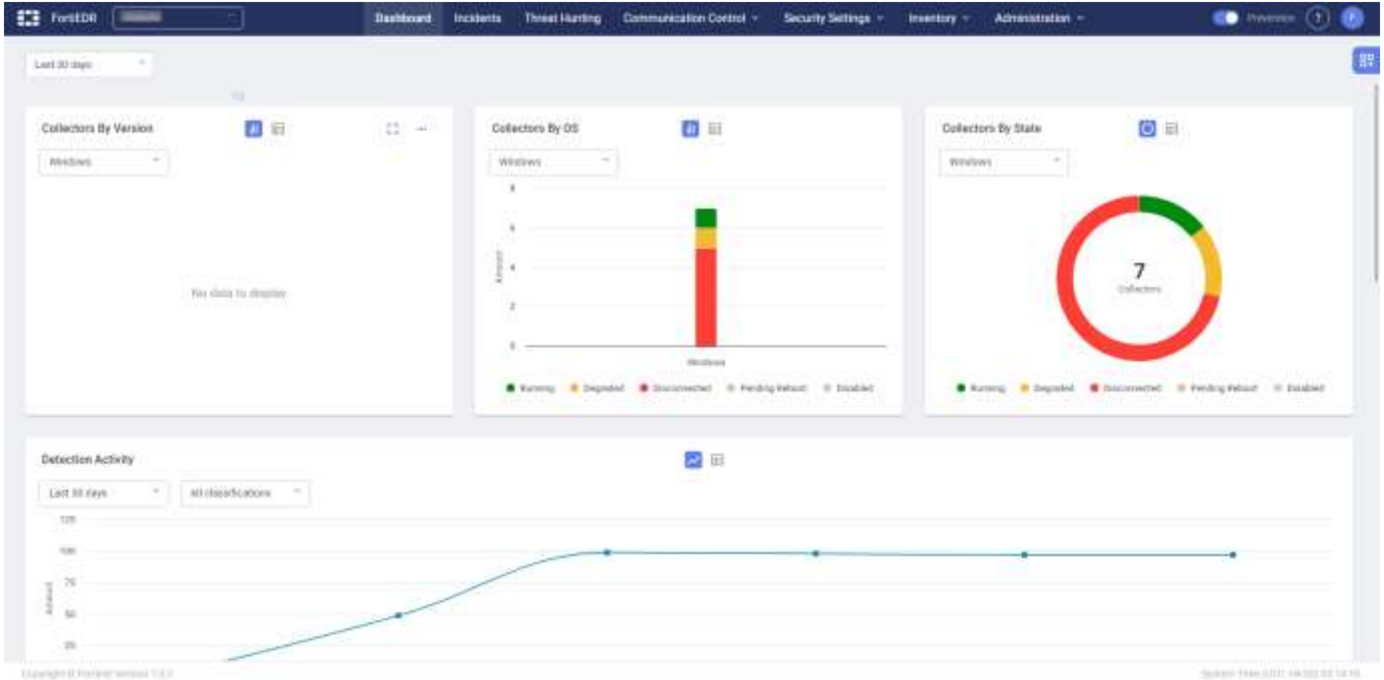
- **Forensic analysis:** The Forensic Analysis add-on enables the security team to use the various options provided by the FortiEDR Central Manager console to delve deeply into the actual security event and the internal stack data that led up to it.

FortiEDR Traffic Flow


Traffic Flow
Collectors
FORTINET
Collect OS metadata
Registration & ongoing status
Configuration
Compressed OS metadata
Authorization to pass or block
Configuration
Central Manager
Aggregator
Threat Hunting Repository
Alert aggregation and correlation, system configuration, h heaith
Registration
Threat Hunting Repository
Core (on-premises, cloud, or both)
Policy enforcement
Cloud Service (FCS)
FCS

