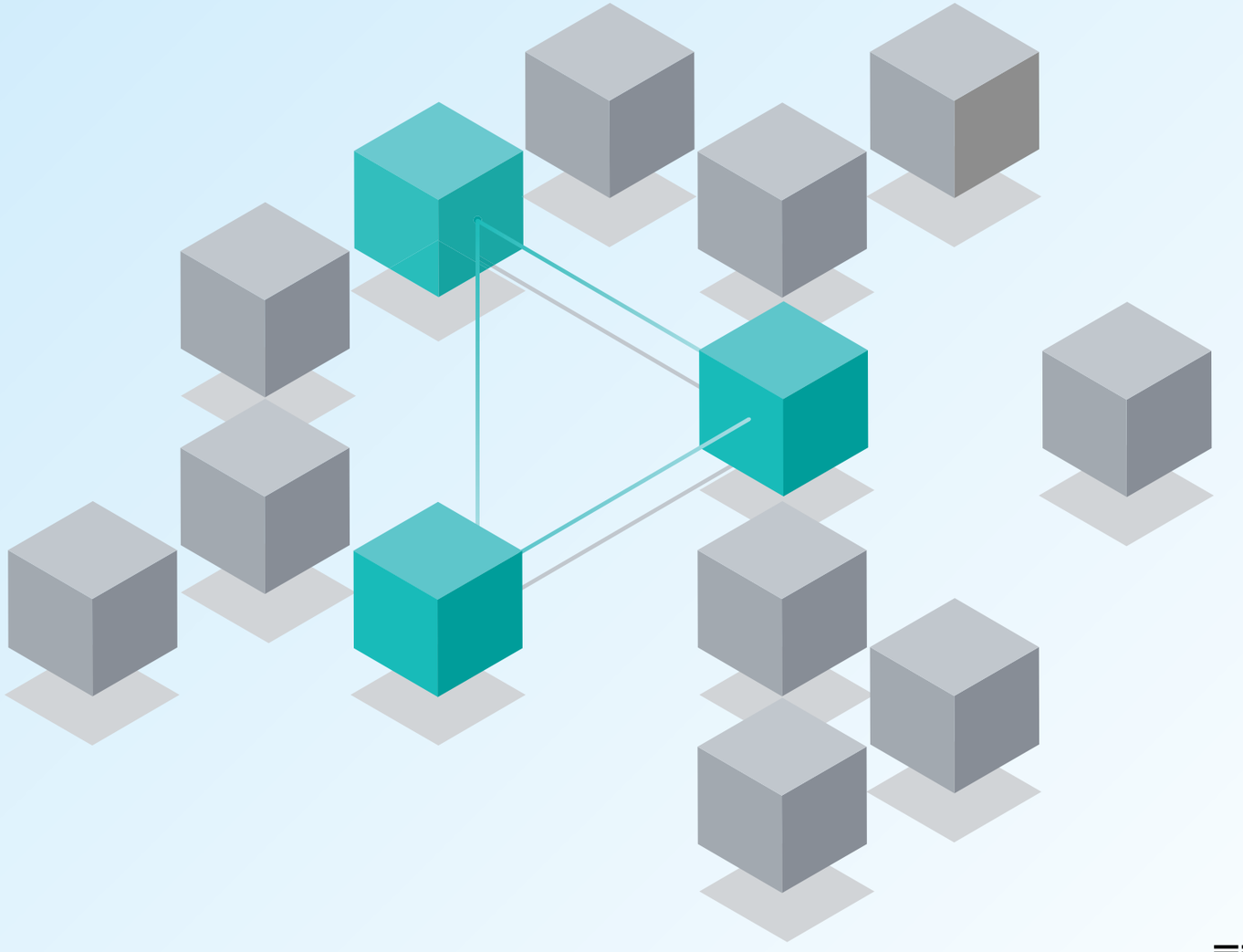
# EDR Buyer's Guide

How to pick the best endpoint detection and response solution for your business



REAQTA
an IBM Company

IBM

# Contents


01
Introduction

02
Complete visibility over your endpoint estate

03
Automation and ease of use

04
Alert management

05
Threat hunting


# 01
# Introduction

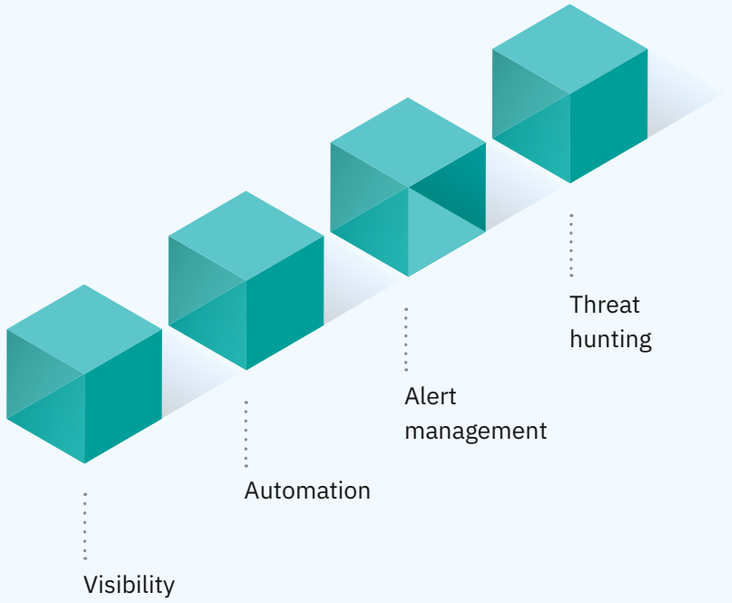
**What is EDR and why do I need it?**
We're witnessing an increased proliferation and interconnectivity of endpoints and data in recent years, coupled with the rise of malicious activities from threat actors. These factors have created a substantial threat to business continuity for organizations both large and small. More and more businesses are falling victim to attacks from cybercriminals and nation-state actors.

Traditional protection methods fight known threats but are vulnerable to sophisticated and unknown attack techniques and don't provide visibility into assets, which is one of the primary impediments to securing these systems. Expert endpoint protection skills are usually only available to the largest or most well-funded organizations. Combined with the fact that many attacks are now happening at machine speed with many moving parts, this has led to a situation where human teams, relying on traditional endpoint protection solutions, cannot keep up.

An endpoint detection and response (EDR) solution proactively and automatically blocks and isolates malware while equipping security teams with the right tools to confidently deal with these challenges. A modern EDR can ensure business continuity by effectively mitigating fast-growing, automated and advanced threats, such as ransomware or fileless attacks, without increasing analyst workloads or requiring highly skilled security specialists.

**Do you face any of these challenges?**
- Failure of existing solutions
- Limited visibility
- Lack of skilled headcount
- Alert fatigue
- Dormant threats

