blackpoint

SLICK SHEET

A Closer Look at EDR vs Managed EDR

The Necessary Capabilities of an **Endpoint Detection and Response** Provider:

- Detects malware on endpoint devices
- Utilizes the signature-based detection engine of an antivirus
- Includes machine learning to capture malicious behavior
- Comprehends activity on independent endpoints
- Provides alerts on and isolate threats
- Retains information on threat behavior, root-cause analysis, etc.

The Advanced Services of a **Managed Detection and Response** Provider:

- Provides 24/7 continuous monitoring performed by highly specialized security analysts
- Utilizes in-house technology to gain visibility into tradecraft techniques
- Comprehends activity with machine-to-machine understanding and our live network map
- Understands the network holistically to track malicious behavior between all endpoints
- Makes appropriate, decisive action based on the context of the activity
- Provides immediate response within the first stages of a breach to prevent lateral spread
- Eliminate alert fatigue and false positives

With more and more adversaries abusing trusted IT Tools, next-level protection is critical to withstand advanced cyberthreats. While EDRs do provide necessary malware detection, they are unable to detect tradecraft—techniques used by adversaries to evade companies' cybersecurity efforts. They disguise their behavior as administrative activity by maliciously using trusted tools and executions native to operating systems. When this behavior is performed, EDRs typically fail to detect it, as they cannot distinguish these actions from that of an IT admin moving within a network.

That is why Blackpoint takes a Managed EDR approach, partnering with the EDR of your choosing to ensure the removal of threats occur within the first moments of intrusion. In addition to responding to your EDR alerts on your behalf through our service offering, Managed EDR, we also catch advanced activity that your solution is incapable of detecting.

In 2022, our SOC found that in environments with an integrated AV/EDR, 86% of their responses involved no alerts from the integrated tool. These solutions aren't comprehensive and would have likely alerted the threat further down the attack chain once malware was in use. In that case, the impact of the breach would be higher. Therefore, detection prior to the execution of malware is mission critical.

WE CURRENTLY INTEGRATE WITH:

- Bitdefender
- CrowdStrike
- Cylance
- Malwarebytes
- Microsoft Defender for Endpoint
- SentinelOne
- Sophos

If you're ready to provide backup for your EDR and stand firm against innovative threat actors, set up Managed EDR with your preferred endpoint security solution today.

BOOK A DEMO TODAY

blackpointcyber.com