Harvest
MSP

Achieve Complete Endpoint Security with AV and EDR

Antivirus software, also known as antimalware, is software used to prevent, detect and remove malware. It was originally developed to detect and remove computer viruses, and for many years it was the primary source for defending networks against ransomware.

Endpoint detection and response (EDR) is a layered, integrated endpoint security solution that monitors end- user devices continuously in addition to collecting endpoint data with a rule-based automated response. See the difference:

Antivirus

Antivirus (AV) tools are good and necessary for protecting endpoints from daily cyber threats. They detect and respond to malware on an infected computer. But because they rely on signature detection or the ability of the software to detect “known threats,” sophisticated threat actors can bypass AV at by using a variety of attack techniques that standard AV solutions simply cannot detect. Additionally, AV software must be updated on a regular basis — if it is not up to date or a threat is not yet known, it will not be detected. This leaves many MSPs and their customers open to ransomware, fileless malware, credential harvesting, data loss and other types of cyber-attacks.

Endpoint Detection and Response (EDR)

Endpoint Detection and Response (EDR) is a layered, integrated endpoint security solution that monitors end-user devices continuously in addition to collecting endpoint data with a rule-based automated response. EDR platforms record and remotely store system-level behaviors of endpoints, analyze these behaviors to detect suspicious activity and provide various response and remediation options. EDR agents collect and analyze data from endpoints and respond to threats that have appeared to bypass protections and continues to analyze, detect, investigate, report and alert your security team of any potential threats in development.

Are both needed?

Yes. Mainstream AV products work well to stop common threats and should always be used to protect endpoints, but because they are signature-based, they often fail to catch zero- day threats, multi-staged attacks, or other types of sophisticated threats. Most traditional endpoint protection products protect endpoints by using a signature-based library of known threats. As such, AV by itself is not enough.

EDR products add additional layers of endpoint security by detecting suspicious behaviors and provide actionable alerts to the threat indicators that matter most. This is done by utilizing advanced technologies, such as behavioral analysis, heuristics - or machine learning, to catch advanced threats that bypass traditional AV solutions. EDR incorporates AV and other endpoint security functionality providing more full-featured protection against a wide range of potential threats.