

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 and 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 and sweeping

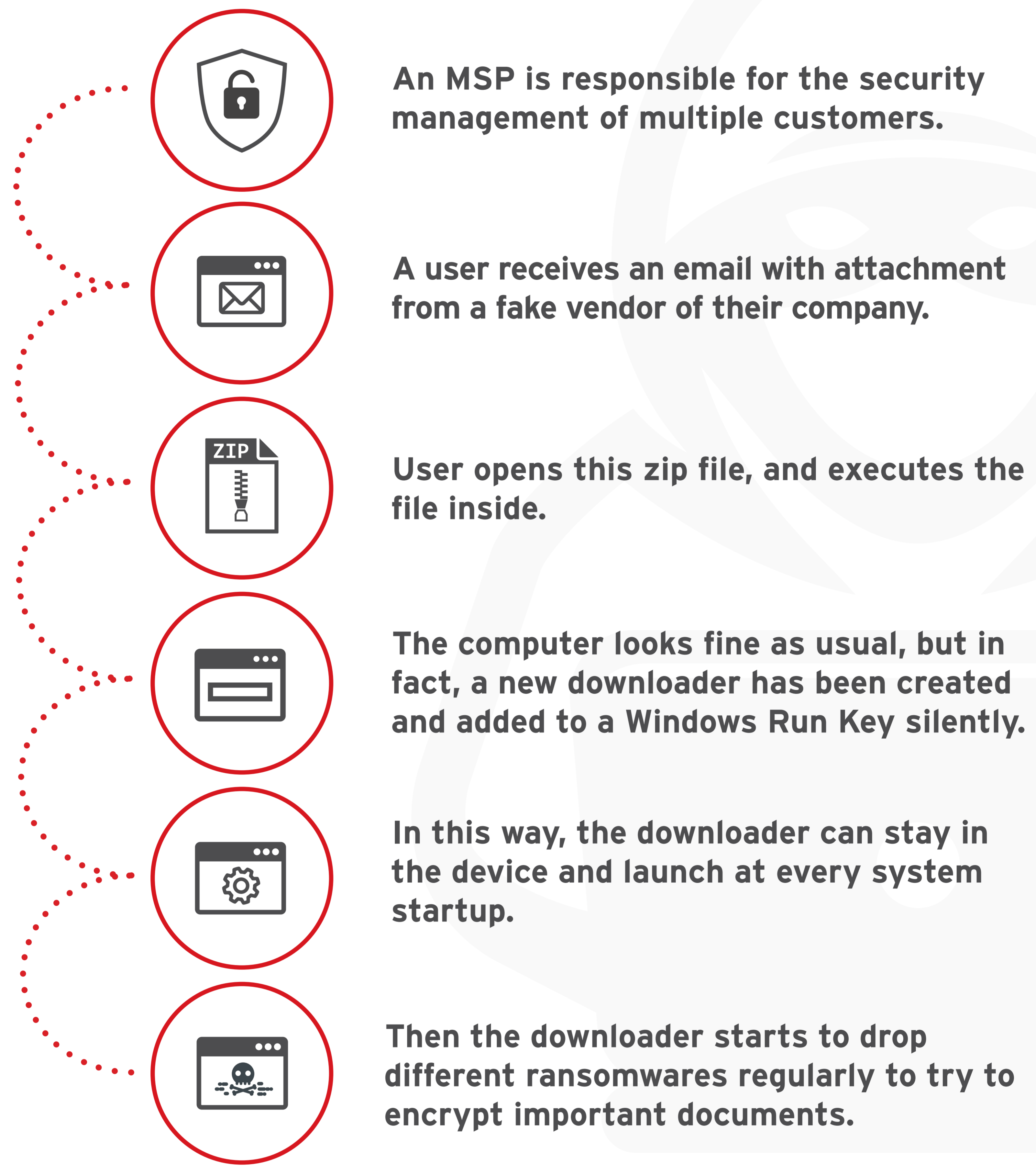
THE XDR ADVANTAGE

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



