5 THINGS YOU CAN'T DO WITH EDR

1. See all your endpoints

With endpoint protection and detection (EDR), there are so many endpoints that you don't have visibility into or can't manage. Consider internet of things (IoT) devices that can't have an agent installed on it, connected printers in your environment, or rogue laptops and mobile devices that employees and contractors bring onto your network.

2. Effectively address containers and serverless environments

New cloud models, like containers and serverless, are remarkably different from endpoints and more difficult to protect. Current EDR is not designed or optimized to efficiently address these environments.

3. Identify who else may have received a malicious email

Nearly all endpoint threats come from email, but they aren't visible with EDR until an attachment or link is opened on an endpoint. When a threat is identified, EDR can't tell you who else received the email and if/where the undetonated threat may be sitting in other inboxes.

4. Get an overall view of how targeted attacks spread laterally

EDR is only capable of looking at hosts that have an EDR solution installed on them, and therefore can't see the full picture of how an overall attack transpired.

5. Correlate data and activity data across multiple vectors

Security layers are often treated in silos, which allows threats to avoid detection.

You can't break down these silos with EDR. Since you are unable to bring data from network, email, servers, and cloud workloads together, you can't correlate and apply analytics across them to identify threats that may have otherwise gone unnoticed.

THE BEST OF XDR WITH TREND MICRO VISION ONE™

X = multiple layers

Trend Micro Vision One extends detection and response beyond the endpoint to enable more than EDR can offer alone.

Example of an attack:

Step 1. Several people receive a phishing email containing a malicious attachment.

Step 2. One user opens the attachment, which invokes Microsoft PowerShell to establish the initial communication.

Step 3. Attacker proceeds to establish foothold, thus downloading remote access Trojan (RAT) on their system.

Step 4. The attacker can utilize the RAT to run on a remote PC, often using admin PowerShell, as the attacker burrows within the company network.

Step 5. Server communicates with multiple IP address and domains that are used for Command and Control (C&C).

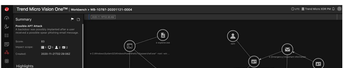
Step 6. The attacker utilizes malware to spread to assets of value and may subsequently use malware to spread to an unmanaged IoT device as to establish further persistence.

How does EDR respond?

Looking at endpoints only, EDR detects the PowerShell activity, sends a grey alert, as on its own it's not indicative of an attack.

How Trend Micro Vision One responds:

- Trend Micro Vision One uses sophisticated XDR capabilities to correlate the PowerShell endpoint activity with the network east-west traffic and the C&C communication with the server. By connecting the dots, it sends a critical detection alert.
- A root-cause analysis uncovers the email where the threat came from and automatically sweeps all inboxes for other copies of this threat. With this information, the security analyst quarantines the emails and stops the threat from impacting other endpoints.
- Threat is isolated and remediated across the environment.
- An indicator of compromise (IoC) is automatically shared with all protection points to prevent any recurrence.



Learn more about Trend Micro Vision One, XDR and how it can help you, visit **www.trendmicro.com/visionone**

TREND MICRO