MATT BACAK'S CHECKLIST

Checklist 12 - Establishing Endpoint Detection And Response (EDR)

Project Name: _____ **Date:** _____

	Yes	No

Advanced endpoint detection response security is a better alternative to antivirus in the sense that EDR has the ability handle ransomware attacks and block potential threats that manage to get past the implemented security controls. With EDR, while the software is installed on the end-user devices such as mobile phones and laptops, data is stored in a centralized database. The software is monitored regularly and upon detection of a potential attack, the user is provided with a prompt detailing the plausible actions to undertake in order to deter the attack from blossoming into a full blown breach. EDR provides your business with higher threat detection in the sense that the centralized database concept enables your security team to gather and aggregate endpoint data. This therefore affords the team the ability to anticipate and detect potential attacks. Here are factors to consider when evaluating an EDR solution.

1 What are your business' objectives/goals? ☐ ☐

2 Does the EDR solution offer industry-specific services? ☐ ☐

3 Does the EDR have a fast and accurate response to incidences? ☐ ☐

Notes

MATT BACAK'S CHECKLIST

Checklist 12 - Establishing Endpoint Detection And Response (EDR)

4	Does the EDR solution perform analysis, investigations, and searches in real time?	☐	☐
5	Is the EDR solution cloud-based?	☐	☐
6	Does it come with behavioral analysis?	☐	☐
7	Are email filtering and attachment scanning part of the EDR package?	☐	☐
8	Is the EDR affordable/within your budget?	☐	☐
9	Does it offer encrypted algorithms?	☐	☐
10	Is offline support and forensics integrated therein?	☐	☐

Notes

MATT BACAK'S CHECKLIST

Checklist 12 - Establishing Endpoint Detection And Response (EDR)

11	Is configuration management part of the EDR package?	☐	☐
12	Does the EDR cater to the needs of your business?	☐	☐
13	Is it characterized by automated remediation?	☐	☐
14	Does the EDR solution offer forensic capabilities for full visibility?	☐	☐
15	Does the EDR solution come with quick deployment and ease of management?	☐	☐
16	How are the solution's detection, remediation, and prevention capabilities?	☐	☐
17	How fast is the EDR solution's analysis capability?	☐	☐

Notes

MATT BACAK'S CHECKLIST

Checklist 12 - Establishing Endpoint Detection And Response (EDR)

18	Does it come with near-zero false positives?	☐	☐
19	Is the EDR solution part of a broader security platform?	☐	☐
20	Is it characterized by threat database?	☐	☐
21	Does it have an alerting power with details of the threat?	☐	☐
22	How scalable is the EDR solution?	☐	☐
23	Does it offer patch management in terms of patch priorities?	☐	☐
24	Are other management options offered?	☐	☐

Notes

MATT BACAK'S CHECKLIST

Checklist 12 - Establishing Endpoint Detection And Response (EDR)

25

Does the EDR support multiple devices? ☐ ☐

26

Does the EDR have HTTP/Malicious Traffic Detection (MTD) and HTTPS Malware Detection capabilities? ☐ ☐

27

Does it support peer-to-peer (P2P) applications? ☐ ☐

Notes:

EDR vendors in the market include the following:

- *Symantec Endpoint Protection.*
- *Cynet 360 Autonomous Breach Protection Platform.*
- *CrowdStrike Falcon Insight.*
- *RSA NetWitness Endpoint.*
- *Cybereason Endpoint Detection and Response.*

Notes