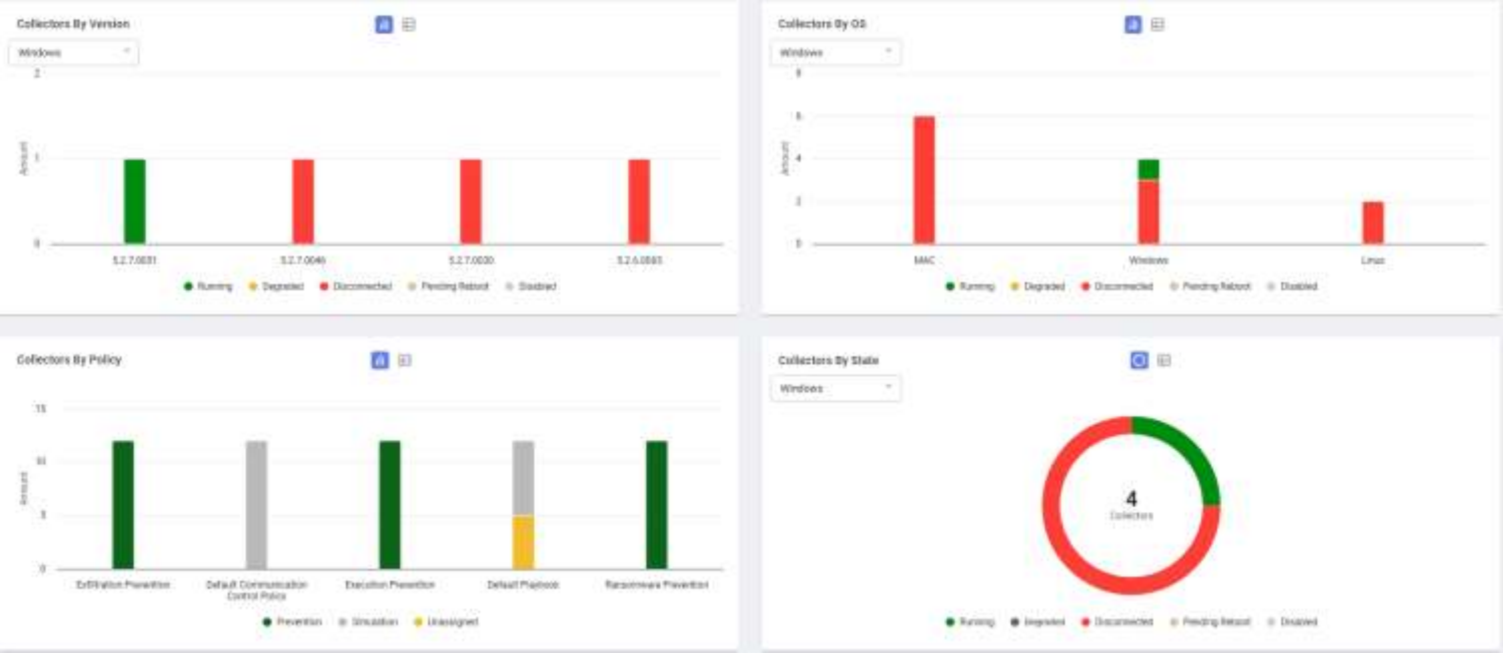
FortiEDR Dashboard

- The FortiEDR Dashboard provides a visual overview of the FortiEDR protection of your organization.



