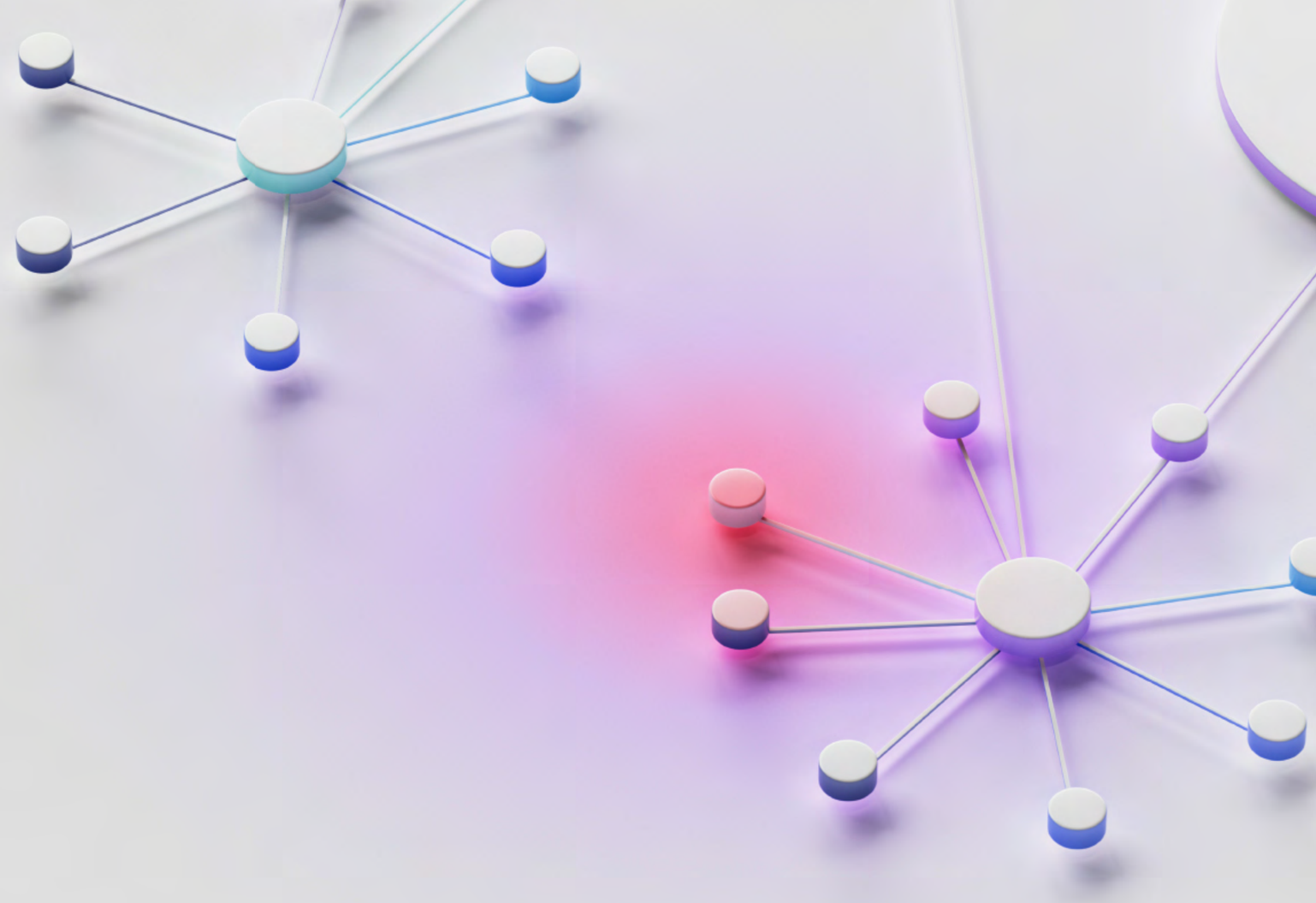
The Buyer's Guide to EDR

A detailed guide for choosing the best endpoint detection and response solution for your business



