Requested by client: I am looking to build out a small section of technical overviews on the topics of: Endpoint Detection and Response. Sub-sections should include: What is Endpoint Detection and Response? How EDR works How Companies use Endpoint Detection and Response to Secure EDR Tools Threats Mitigated by EDR Shortcomings of EDR Tools The content should be written without voice, be agnostic and informative providing useful links and references to any factual claims. 1,500 words.

What is Endpoint Detection and Response?

Endpoint detection and response, or EDR, refers to the assortment of solutions used to continuously monitor the relevant hosts or endpoints of a system to obtain the comprehensive visibility necessary to identify, investigate and mitigate advanced internal and external threats. Enterprises can include EDR as integral part of their cybersecurity infrastructure and strategy to quickly and efficiently mitigate endpoint infiltrations and to stop system failures, thefts or loss of data. EDR tools gather, record, store and analyze the significant amounts of data produced by endpoint activities and are critical factors in threat hunting, a proactive and aggressive defense strategy against threats.

According to the U.S. Department of Commerce's National Institute of Standards and Technology (NIST) Cybersecurity Framework, a network security program should adhere to a methodology that has not only preventative features, but also detection and response capabilities. Endpoints, such as laptops, desktops, tablets, servers, smartphones and printers, are the preferred targets of cybercriminals, as they are considered the weakest aspect of the IT system due to their quantity, software vulnerabilities and susceptibility to human error. While enterprises can implement preventative endpoint protection measures with traditional antivirus tools, attackers are still capable of penetrating the endpoints of networks because of the inventive techniques employed to compromise the systems without setting off preventative endpoint protection defenses (such as automatically preventing new files from entering a system if they have been flagged as malicious).

Because the majority of advanced threats can circumvent automated defense measures, it is important that humans are able to intervene to stop the threats. EDR prioritizes providing actionable insights that help security analysts to quickly identify indicators, such as certain behaviors and patterns, that are left behind by attackers as they attempt to infiltrate systems. It can provide an accurate view of how a threat originated and how much damage it has caused. Security analysts are also able to use EDR insights to take the appropriate actions to mitigate the threats.

How EDR Works

According to Gartner Research, valid EDR solutions should have the following capabilities:

- Security incidents detection
- Containment of the incident at the endpoint
- Remediation of endpoints back to a pre-infection condition

While the various EDR solutions available may have differing capabilities and features and there are unique methods that are used to execute the solutions, the purpose of all EDR solutions remains the same: to provide a way for security analysts to detect, investigate, isolate and eliminate the intrusions and threats across of the endpoints of a system. It is also important to note that as with all cybersecurity tools, EDR is not intended to be used as a stand-alone cybersecurity solution.

All EDR solutions have certain critical processes:

- **Monitoring.** Continuous monitoring of endpoint of the activities and events taking place within the network is critical. Monitoring encompasses the integration and use of different endpoints, software platforms, digital settings or hardware elements.

- **Recording of Events**. A central database is used as the recording place for the events occurring within the network through the collection of different endpoint. Software agents are installed on the host system to serve as the foundation for event monitoring and reporting. Data sources may include sockets, memory dumps, IP addresses, DNS, system calls, hardware types, registry and more.
- **Analysis.** The recorded events are analyzed for potential threats and intelligence that can be leveraged for multiple tasks, including informing protection strategies, identifying suspicious activity and investigating, reporting and issuing alerts of potential threats for security analysts to investigate. Security analysts will be able to prioritize the alerts, have full visibility of the extent of intrusions and take the necessary actions to nullify the threats.

Additional security capabilities of EDR include, but are not limited to, application management, device management, encryption data encryption and network access control.

How Companies use Endpoint Detection and Response to Secure EDR Tools

IT security teams can use EDR tools to surveil a system, giving them the visibility required to investigate past incidents or to implement proactive searches for threats in their environment. The tools provide the capability of isolating an event so that is does not expand and compromise other parts of the network environment.

