Endpoint Perimeter Detection

Prepared By:
Kazim Ali Obad

Supervisor:

Anmar Mohammed

MOHAMMED .B. HASSAN

Table of Contents

Defining the Endpoint

Endpoint is any device that a person uses, or that acts as a server inside the network. A company PC is an Endpoint. A server is an Endpoint. A mobile phone is an Endpoint. Network devices like a Firewall — those are not Endpoints. A Firewall checks traffic. An Endpoint is where the actual work happens

Network Security	Endpoint Security
Protects the perimeter of the entire network	Protects each individual device (each endpoint)
Examples: Firewall, IDS, IPS, Suricata, Wireshark, NMap, RITA	Examples: WAZUH, Local Firewall, Antivirus, EDR, Sysmon
Checks traffic as it enters or leaves the network	Checks what is happening inside the device itself
A Network Security Engineer specialises in this	A Cybersecurity Engineer spends most of their time here
Catches threats at the network boundary	Catches threats that make it through the network layer

> ***Note:****You have to combine both. Without both together you cannot get complete Visibility. If you only protect the network but not the endpoint an attacker who gets past the network layer runs free on every device. If you only protect endpoints but not the network you never see the threat coming.*

Endpoint Perimeter Detection

Endpoint Perimeter Detection is the second level of security detection.

> ***Analogy :***
>
> *Think of a medieval castle. A castle does not have just one wall it has multiple layers. The outermost wall is the first line of defence. If an attacker breaks through that outer wall, they run straight into the second, inner wall. The outer wall is your Network Security your Firewalls, your IDS, your IPS. The inner wall is your Endpoint Security. If an attacker gets past the network layer, you catch them at the Endpoint layer.*

Every endpoint has two directions of traffic: data flowing into the device (**Inbound**) and data flowing out of it (**Outbound**). Endpoint Perimeter Detection monitors both directions at the device's own boundary, independently of any network-level monitoring that may also be in place.
The Endpoint Perimeter is the second level. If an attacker managed to break through the first level the network we can still catch them at the second level, which is the Endpoint. This is exactly what Endpoint Perimeter Detection means.

- Level 1 Network Perimeter Security: Firewall, IDS, IPS, NMap scans, traffic analysis. This is your first line of defence.
- Level 2 Endpoint Perimeter Security: What happens on each individual device. This is your second line of defence, and the focus of today's lecture.

Every device has two directions of traffic — data coming IN (Inbound) and data going OUT (Outbound). The Endpoint has its own perimeter, its own boundary. Endpoint Perimeter Detection means watching both directions of traffic at that device's boundary and detecting anything suspicious.

Inbound Threat	Outbound Threat
Someone from outside is trying to get INTO your device	Someone already has access and is trying to get data OUT
Example: an attacker running an NMap scan against your server	Example: malware on your machine connecting to a C2 server and sending files
Example: someone sending you malware in a file hoping you run it	Example: an attacker who has already compromised the machine exfiltrating your data
You stop them before they enter	You stop them before they exit with your data
The threat is at the DOOR	The threat is already INSIDE carrying your belongings out

The Insider Threat Complication

We cannot always classify a threat as Inbound or Outbound just by asking whether the person is inside or outside the network. Here is why:

- An attacker might have compromised an internal machine and is using that machine as a pivot point to scan other devices. The scanning looks like it is coming from inside but it is still an Inbound threat from the attacker's perspective.
- There could be a genuine Insider Threat a disgruntled employee with legitimate access who is intentionally stealing data. This looks like Outbound, but it started from inside.

> ***Note :*** *The simple rule to memorise: if someone is trying to exfiltrate data that is* ***Outbound****. If someone is trying to gain access to a device that is* ***Inbound***

If an attacker first breaks in (Inbound) and then starts stealing data (Outbound), what do we call the whole thing?

They are **two separate stages** of the same attack, not happening at the same time.

The Inbound phase is: the attacker is working to get access.

The Outbound phase starts only after access has been established.

> *A C2 connection where the attacker's malware phones home to the Command and Control server is Outbound. Why? Because the traffic is going OUT from your device to theirs. The connection originates from inside your machine going to the outside."*

Detect Attacks at the Endpoint Level

1. External Scanning

External Scanning is you perform a scan on your own server or device from the outside, just as an attacker would. You use tools like NMap or Nessus to identify what ports are open and what services are running.

