Considerations for Evaluating Endpoint Detection and Response (EDR) Solutions

Endpoint security solutions range from signature-based endpoint protection platforms (EPP) or antivirus (AV) solutions to extended detection and response (EDR) platforms that tie multiple security solutions together.

Organizations that are evaluating endpoint detection and response (EDR) solutions need to ensure that the products they are considering will meet their needs in the following areas.

1. **Threat Protection**
   Any evaluation of EDR solutions needs to start with this product’s ability to reduce the attack surface and to protect against the current and future threat landscape.

2. **Ransomware Defense and Recovery**
   Solutions should determine the level of data exfiltration and file deletion (EDM) capabilities of the ransomware defense and ransomware antidote features in multiple types of systems.

3. **Anti-tampering**
   An EDR solution should act as a zero-trust firewall to protect the system against system attacks or the manipulation of files and applications.

4. **Operating System Support**
   Make sure your EDR solution can support the overwhelming majority of operating systems, including intruder and working from any patterns, and ensure your solution is the same for both services and administrators.

5. **Resources**
   While virtualization and containers can have a considerable impact on system resources, organizations should look for solutions that use less than 1% of CPU utilization.

6. **Automation**
   Monitor and protect the security operations center (SOC) or IT staff, as they can focus on other tasks. Also consider how it may integrate with other security-related applications and services.

7. **Managed Services**
   Reduce the burden by augmenting your staff with your EDR vendor’s external incident response staff. Make sure these teams match your security policies and are aware that EDR services are not outsourced to a third party.

8. **Threat Hunting**
   Advanced threats may move laterally across the network through memory and other communications. Ensure your solution identifies threat hunting in real-time but isn’t just watchdog, and that the solution can signal threat status data for up to 90 days without paying for storage.

9. **XDR Readiness**
   Although you may not be ready to move to an EDR platform, you need to be ready to shift your current EDR solution or EDR real-time integration with your EDR and other security solutions. Find out how other vendors think about the product and if they are ready to support all endpoints to network where they are and how they connect.

10. **Conclusion**
    Not all EDR vendors are the same. To find the right solution, organizations need to get answers to critical questions about the product, the company, and the service. Find vendors that are ready to support all endpoints to network where they are and how they connect.