5 THINGS YOU CAN'T DO WITH EDR

1. See all your endpoints

There are so many endpoints you just don't have visibility into, or can't manage, with endpoint protection and detection (EDR) alone. Consider IoT devices that can't have an agent installed on it, connected printers in your environment, or rogue laptops or 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 than traditional endpoints and more difficult to protect. Current EDR is not designed to address these environments in an optimal way.

3. Identify who else may have received a malicious email

Nearly all endpoint threats come from email, but 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 is 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. EDR doesn't allow you to bring data from network, email, servers, and cloud workloads together so that you can correlate and apply analytics across them to identify threats that may have otherwise gone unnoticed.

THE XDR ADVANTAGE

X = multiple layers

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

Example of an attack

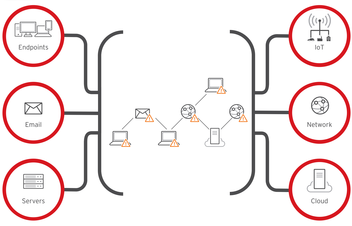
- Several people receive a phishing email containing a malicious attachment
- One user opens the attachment, which invokes Microsoft® PowerShell to establish the initial communication
- Attacker proceeds to establish foothold, thus downloading remote access Trojan (RAT) on their system
- The attacker can utilize the RAT to run on a remote PC, often using admin PowerShell, as the attacker burrows within the company network
- Server communicates with multiple IP address and domains that are used for Command and Control
- The attacker utilizes malware to spread to assets of value and may subsequently utilizes malware to spread to an unmanaged IoT device as to establish further persistence

How EDR responds

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

How XDR responds

- XDR correlates the PowerShell endpoint activity with the network east-west traffic, and the C&C communication with the server. 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 reoccurrence.



Learn more about XDR and how it can help you, visit
www.trendmicro.com/xdr

TREND MICRO