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) solutions that tie together multiple security solutions.

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 protect against the current and future threat landscape.

2. **Ransomware Defense and Recovery**
   Solutions should determine the level of stealthiness endpoint incidents and ransomware tactics (RAT) capabilities in the posture scan for ransomware defense and respond quickly to threats, in multiple stages.

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

4. **Operating System Support**
   Make sure your EDR solution can support the overwhelming majority of running operating systems, including Windows and Mac, and that the learning cost should be the same for both services.

5. **Resources**
   Not all EDR solutions can have a considerable impact on a system resource, organizations should look for solutions that use less than 1% of CPU utilization.

6. **Automation**
   Evaluate the solution's ability to detect security operations center (SOC) or IT staff, so they can focus on other tasks. Also consider how it may integrate with other security applications and services.

7. **Managed Services**
   Reduce the burden by augmenting your staff with your EDR vendor’s incident incident response staff. Make sure these teams match your SOC’s and are sure your EDR vendor’s are not outsourced to 3rd party.

8. **Threat Hunting**
   Advanced threats may move laterally across the network through multiple devices and endpoints. Make sure your EDR solution balances threat hunting in an order that justifies and meets the threat hunting data for 90 days without paying for storage.

9. **XDR Readiness**
   Although you may not be ready to move to an XDR platform, you need to read with EDR solutions that can easily integrate with your SOC and other vendor solutions at the same time.

10. **Conclusion**
    Not all EDR vendors are the same. To find two right solutions, organizations need to set correct on evaluating the vendors and the solutions they are considering to make sure they are all acceptable and where they are and how they interact.

Visit Fortinet.com/EDR for more information