Cynet

ADVANCED THREAT PROTECTION BEYOND THE AV:

THE SECURITY GAPS NO ONE WILL TELL YOU ABOUT IN EPP/EDR AND NTA/NDR

FOREWORD

In 2020, it is common knowledge that the standard signature-based Antivirus (AV) and Firewall security stack doesn't provide sufficient protection from the rapidly evolving threat landscape.

While large enterprises can cover their attack surfaces with various complementary products, aggregate and correlate their signals in a SIEM, and employ a staff of skilled security operations center (SOC) analysts – mid-sized organizations have to address similar cyber risks with significantly less resources at their disposal.

In practice, the typical mid-sized organization can make a single advanced security investment, leading to the inevitable question: what choice would yield this investment the highest return?

In this paper, we present and analyze the relative strengths and weaknesses of the two prominent advanced threat protection alternatives: the endpoint protection approach of vendors like Crowdstrike and Carbon Black, as well as the Network Detection Rules or Network Detection and Response that is practiced by Darktrace, Vectra Networks, and others. Our analysis shows that while each approach introduces distinct upgrades in the resilience to cyber threats, neither provides the full threat coverage mid-sized organizations actually need.

THE ENDPOINT APPROACH

EPP Endpoint Protection Platform
EDR Endpoint Detection and Response

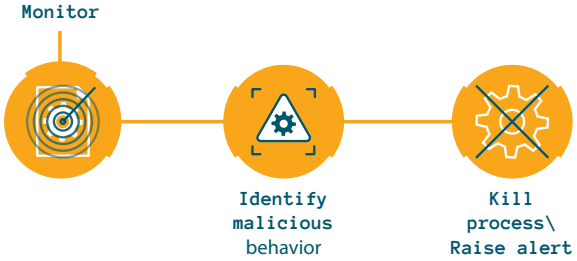
EPP/EDR work through an endpoint agent that supports two main workflows:

FILE EXECUTION PREVENTION

The agent analyzes files before execution and searches for malicious attributes in their format and structure, preventing the execution of the file if such attributes are discovered.

RUNNING PROCESS MONITORING

The agent monitors running processes and either terminates them or raises an alert if malicious behavior is detected.



STRENGTHS

PREVENTION

Both file analysis and process monitoring make endpoint protection an efficient prevention tool against zero day malware, exploits, scripts, and Macros.

DETECTION

Commodity hacking tools such as Mimikatz, PowerSploit, and others generate memory patterns that are easily detectable.

INVESTIGATION

The endpoint agent continuously monitors and records logon activities, internal and external communications, and process executions – providing rich investigation. context.

OPERATION

EPP/EDR can easily replace AV as all AV functionalities are a small subset from the EPP/EDR offering.

WEAKNESSES

THREAT PROTECTION

Limitations

EPP/EDR cannot reliably distinguish between legit use of admin tools (like PSexec.exe , PowerShell, WMI, etc.) and their malicious abuse by attackers performing reconnaissance, credential theft, and lateral movement, resulting in a high rate of false positives.

Blind spots

EPP/EDR are blind to any malicious activity that doesn't entail a distinct process behavior change including a multitude of commonly used attack vectors like ARP spoofing, DNS responder, lateral movement, tunneling attacks, and more.

REMEDIATION

Cyberattacks have a cross-environment impact on endpoints, user accounts, and network traffic. The recovery processes must address all of them. While EPP/EDR can isolate and join endpoints, they have zero capabilities across users and network traffic.

OPERATION

Efficient operation of EPP/EDR alerts requires highly skilled security staff which is practically out of reach for most to all organizations.