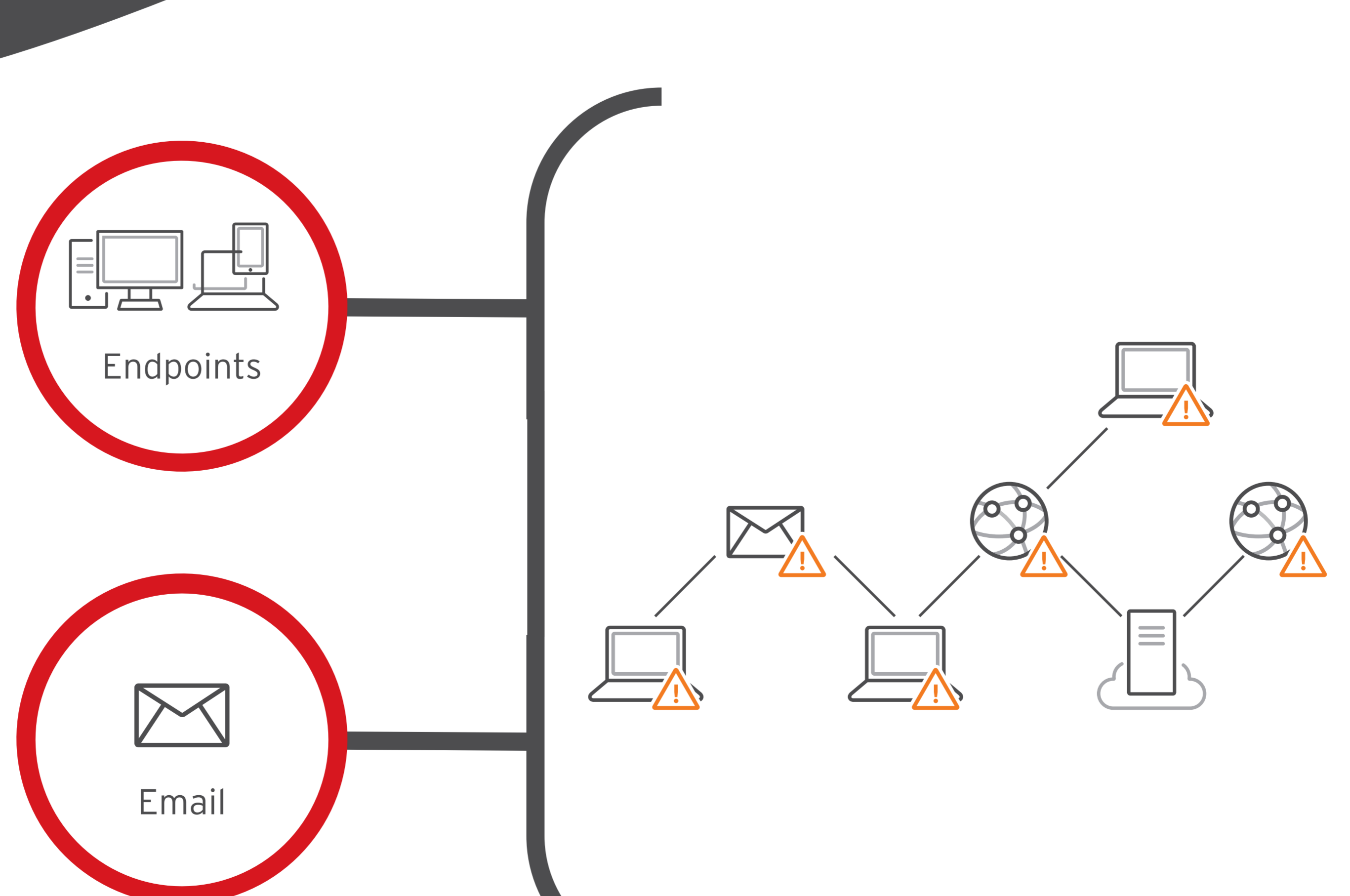
How EDR responds

- 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 Trend Micro™ Co-Managed XDR and how they can help you and your customers, **visit www.WorryFree.com**