# Anti-Virus

- Protects systems against malwares

**Signatures**

**Database of known malware files**

**AV signatures are updated everyday**

**Anti-Malware**

**Anti-Virus**

- The detection happens in 2 ways

**On-Access**

When a user or system access the file.
Opening a file, downloading the file,
copying the file etc.

**On-Demand**

This is a scheduled run.
Most companies run On-Demand scan once a
week, preferably Thursdays or Fridays

# Antivirus actions

| | | |
|---|---|---|
| **CLEAN** | Remove the malicious code and let the rest of the file run | **Clean Failed** |
| **DELETE** | Delete the file | **Delete Failed** |
| **QUARANTINE** | Put the file in a place where it cannot execute | **Quarantine Failed** |

**Antivirus action helps during alert analysis**

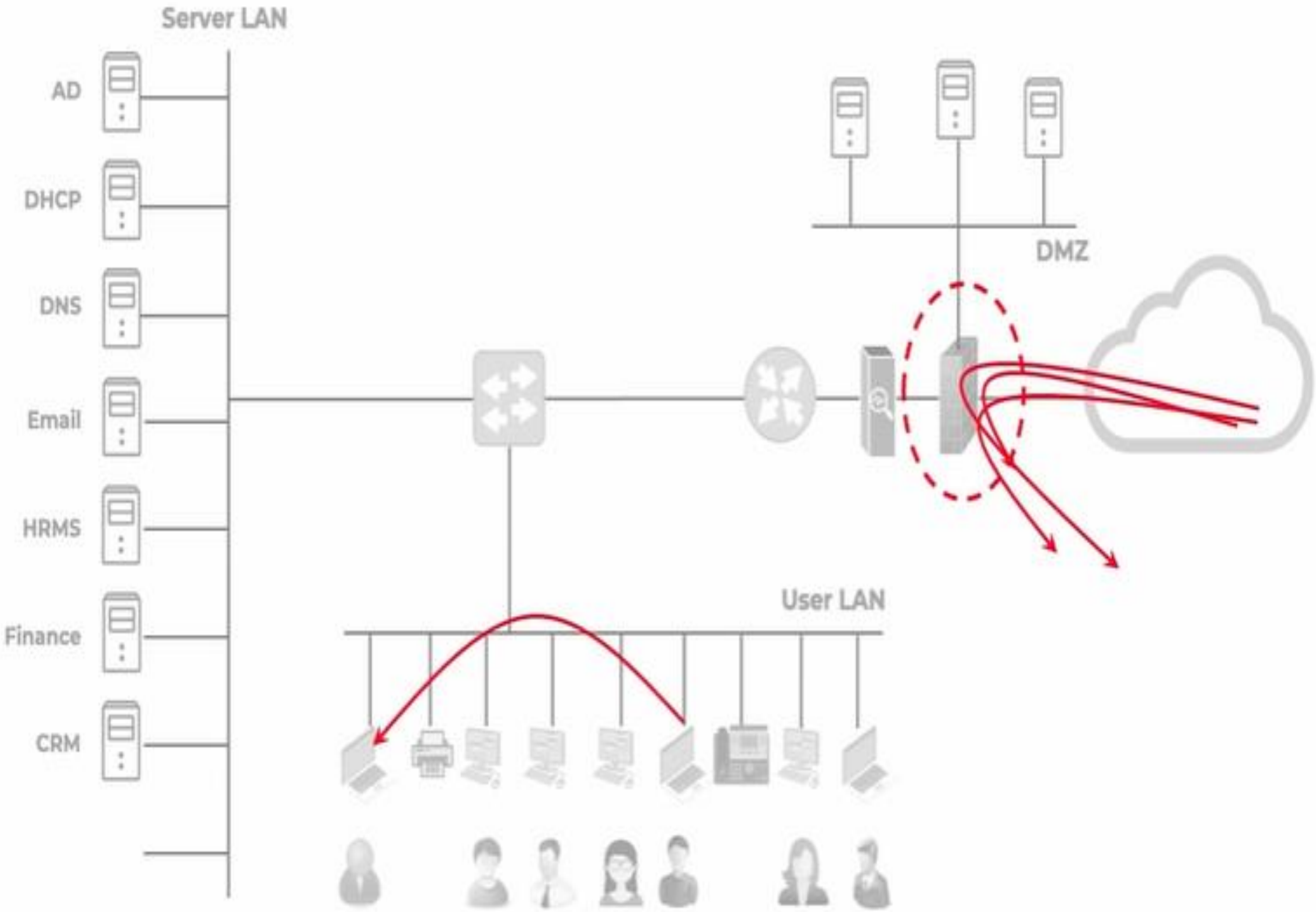
# SOC and AV

- Checking is a system is running with **latest AV signature**