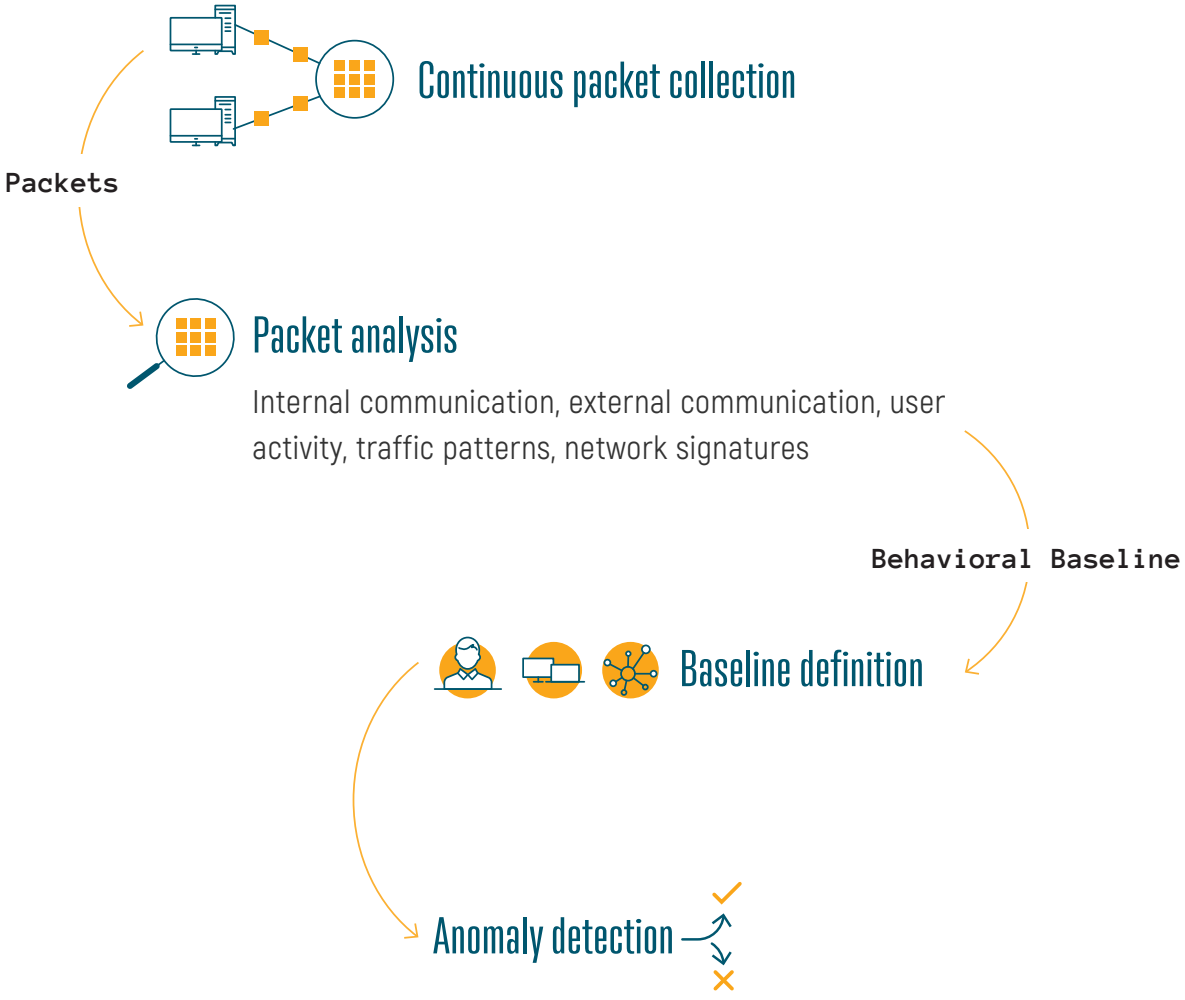
DEPLOYMENT

Many EPP/EDR agents are hard to deploy and clash with existing software on the endpoint. Typically, EPP/EDR projects result in at least 20% undeployed endpoints.

THE NETWORK APPROACH

NTA Network Traffic Analysis
NDR Network Detection and Response

NTA/NDR products connect to a SPAN port on network switches. The SPAN port is a built-in utility in modern switches that produces a real-time replication of all the traffic that runs through the switch and relays it to the NTA/NDR tool. This tool analyzes the packets and builds a behavioral baseline for users, endpoints, and network connections. Once the baseline is established, the network analytic tools can determine whether any given traffic indicates standard state or malicious presence.



STRENGTHS

THREAT PROTECTION

NTA/NDR tools have direct visibility to user logon activities and to the standard communication endpoints, making them efficient in detecting post-compromise activities that reflect anomalous network traffic. Examples of such malicious activity detections can include:

- Malicious authentication through anomalous user activity
- Identity attacks via analysis of DC authentication traffic
- Network-based reconnaissance activities
- Mass automated network propagation (WannaCry style)
- Login attempts that deviate from standard user and network behavior patterns
- Network-based identity attacks (SMB relays, DNS responder, ARP spoofing, etc.)

OPERATION

NTA/NDR are 100% non-intrusive, and do not affect live traffic nor require installation of an agent.

WEAKNESSES

THREAT PROTECTION

Zero Endpoint Visibility and Control

NTA/NDR tools are blind to file activity and process execution on the endpoint as these are not encapsulated in the network traffic. As most attacks start with endpoint compromise, relying on NTA/NDR alone leaves critical security gaps. Even if some attacks can be hunted later down the road, there are many (like ransomware and wipeware) which conclude their entire damage in the initial malicious code execution – NTA/NDR cannot protect against these types of attacks.

Zero prevention

NTA/NDR tools cannot prevent, they can only detect and alert, meaning that malicious activity goes on undisrupted until manual security team intervention.

False Positives

There are many cases in which network traffic alone doesn't provide sufficient context to reliably determine whether a communication instance indeed indicates malicious activity – regardless of the used machine learning algorithm – resulting in high rate of false positives.

REMEDIATION

Cyberattacks have a cross-environment impact on endpoints, user accounts, and network traffic. The recovery processes must address all of them. NTA/NDR tools have zero remediation capabilities.

OPERATION

Efficient operation of NTA\NDR alerts requires highly skilled security staff which is practically out of reach for most to all organizations.

DEPLOYMENT

Any non-trivial network topology creates complexities in deployment that result in network portions that aren't monitored.

CONCLUSION

While each of the analyzed approaches have distinct advantages, neither endpoint protection nor NTA/NDR can be relied on as a single advanced threat protection solution.

From a threat protection perspective, it seems that both approaches complement each other. However, both lack in terms of remediation and operational complexities.

Organizations that want to protect themselves from advanced threats should seek an autonomous breach protection solution that encompasses the threat protection strengths of EPP/EDR and NTA/NDR, along with full remediation capabilities and the ability to be efficiently operated without deep security knowledge.

ABOUT CYNET

Cynet 360 is the world's first Autonomous Breach Protection platform that natively integrates XDR endpoint, user and network attack prevention, and detection capabilities with an incident engine that fully automates investigation and remediation actions – all backed by a 24/7 world-class MDR service. End to end, fully automated breach protection is now within reach of any organization, regardless of security team size and skill level.

To learn more visit **www.cynet.com**