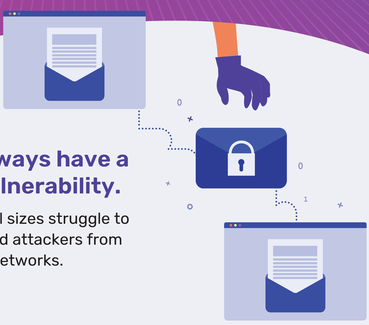
datto

Achieve Complete Endpoint Security with AV and EDR



Networks always have a degree of vulnerability.

Organizations of all sizes struggle to prevent determined attackers from getting into their networks.

Skilled attackers can remain hidden for months, **sometimes years**, before detection.

Differences Between AV and EDR

Antivirus (AV)

AV tools are good and necessary for **protecting endpoints from daily cyber threats** and provide the ability to block a variety of cyber threats, including viruses, trojans and more.

AV relies on **signature detection** or the ability of the software to detect "known threats".

Sophisticated **threat actors can bypass AV at will** by using a variety of attack techniques that standard AV simply cannot detect.

Antivirus 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.

Endpoint Detection and Response (EDR)

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.

Record and remotely store system-level behaviors of endpoints, analyze these behaviors to detect suspicious activity and provide various response & remediation options.

Collect and **analyze data from endpoints and respond to threats** that have appeared to bypass existing antivirus.

Continues to **analyze, detect, investigate, report and alert your security team** of any potential threats even after.

Are both needed?

Yes.

Mainstream AV products work well to stop common threats and should always be used to protect endpoints.

EDR products add additional layers of endpoint security by detecting suspicious behaviors and provide actionable alerts to the threat indicators that matter most.

EDR adds to AV and other endpoint security functionality, providing more **fully featured protection** against a wide range of potential threats.

Learn more