A modern and effective EDR comprises four key elements that we'll review in the next chapters:



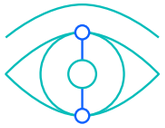
# 02
# Complete visibility over your endpoint estate

One of the primary impediments to securing endpoints is lack of visibility. As such, a modern EDR solution should provide complete and deep visibility into the applications and processes that are running.

When a threat appears, real-time alerting of its behavior with a graphical storyline needs to be automatically created as the attack unfolds, which includes MITRE ATT&CK mapping to give analysts full visibility and understanding of what's happening.

Most, if not all endpoint security software solutions, work within the operating system, which creates a boundary for the endpoint agent. This limits the capabilities and visibility of the agent while consuming more computer resources. Having an agent that works at the hypervisor layer and is designed to be undetectable not only minimizes resource use but also provides exceptional visibility to monitor all process behaviors while staying invisible to attackers.

**What to look for:**
- Full endpoint visibility
- Real-time alerting
- Storyline creation
- Frictionless agent
- Unified workflow



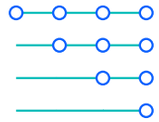
## Questions to ask:

→ Does your solution provide complete and deep visibility into applications and processes that are running?

→ As an attack unfolds, how does your solution provide meaningful, real-time information to better understand the threat?

→ Besides detecting a breach and alerting you, does your MSSP deliver end-to-end response and remediation?

# 03
# Automation and ease of use



With sophisticated threats and attack surfaces expected to grow in 2022 and beyond, many organizations are hard pressed to stay ahead of cybercriminals. A modern EDR should alleviate a growing workload through smart automation while being easy to use to limit the need for highly skilled security specialists.