- When a malware detection happens what is the **action taken by Antivirus** i.e. did it clean the file, delete or quarantine.

- During analysis, **we raise tickets and assign them to end-point security team** to run malware scans on the suspiciously behaving host.

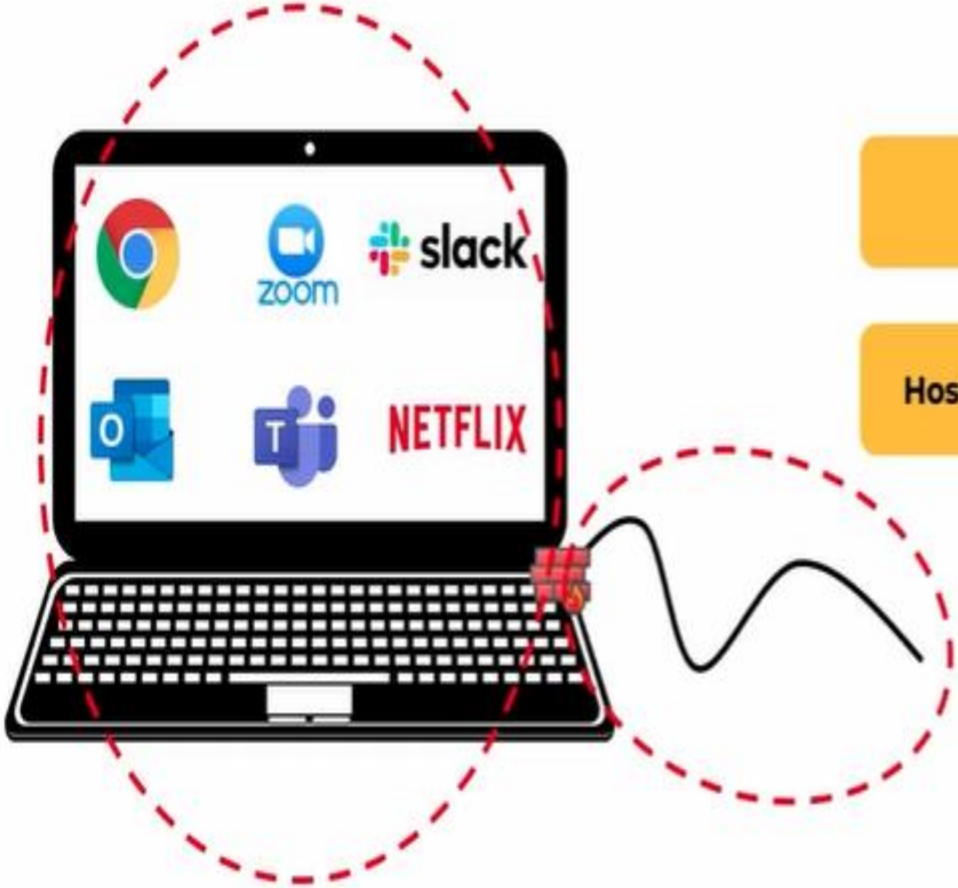
# Host Firewall



## Host Firewall

- Working from home for 10 days
- AV signatures are not updated for 10 days
- Has visited several website for personal work
- Has accessed mails and attachments from his personal email
- **His machine is infected.**
- **Malware disabled Anti Virus.**

# Host Firewall



Firewall Rules (ACLs)

Host Firewall woks at NIC level

# Data Loss Prevention

Data Loss Prevention (DLP) is the practice of detecting and preventing data breaches, exfiltration, or unwanted destruction of sensitive data.