In order to make the best decisions regarding how to best secure EDR tools for an enterprise, it is important to conduct an uncompromising examination of the enterprise, its objectives, and network systems. Multiple questions should be addressed to ensure that the solutions that are being obtained are in the best interest of the enterprise:

- What business problems are the EDR tools meant to solve?
- What has to be done to limit the enterprise's possible risk exposure?
- How will the EDR tools impact the performance of the devices that they are meant to protect?
- Will the EDR tools complement or integrate with the enterprise's existing tools and platforms?

Threats Mitigated by EDR

EDR facilitates the detection of the threats that can bypass antivirus or next-generation antivirus across all endpoints of a system. The design of EDR tools allows security professionals to understand how attackers are able to infiltrate the network. EDR tools identify the route the activities follow, allowing security professionals to see how attackers learn about the network, migrate to other endpoints and try to accomplish their goals in the attack. EDR provides actionable insight to combat:

- **Known and unknown malware.** There are many vulnerabilities that can be exploited by attackers to launch various types of malware, including crimeware, adware, spyware, viruses, worms, ransomware and more, with the vulnerabilities only being noticed when the breach has occurred. EDR applies sophisticated logic that is able to identify patterns of related events that may not seem malicious on their own, but can indicate malicious intent when taking place simultaneously.
- **Fileless attacks**. Because fileless malware attacks do not adhere to the path usually taken by traditional malware, conventional antivirus tools are unable to provide sufficient protection. Fileless malware is executed using existing software, authorized protocols and applications. The monitoring of how one event leads to and relates to another is necessary to detect such attacks. EDR tools are able to monitor

many aspects of a system, such as the activity of users, applications and services, related processes, inbound and outbound network traffic, requests to run applications and changes to credentials or permission levels. Records are maintained on what initiated the events, allowing the EDR tools to not just monitor individual events on an endpoint, but also rather monitor and analyze the relationships among them.

- **Phishing**. To mitigate phishing attacks, it is necessary to immediately and accurately detect any malicious links visited, attachments opened and the downloads that resulted from those actions. EDR allows the constant monitoring, detection and response that is necessary.

Shortcomings of EDR Tools

While EDR tools provide a number of benefits for enterprises wanting to locate the indicators of the threats that are jeopardizing their systems, the tools do present certain challenges:

- **Poor scalability.** The increased visibility provided by EDR relies on an increased amount of data, which requires an increased amount of analysis. The resources this requires, including bandwidth, money, time and a properly skilled personnel, many EDR technologies cannot be scaled properly to adjust to an organizations changing needs.
- **False positives.** False positives occur when alerts are issued when there have been no malicious activity. In addition to diverting staffing and financial resources away from real issues, false positives can also leave an enterprise more vulnerable to an actual attack. Enterprises have to develop a balanced approach between detection and alerting and preventing real malicious activity. However, this can be difficult to accomplish without being bombarded with false alerts
- **Slow reaction times for cloud-based EDR tools.** One of the most important challenges in EDR is the need to minimize the time that elapses between when an organization detects a threat and develops an appropriate response, as well as the time it takes for an organization to take that response and incorporate it into preventive security measures. For some cloud versions of EDR, some data and logs are transferred to the vendor's cloud storage instead of being held in the centralized database or on the software agents installed on the endpoints. This results in slower reaction times for detecting and responding to suspicious activity, and in some cases, results in no reaction. Having to want for a response from the cloud or for the security personnel to take the appropriate action to end the attack hinders the effectiveness of the EDR tools.
- **Personnel with highly personalized skills.** Even though EDR tools can help increase the visibility of a system, that and all of the other benefits they provide can be absent if there is no qualified and trained security staff to interpret the events and take the appropriate actions. The implementation of EDR tools can be very complex and requires that security personnel handling them have extensive experience with data exfiltration, network traffic, API calls, system and data integrity, file systems and more.