EDR vs XDR

Endpoint Detection and Response (EDR)

- Has a narrow view – only looks at endpoint data
- Doesn't correlate data across threat sources
- Slower to find, investigate and mitigate threats
- Siloed security analytics and data
- Single customer threat hunting & sweeping

Cross-Product Detection and Response (XDR)

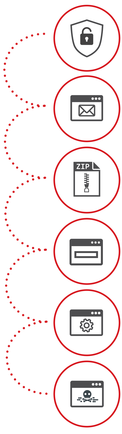
- Has a broad view of the threat vectors – email and endpoint
- Correlates data across threat sources
- Faster to find, investigate, and mitigate threats
- Removes silos by centralizing security analytics and data
- Cross-customer threat hunting & sweeping

THE XDR ADVANTAGE

X = cross-product

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

EXAMPLE OF AN ATTACK



An MSP is responsible for the security management of multiple customers.

A user receives an email with attachment from a fake vendor of their company.

He opens this zip file, and executes the file inside.

The computer looks fine as usual, but in fact a new downloader has been created and added to a Windows Run Key silently.

In this way, the downloader can stay in the device and launch at every system start up.

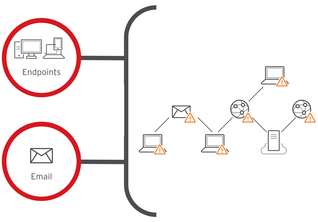
Then the downloader starts to drop different ransomwares regularly to try to encrypt important documents.

How EDR responds

- Looking at traditional endpoints only, EDR detects the PowerShell activity and blocks the ransomware.
- However, the downloader on the infected computer continues to download new ransomware to infect the system.
- Looks at only the endpoints of a single customer.

How Worry-Free XDR responds:

- Based on Trend Micro threat expert rule, Worry-Free XDR will help you identify the three potential threats behind the known ransomware detection, and they will be highlighted in the Noteworthy Events list.
- Since the infection channel is email, Worry-Free XDR will automatically correlate email and endpoint information, and let you know the specific email that triggered the event.
- Furthermore, from our automated sweeping result, you can know which other users also received the same email within the organization.



Learn more about Trend Micro Worry-Free XDR and Co-Managed XDR and how they can help you and your customers, **visit www.worryfree.com**