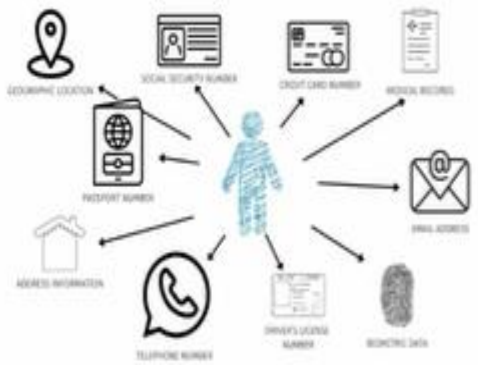
**Data Loss Prevention** - an event in which important data is lost, such as in a ransomware attack.

**Data Leakage Prevention** - focuses on preventing illicit transfer of data outside organizational boundaries.

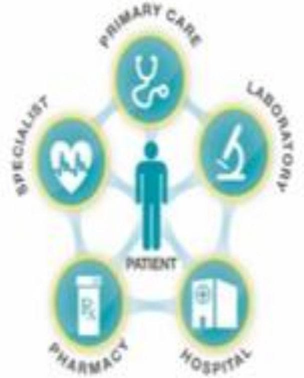
**Comply with regulations**

**Hefty fines are imposed**

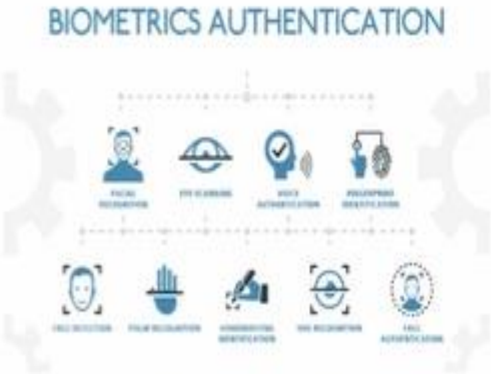
# Sensitive Data



Personally Identifiable Information (PII)



