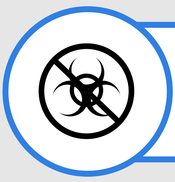
Considerations for Evaluating Endpoint Detection and Response (EDR) Solutions

Endpoint security solutions range from signature-based endpoint protection platform (EPP) or antivirus (AV) solutions to extended detection and response (XDR) 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 the product's ability to reduce the attack surface and to protect against the current and future threat landscape.

2 Ransomware Defense and Recovery

Organizations should determine the level of artificial intelligence (AI) and machine learning (ML) capabilities the solution uses for ransomware defense and evaluate rollback features on multiple types of systems.

3 Anti-tampering

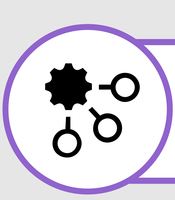
An EDR solution should act as a kernel-level firewall to protect the system against operating system attacks or the manipulation of files and applications.

4 Operating System Support

Make sure your EDR solution can support the overwhelming majority of operating systems (working internally and working from anywhere), and licensing costs should be the same for both servers and workstations.

5 Resources

Some EDR solutions can have a considerable impact on system resources; organizations should look for solutions that use less than 1% of CPU utilization.

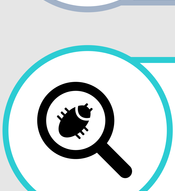


6 Automation

Automation relieves the burden on security operations center (SOC) or IT staff, so they can focus on other tasks. Also consider how it may integrate with other security appliances and services.

7 Managed Services

Reduce the burden by augmenting your staff with your EDR vendor's internal incident response staff. Make sure these teams match your global footprint and are make sure that MDR services are not outsourced to a 3rd party.

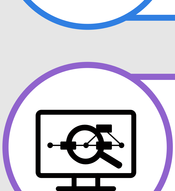


8 Threat Hunting

Advanced threats may move laterally across the network through multiple systems. Make sure your EDR solution facilitates threat hunting on more than just Windows and that the solution saves threat hunting data for 30 days without paying for storage.

9 XDR Readiness

Although you may not be ready to move to an XDR platform, you need to work with an EDR solution that is XDR ready and can integrate with your firewall and other same-vendor solutions before considering 3rd party API connections.



10 Conclusion

Not all EDR vendors are the same. To find the right solutions, organizations need to get answers to critical questions about the capabilities of EDR platforms to determine if they can protect all endpoints no matter where they are and how they connect.

Visit Fortinet.com/EDR for more information