Endpoint Detection & Response Is Not Enough

Only One Piece of the Security Puzzle

Unify Your Security Arsenal

- EPP focuses on preventing well-known attacks, but cannot detect unknown or zero-day threats.
- EDR detects and responds to unknown threats on endpoints, but does not provide network visibility
- MDR leverages your existing endpoint and network solutions and creates a unified view of security posture

A war cannot be won on one front with a single arsenal–you need a well-trained army, navy, and air force. Likewise, fending off criminal hackers requires a diverse pool of technologies and trained security experts that tried and tested practices for the best results.

Nevertheless, small and medium-sized businesses are often forced to choose between tools and services that perform different functions. One of the more popular solutions they've settled on in the past few years, according to Gartner, is endpoint detection and response (EDR). While EDR is an important part of a security strategy, it isn't enough by itself.

Endpoint protection (EPP)

Endpoint protection (EPP) focuses on preventing well-known attacks based on existing signatures. Firewalls, web filters, and application whitelisting and blacklisting identify known threats and stop them from executing. These tools are centrally managed and typically quick to deploy, making them convenient resources.

However, EPP is not made to detect unknown or zero-day attacks, and they provide no network visibility. So, for example, if an intrusion has already occurred, a hacker can exfiltrate critical data undetected. Likewise, keyloggers or entirely new forms of ransomware can communicate with command and control servers unbeknownst to anyone. In this way, EPP is necessary, but also very limited.

Endpoint detection and response (EDR)

Unlike EPP, EDR enables customers to detect security incidents, investigate them and even remediate them on endpoints. This provides a level of visibility into endpoints that EPP cannot; EDR can detect unknown threats through forensics tools that detect anomalous behavior. So while EPP holds down the fort against the known threats, EDR identifies and interprets anything unusual living on an endpoint. There are caveats, though. First, EDR

has blind spots. EDR cannot provide visibility into an endpoint without an EDR agent. Second, EDR requires security staff that is trained in detection and response. This is feasible for most large enterprises, but not for SMBs. Finally, EDR doesn't provide network visibility. Threats that sneak through can move laterally across the network, and clandestinely talk to a remote C&C server, uninhibited.

Network monitoring, data security and the SIEM

The complement to EDR's functionality is continuous network monitoring. While EDR provides endpoint visibility, network |monitoring shows you what is actually happening on your network. Simply put, you need both.

Heavily regulated industries also need data and application protection that can safeguard their crown jewels: the actual data hackers would seek to steal and then sell on the dark web.

Lastly, there's security information and event management (SIEM). This is the hub that aggregates flow logs from EDR and network monitoring together into a single management platform. The only downside of this log data aggregation and correlation can take a long time to implement (6 to 12 months), and management and/or licensing is quite costly.

MDR: Completing the picture

MDR focuses holistically on improving an organization's security posture.

In a recent webinar Senior Director of Product Marketing at Arctic Wolf Networks Narayan Makaram explained how MDR helps SMBs create the equivalent of a security operation center (SOC) at an affordable price with little-to-no security expertise in house.

Specifically, MDR supplies log aggregation (SIEM), remote continuous monitoring, threat triaging and incident response, and 24/7 access to a concierge security engineer. Organizations can continue to use their existing EPP, EDR and data protection solutions, but MDR will aggregate those logs, continuously monitor them, triage events and provide incident response guidance.

To hear more about how MDR creates a unified security environment that can protect against even the most nuanced of threats, watch Makaram's webinar, available here

ARCTIC WOLF

Contact us
arcticwolf.com
1.888.272.8429
ask@arcticwolf.com