Patient Health Information



Biometric Data

www.socexperts.com
suryaveer@socexperts.com

Credit Card Numbers

Financial/Tax Information

Intellectual Property

Classified Information

# Cause of Data Leaks

Insider threats

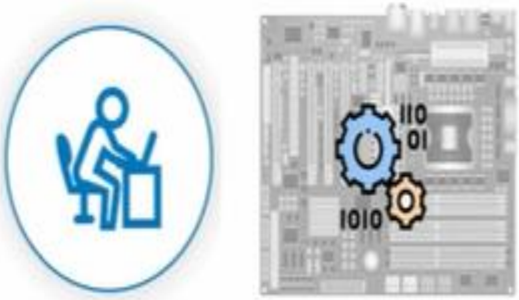
Extrusion by attackers

Unintentional or negligent data exposure

# Data Loss Prevention

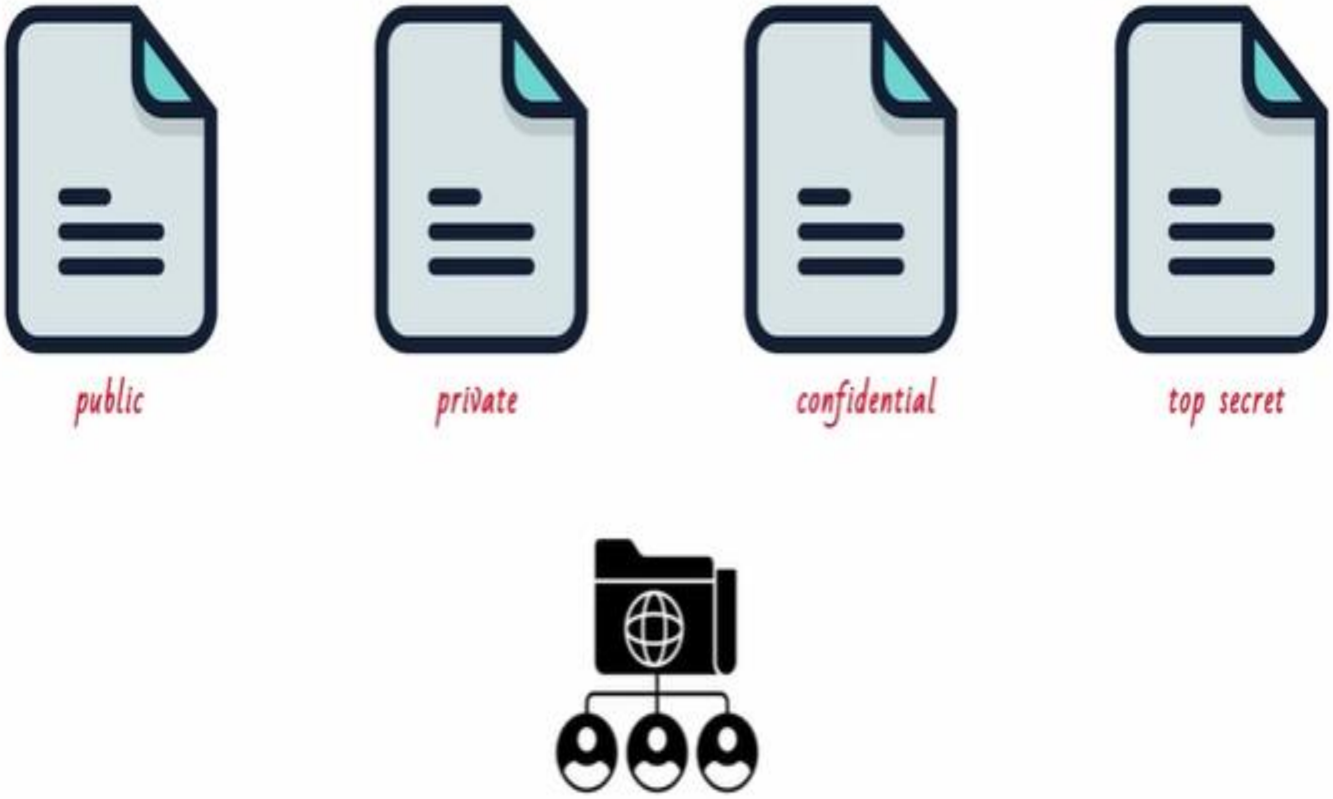
