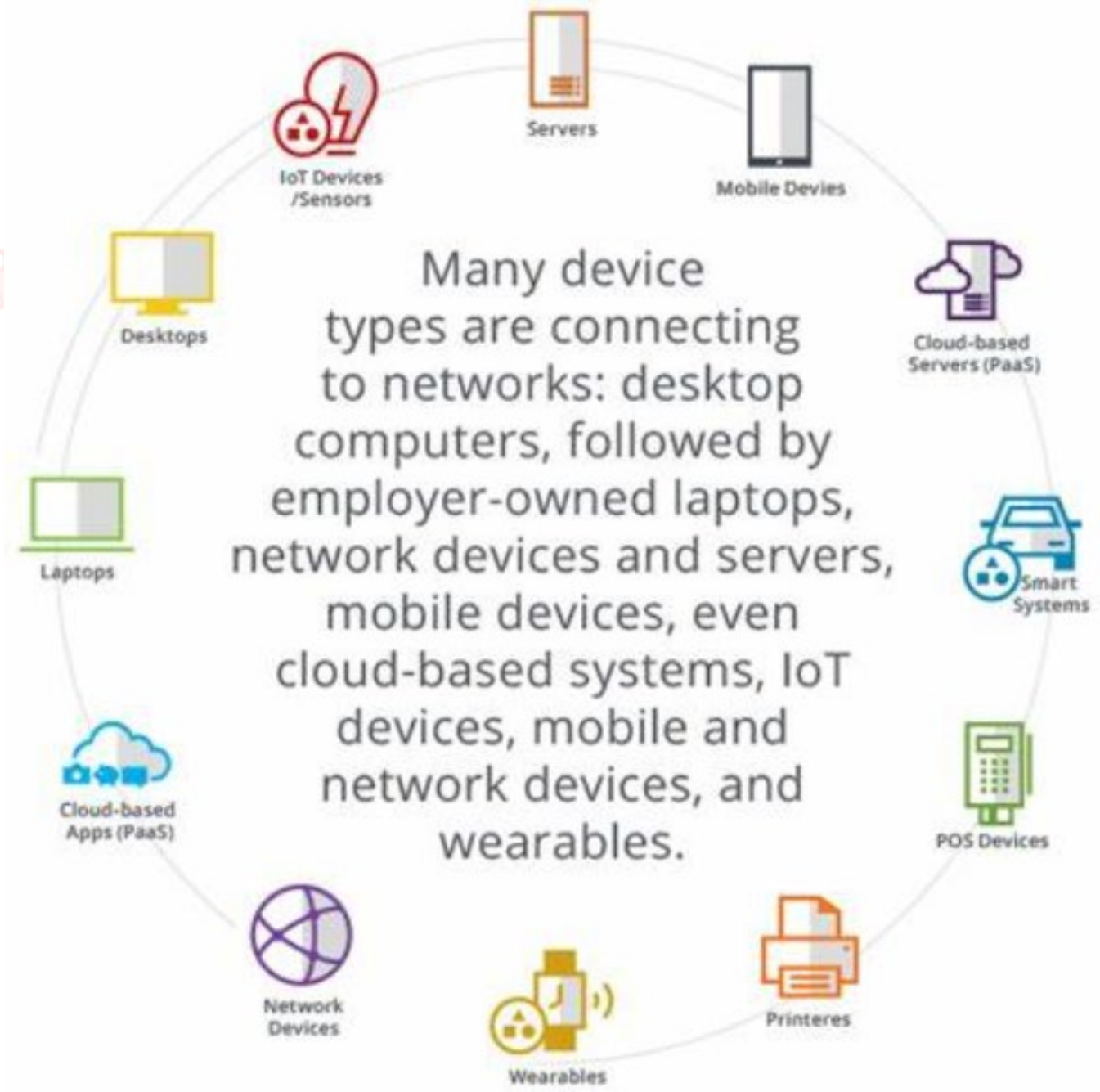
ENDPOINT SECURITY

WHAT IS AN ENDPOINT?

An endpoint is a device that is connected and communicates across a network.

EXAMPLES


IoT Devices /Sensors
Servers
Mobile Devies
Desktops
Cloud-based Servers (PaaS)
Many device types are connecting to networks: desktop computers, followed by employer-owned laptops, network devices and servers, mobile devices, even cloud-based systems, IoT devices, mobile and network devices, and wearables.
Laptops
Smart Systems
Cloud-based Apps (PaaS)
POS Devices
Network Devices
Wearables
Printeres

Hackers use endpoints as the first entry point for cyber attacks and laterally move across to other devices in the network.

EDR

EDR (Endpoint Detection and Response) is a cybersecurity technology designed to identify and respond to advanced threats on individual devices or endpoints within a network.

Note: It’s based on **behavior** NOT only **signatures**

E.g: malware, ransomware, and exploits.

KEY COMPONENTS:

key components of EDR solutions include:

- real-time monitoring
- data collection analysis
- response capabilities.

MONITORING AND DETECTION

EDR solutions continuously monitor endpoint activities, analyzing behaviors and patterns to detect unusual or malicious activities.

DATA COLLECTION:

The types of data collected by EDR solutions:

- logs
- registry changes
- network connections
- file activities.

ANALYSIS AND THREAT INTELLIGENCE:

EDR solution is used to identify known malware and the behavior analysis to detect new or evolving threats.

INCIDENT RESPONSE:

EDR assists in incident response by providing real-time information about security incidents, enabling faster and more effective response actions.

FORENSIC CAPABILITIES:

EDR's forensic capabilities allow organizations to investigate and understand the scope and impact of security incidents.

INTEGRATION WITH SIEM:

EDR solutions integrate with Security Information and Event Management (SIEM) systems to provide a comprehensive security posture.

CHALLENGES AND CONSIDERATIONS:

EDR solutions face challenges such as

- False positives

- Employees privacy

- it requires skilled personnel to effectively utilize EDR solutions.

EDR SOLUTIONS OVERALL

- EDR allows organizations to ensure employees, critical systems, and data are **protected** from **cyber attacks**.

- **EDR** is used to monitor, analyze, and mitigate suspicious/malicious activities within endpoints.

EDR tools example:

Qradar, CrowdStrike, SentinelOne, Carbon Black, FireEye HX