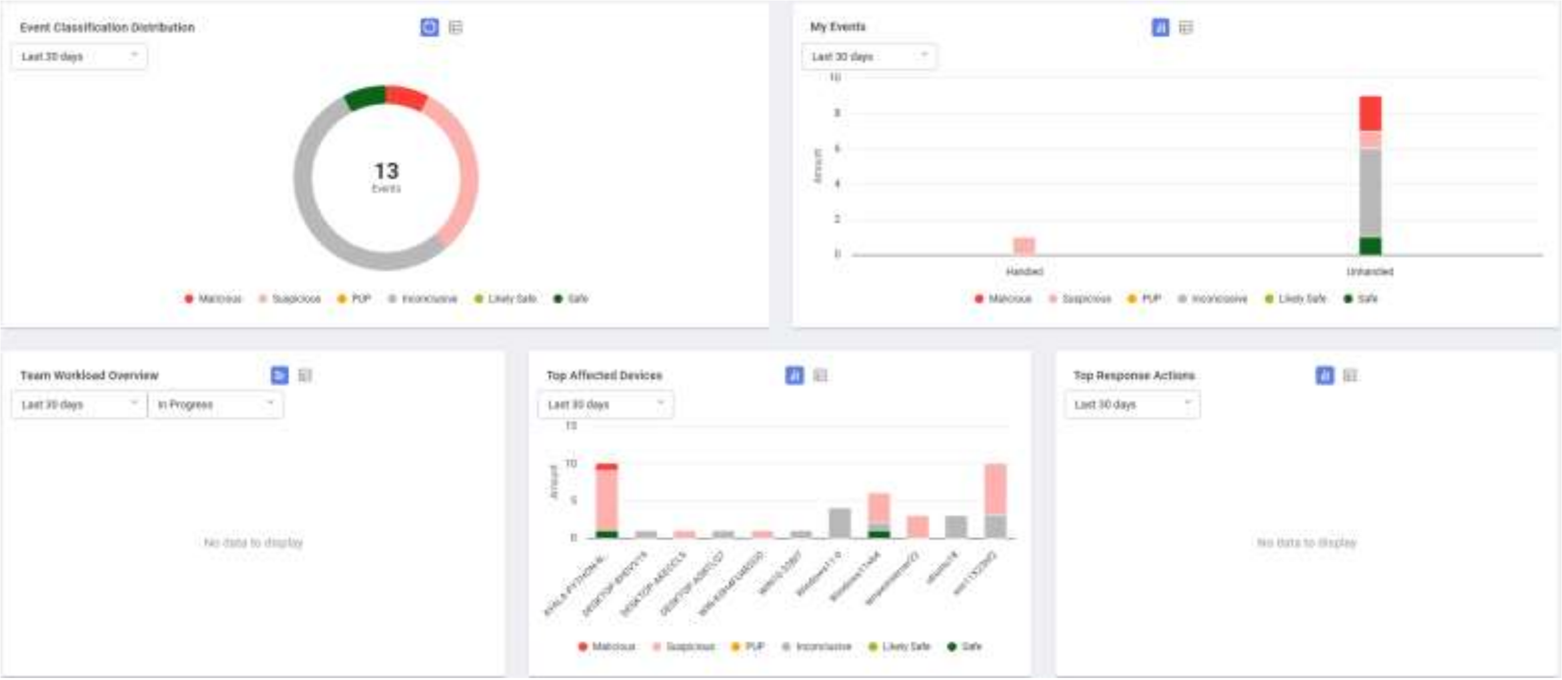
Collectors Charts

- The COLLECTORS chart provides an overview of FortiEDR Collectors. You can view Collectors by OS, policy, state, or version.



Event handling Widgets

- The Event Handling widgets show the number and classification of the FortiEDR security events.


Event Classification Distribution
Last 30 days
13
Events
● Malicious ● Suspicious ● PUP ● Inconclusive ● Likely Safe ● Safe
My Events
Last 30 days
10
8
6
4
2
0
Amount
Handled
Unhandled
● Malicious ● Suspicious ● PUP ● Inconclusive ● Likely Safe ● Safe
Team Workload Overview
Last 30 days
In Progress
No data to display
Top Affected Devices
Last 30 days
15
10
5
0
Amount
● Malicious ● Suspicious ● PUP ● Inconclusive ● Likely Safe ● Safe
Top Response Actions
Last 30 days
No data to display

For more details plz visit below link

- https://docs.fortinet.com/document/fortiedr/7.0.0/administration-guide/354083/introducing-fortiedr

EDR Challenge and Limitation

EDR Challenge and Limitation

1. **High Volume of Alerts (Alert Fatigue)**
   - EDR tools can generate a large number of alerts, many of which may be false positives.
   - Security teams can become overwhelmed, leading to missed real threats.

2. **Limited Visibility into Non-EndpointsEDR**
   - Focuses on endpoints only (e.g., laptops, servers).
   - It does not monitor network traffic, cloud workloads, or mobile devices unless integrated with other tools (like XDR or SIEM).

3. **Requires Skilled Analysts**
   - EDR tools provide raw telemetry and detailed data.
   - Effective use requires experienced analysts to investigate and respond to threats.

4. **Resource Intensive**
   - Agents consume CPU and memory on endpoints.
   - Analysis and storage of logs require substantial backend infrastructure.

EDR Challenge and Limitation Cont.

5. **Can Be Bypassed**
   - Sophisticated malware can evade EDR by using techniques like: Fileless attacks, Kernel-level rootkits.
6. **Integration Complexity**
   - Integrating EDR with existing tools like SIEM, SOAR, or threat intelligence platforms can be complex and time-consuming.

Thanks!

Photo Time