At Rest

In Motion



In Use

# Detect by Classification



public

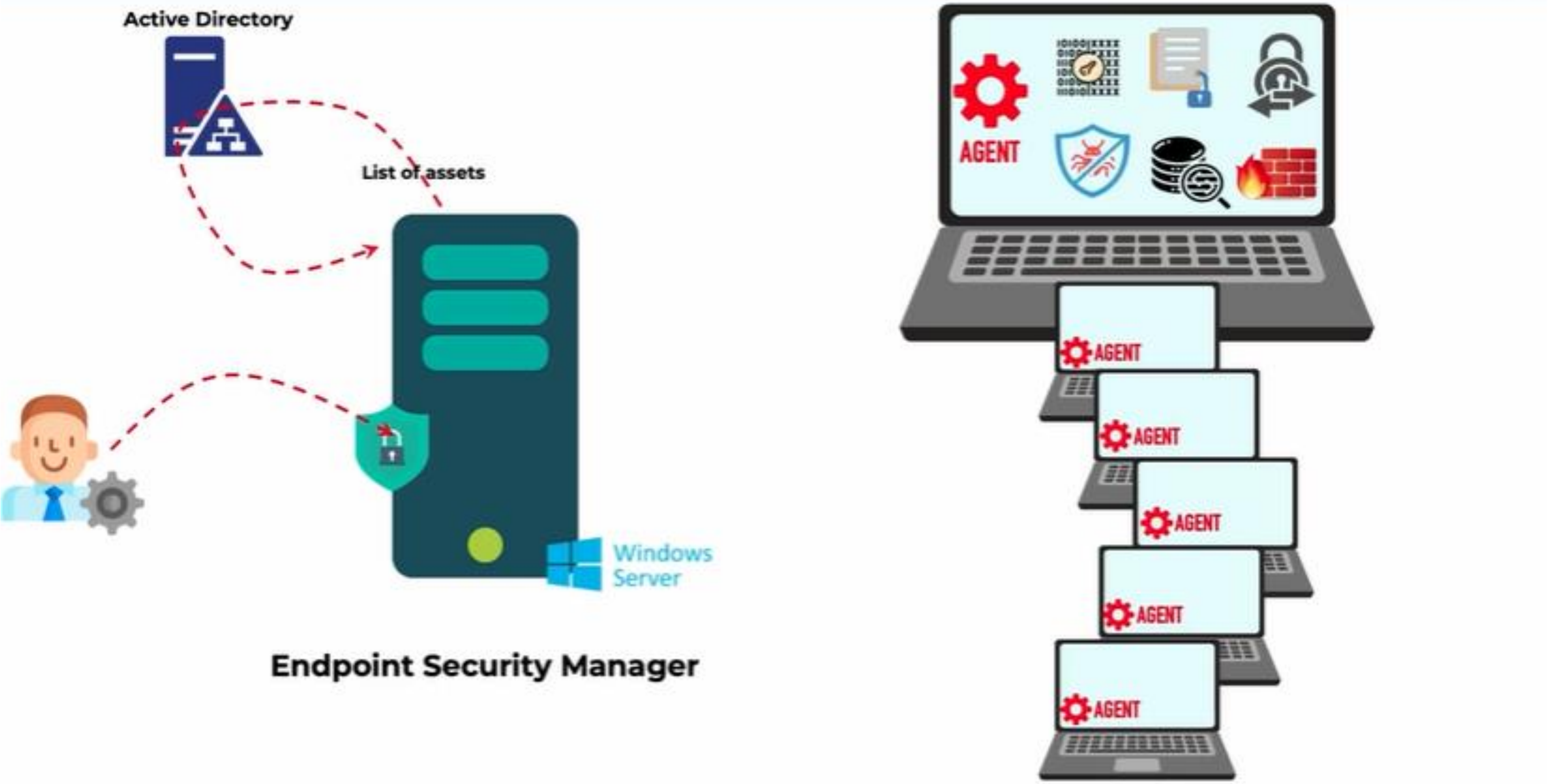
private

confidential

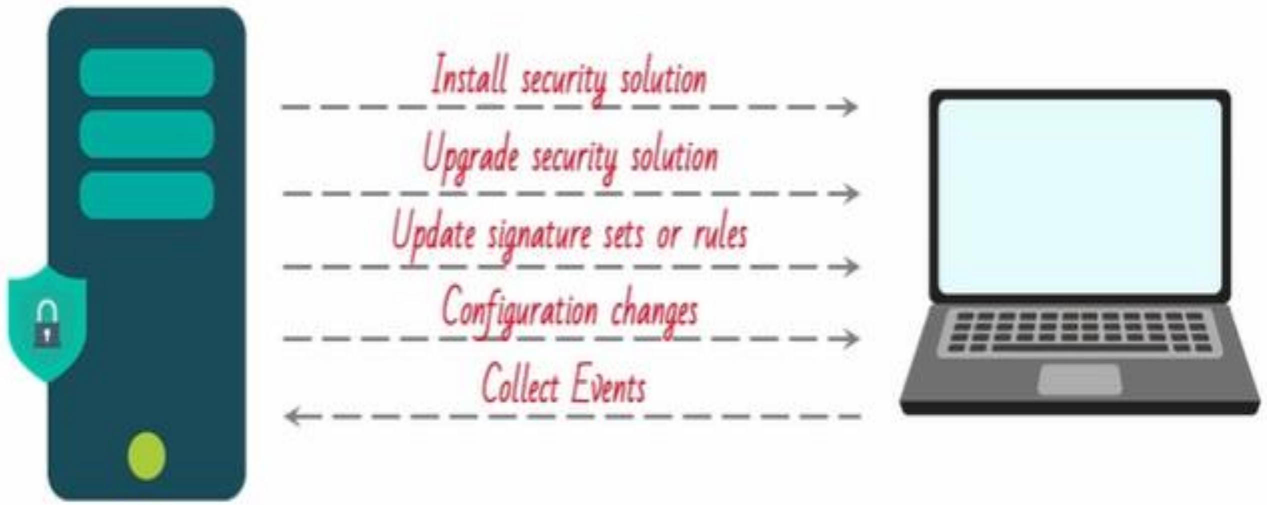
top secret

Active Directory

# Architecture



# Functions of the Endpoint Security Platform


Install security solution
Upgrade security solution
Update signature sets or rules
Configuration changes
Collect Events