> ***Note***
>
> *The first thing we need to know is: what ports are open on my server right now? I come in and run an NMap scan, and I look at what comes back. For example, maybe I see Port 135 is open OK, that is normal because SMB uses it. But if Port 4444 shows up that is a Red Flag. Port 4444 is the port attackers use most commonly, especially with Metasploit .*

Why Port Numbers Matter because Every service on a system uses a specific port number. As a Cybersecurity Engineer, you should know which ports are expected on your systems:

Port	Service / Protocol	Status on a typical server
135	RPC / SMB (Windows file sharing)	Expected this is normal for Windows networking
445	SMB Direct (file/print sharing)	Expected normal for Windows file sharing
80	HTTP web traffic	Expected if running a web server
443	HTTPS encrypted web traffic	Expected if running a web server with SSL
4444	Commonly used by Metasploit	NOT expected Immediate Red Flag
4455	Commonly used for custom C2 channels	NOT expected Immediate Red Flag

How Data Exfiltration Uses Ports

Think of a port as a door on your device. When an attacker has access to your machine, they open a specific port let's say 4444. Then from their own machine they connect to that port. Through that door the data starts flowing out. The moment I see a port open that I did not open myself, and I do not recognize its number that is immediately a Flag. That is detection right there, at the Endpoint Perimeter level

Coordination Required Before Scanning

Before you scan, you must coordinate with the Network Team. They need to create a Whitelist for your scanning IP address in the Firewall so that your scan traffic is not blocked or flagged as an attack. You also need to ask them to temporarily disable Deep Packet Inspection on the Firewall for your scan window. Without this coordination, your scan will be partially or fully blocked and you will get incomplete results.

The Limitation The Blind Spot Problem

the problem with External Scanning: you only know what ports were open at the exact moment you ran the scan. What about before you scanned? You do not know. What about after? You do not know. If an attacker opened a port three hours before your scan and then closed it you missed it completely. If they opened a port one hour after your scan you missed that too. This gap is the Blind Spot.

> *We can't run scan every day to eliminate the Blind Spot because Running a scan every day puts significant load and stress on the network. It degrades performance. And more importantly every time you run a scan you need to coordinate with the Network Team, get a Whitelist created, and disable Deep Inspection. Doing this every single day is not practical at all. This is why we need a second method that runs continuously without these constraints.*

2. Internal Watchers

Internal Watchers are tools that run continuously inside the device itself, 24 hours a day, 7 days a week. They do not need you to schedule them, coordinate with anyone, or do anything they watch constantly and alert you the instant something abnormal happens.

> ***Note***
>
> *The Internal Watcher is a tool that lives inside the Endpoint. The moment anything abnormal happens on that device was for example, a new port opens that was not open before the watcher immediately gives you an Alert. It tells you: Hey, a port just opened on your machine. You do not have to wait for the next scan. You do not have to coordinate with anyone. It tells you at the exact moment it happens.*

Examples of Internal Watchers

Tool	Type	What it watches and how
Windows Local Firewall	Built-in (free)	Monitors all Inbound and Outbound connections on the device. Alerts and can block on any new unexpected connection. Shows exactly which ports are open and which applications are using them.
WAZUH	Open Source HIDS	Host-based Intrusion Detection System. Watches files, ports, processes, and system events. Sends alerts to a central dashboard.
Sysmon	Free (Microsoft Sysinternals)	Deep Windows event logging tool. Logs process creation, network connections, file changes, registry changes.
EDR Products (e.g. CrowdStrike, Cortex XDR)	Commercial	Same idea as WAZUH/Sysmon but commercial. Fully automated detection and response. Alerts and can automatically isolate a compromised machine.

When you open the Windows Firewall and look at the Inbound section, you see every open port what service is using it, what protocol, whether it is allowed or blocked. Same for Outbound. This is your live, real-time picture of the Endpoint's perimeter. This is what we mean by Internal Watcher.

> *We can't use SIEM as an Internal Watcher because The SIEM is a centralized log collector. It does not do detection on its own. What it does is collect Logs from everywhere from the Local Firewall, from WAZUH, from NMap results and it centralizes them so you can see everything in one place. The SIEM gives you Visibility. But it does not alert you on its own, and it does not watch anything directly. The Internal Watchers are the ones doing the actual watching the SIEM just gathers their output.*