IBM **QRadar**

IBM

Contents

01 → Introduction

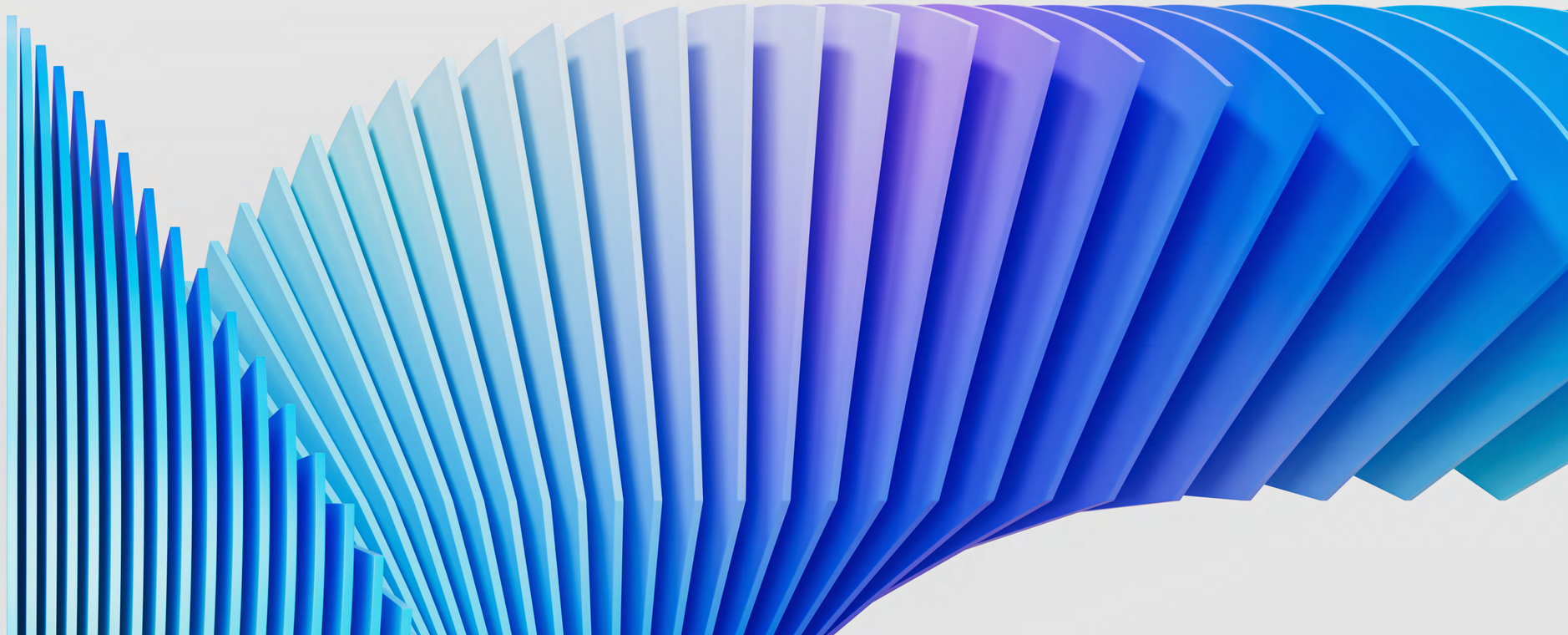
02 → Complete visibility across all endpoints

03 → Intelligent automation and ease of use

04 → Automated alert management

05 → Threat hunting

06 → Solution deployment options



01

Introduction

What's EDR and why do I need it?
The cost and frequency of data breaches continue to rise as the speed and sophistication of attackers advance to a new level. According to the Cost of a Data Breach Report 2023, only one-third of companies discovered a data breach through their own security teams, meaning 67% of breaches were reported externally by either a benign third party or by the attackers themselves. When attackers disclosed a breach, it cost organizations nearly USD 1 million more compared to internal detection, highlighting a need for faster threat detection. Factors such as an increased proliferation and interconnectivity of endpoints and data, coupled with the rise of malicious activities from threat actors, have created a substantial threat to business continuity for organizations.

Traditional protection methods fight known threats but are vulnerable to sophisticated and unknown attack techniques. They also 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. As many attacks are now happening at machine speed with multiple moving parts, security teams are relying on traditional endpoint protection solutions that can't 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

02

Complete visibility across all endpoints

A primary impediment to securing endpoints is lack of visibility. As such, a modern EDR 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. This storyline includes MITRE ATT&CK mapping to give analysts full visibility and understanding of what's happening.

Most endpoint security software solutions work within the operating system that creates a boundary for the endpoint agent. This setup 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 minimizes resource use and 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 managed security service provider (MSSP) deliver end-to-end response and remediation?

03

Intelligent automation and ease of use

With sophisticated threats and attack surfaces continuing to rise, 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.

The true value of an EDR is its ability to automate and simplify. With security AI and automation, the bulk of the work is left to algorithms while minimizing human interaction. Through such AI algorithms, the software becomes easier to use, and teams can be up and running quickly.

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

Look for an EDR that can run autonomously and offer automated detection and response capabilities. These features provide analysts with a clear, real-time overview of an attack as it evolves and can offer guided remediation.

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, can the EDR run 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's no internet connection?

04

Automated alert management

The key differentiator of an EDR compared to traditional antivirus (AV) solutions is that an AV relies on available signatures for detection. Additionally, an AV 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. Also, unlike an AV, an EDR is lightweight by nature and doesn't require frequent updates.

The Al used in a modern EDR must be capable of swift detection, with great accuracy and high fidelity to minimize the volume of alerts and analyst workloads. Compared to Al 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 is more accurate in detections and alerts.