The key for buyers to get value out of an EDR quickly is to automate and simplify. With Al automation, the bulk of the work is left to algorithms while minimizing human interaction. Through such Al algorithms, the software becomes easier to use and teams can be up and running quickly, without lengthy enablement.

As an attack is happening, response times are critical: the investigation time should stay well under one minute to eliminate advanced threats before they can cause harm to your infrastructure.

Buyers should look for an EDR that can run autonomously and offer automated detection and response capabilities. This provides analysts with a clear, real-time overview of an attack as it evolves, and can offer guided remediation to quickly return to normal.

**What to look for:**
- Autonomous detection
- Guided remediation
- Agent analytics
- Fast response times
- Ease of use

Questions to ask:

→ Are advanced skills required to operate the EDR?

→ To reduce analyst workloads, is the EDR capable of running autonomously?

→ With regard to response times, are threats analyzed in the cloud or at the agent?

→ If threats are analyzed in the cloud, what happens if there is no internet connection?

# 04
# Alert management

The key differentiator of an EDR compared to traditional antivirus (AV) solutions is that an AV relies on available signatures for detection and needs to know about a threat in order to block it. An EDR, on the other hand, uses a behavioral approach to identify malware and other potential threats by the way they behave on an endpoint. Also, unlike an AV, an EDR is lightweight by nature and does not require frequent updates.

The AI used in a modern EDR must therefore be capable of swift detection, with great accuracy and high fidelity to keep the volume of alerts—and analyst workloads—to a minimum. Buyers should inform themselves about the AI and machine learning techniques used. Compared to AI engines that rely on pretrained models and analysis for detection, an EDR that uses an initial learning model to identify the normal behavior of each endpoint enables greater accuracy in detections and alerts when there are deviations from the normal.

To reduce response time and alleviate alert fatigue for analysts, a modern EDR should be equipped with a robust, AI-driven alert management system capable of learning from the analyst and then autonomously applying analyst decision-making in day-to-day alert handling. Deploying a fully automated, AI-driven alert management system is key in battling alert fatigue, reducing employee churn and getting back in control.

**What to look for:**
- High-fidelity alerts
- Use of AI models
- Alert fatigue prevention
- Automated alert management

## Questions to ask:

→ Does your solution provide a way to automatically handle and close alerts?

→ How does your solution free up analyst time?

→ How does your solution reduce false positives?

→ If an employee leaves, how will the person's knowledge of our infrastructure be retained?

# 05
# Threat hunting

Threat hunting is an important part of a modern EDR solution and is necessary to maintain a clean, threat-free environment. Threat hunting can quickly determine if new threats have entered an environment and to identify weak spots. Data mining allows you to search for and eliminate dormant threats that may otherwise go unnoticed but could dwell in an environment for months or even years, waiting to be used by an attacker.

By nature, in-memory and fileless threats are hard to track and are even harder to follow when attackers are using different variants as they move within a large infrastructure. A modern EDR should automate the hunting job and use data mining to enable security teams to automatically hunt for threats that share similarities at the behavioral and functional levels with other incidents, delivering results in just seconds.

Flexibility in threat hunting is very important. Buyers should look for an EDR that not only offers a large library of prebuilt detection playbooks that can be deployed out of the box but also custom playbooks that can be easily created, without requiring scripting knowledge, for specific scenarios unique to an organization's security needs.

Threat hunting is often compared to finding a needle in a haystack. EDR searches must deliver comprehensive and granular results in real time by being able to drill down to specific hunting parameters and combining such parameters in an inclusive or exclusive manner. To further aid analysts and free up their time, results should be displayed in an easy-to-understand graphical user interface (GUI) so that analysts can easily and intuitively search for any event, from any endpoint, at any given time.

**What to look for:**
- Dormant threat searching
- Automated hunting
- Custom playbook creation
- No scripting required
- Data mining
- Real-time capabilities
- Graphical overview

## Questions to ask:

→ Can users build their own custom detection strategies and playbooks?

→ Can you automate threat hunting scenarios?

→ Do you provide a graphical overview of a threat hunt for fast triaging purposes?

→ Is scripting knowledge required to create playbooks?

## Next steps

Learn more about IBM Security ReaQta and request a demo.

**MBS Techservices Inc.**

**7783210005 | davem@mbstechservices.c...**

**https://mbstechservices.com/**

IBM Corporation
Route 100
Somers, NY 10589

Produced in the United States of America
April 2022