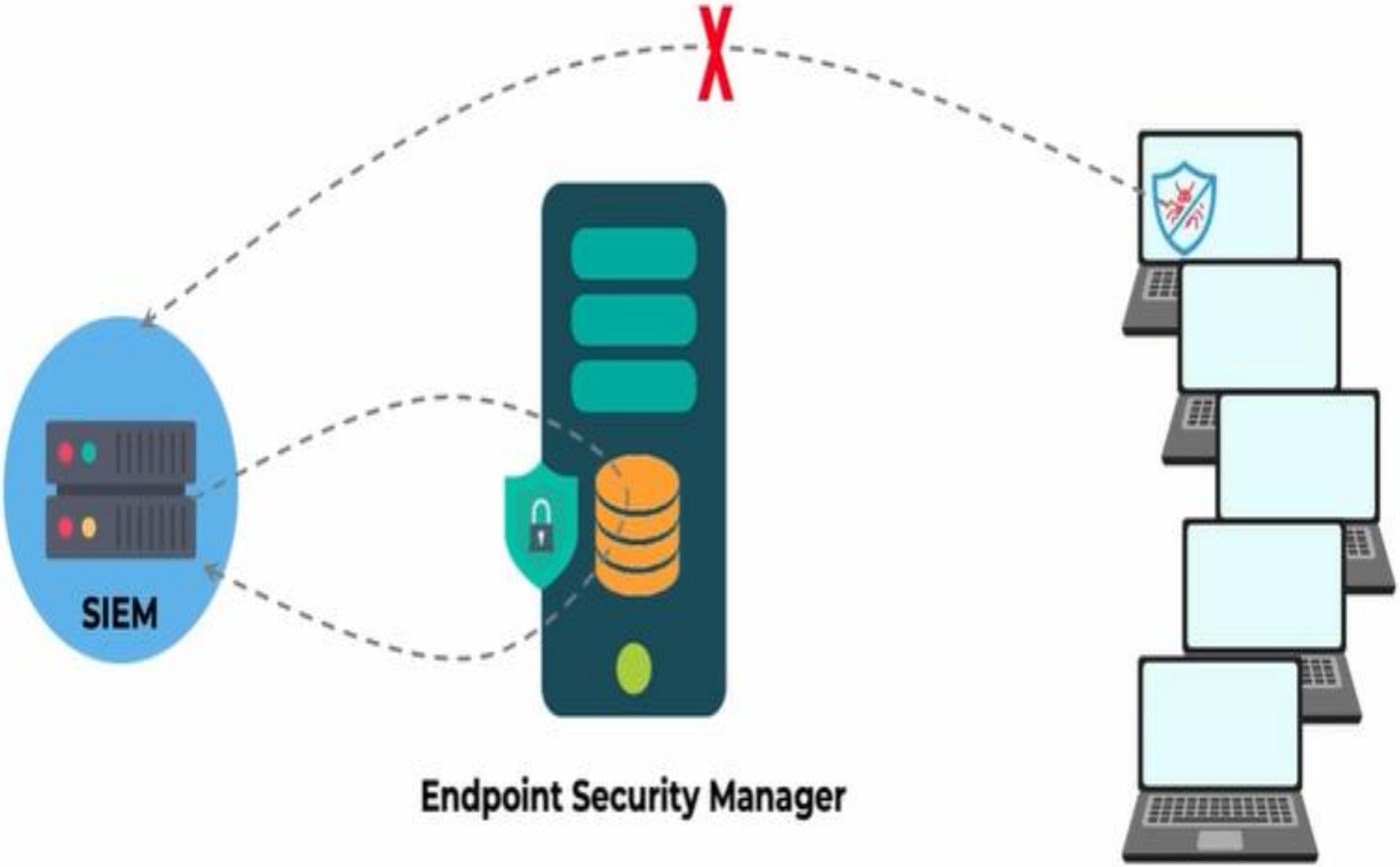
Endpoint Security Manager

Client/Server

**Endpoint Platform is NOT a security solution.**

**Just a manager**

# SOC, SIEM and EPP


SIEM
Endpoint Security Manager