To reduce response time and alleviate alert fatigue for analysts, a modern EDR should have a robust, Al-driven alert management system capable of learning from the analyst. Next, it should autonomously apply analyst decision-making in day-to-day alert handling. Deploying a fully automated, Al-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 you retain their knowledge of your infrastructure?

05

Threat hunting

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

In-memory and fileless threats are hard to track and even harder to follow when attackers are using variants moving within a large infrastructure. A modern EDR should automate the hunting job and use data mining to enable security teams to automatically identify threats that share similarities with other incidents at the behavioral and functional levels. This process delivers results in just seconds.

Flexibility in threat hunting is very important. Look for an EDR that offers a large library of prebuilt detection playbooks that are ready to use. Custom playbooks can also be easily created without requiring scripting knowledge for specific scenarios.

Threat hunting is often demanding and time-consuming. EDR searches must deliver comprehensive and granular results in real time. This practice allows EDRs to drill down to specific hunting parameters and combine them in an inclusive or exclusive manner. To further aid analysts and free up their time, EDRs should display results in an easy-to-understand graphical user interface (GUI). This feature enables analysts to 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 your solution automate threat hunting scenarios?

→ Does your solution provide a graphical overview of a threat hunt for fast triaging purposes?

→ Is scripting knowledge required to create playbooks?

06

Solution deployment options

You can deploy EDR in your organization, either on premises or in the cloud. But what if you don't have the expertise or time to manage it by yourself? Consider a managed detection and response (MDR) solution.

Organizations sometimes lack the required expertise and struggle with having to manage too many security tools and alerts. This situation means they can't adequately reduce mean time to resolution (MTTR) and improve productivity. Alert overload and time-consuming investigations also easily lead to fatigued analysts. But the reality demands 24x7 coverage, and MDR is an increasingly popular solution to address the need for continuous, real-time monitoring for organizations of all sizes.

MDR experts help identify and track sophisticated attackers and run advanced threat hunting campaigns. In particular, MDR services work as a cost-effective alternative for smaller or resource-strapped businesses that might not be able to build and sustain an in-house security operations center (SOC).

An effective MDR solution provider can speed threat response and act as an extension of your team by delivering operational transparency and collaboration. Additionally, it ensures threats are remediated as soon as they're detected, reducing potential damages and securing business continuity.

By using MDR, organizations can gain peace of mind and focus on their core business while leaving their cybersecurity needs to a team of expert defenders.

What to look for:

- 24x7 alert monitoring, investigation and response
- Rapid threat containment
- Proactive threat hunting
- Market leadership in managed security services

Questions to ask:

→ Do you have qualified staff to operate an EDR?

→ Is your security staff on call 24x7?

→ Do you face an overwhelming number of daily alerts that distract you from your core business?

→ Do you face budget or resource constraints in hiring and retaining a SOC team?

→ If you have the required tooling, do you need more support to fill gaps?

Next steps

Endpoints remain the most exposed and exploited part of any network. IBM Security® QRadar® EDR remediates known and unknown endpoint threats in near real time with easy-to-use intelligent automation that requires little-to-no human interaction.

Make quick and informed decisions with attack visualization storyboards and use automated alert management to focus on threats that matter. Advanced continuous learning AI capabilities and a user-friendly interface put security staff back in control and help safeguard business continuity.

If internal security staffing is limited, IBM Security QRadar MDR provides a 24x7 managed endpoint detection and response solution—powered by AI and delivered by IBM Managed Security Services.

Explore a leading EDR that offers all these capabilities in one solution.

Explore QRadar EDR →

IBM Corporation
New Orchard Road
Armonk, NY 10504

Produced in the United States of America
August 2023

This document is current as of the initial date of publication and may be changed by IBM at any time. Not all offerings are available in every country in which IBM operates.

THE INFORMATION IN THIS DOCUMENT IS PROVIDED “AS IS” WITHOUT ANY WARRANTY, EXPRESS OR IMPLIED, INCLUDING WITHOUT ANY WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND ANY WARRANTY OR CONDITION OF NON- INFRINGEMENT. IBM products are warranted according to the terms and conditions of the agreements under which they are provided.

Statement of Good Security Practices: IT system security involves protecting systems and information through prevention, detection and response to improper access from within and outside your enterprise. Improper access can result in information being altered, destroyed, misappropriated or misused or can result in damage to or misuse of your systems, including for use in attacks on others. No IT system or product should be considered completely secure and no single product, service or security measure can be completely effective in preventing improper use or access. IBM systems, products and services are designed to be part of a lawful, comprehensive security approach, which will necessarily involve additional operational procedures, and may require other systems, products or services to be most effective. IBM DOES NOT WARRANT THAT ANY SYSTEMS, PRODUCTS OR SERVICES ARE IMMUNE FROM, OR WILL MAKE YOUR ENTERPRISE IMMUNE FROM, THE MALICIOUS OR ILLEGAL CONDUCT OF ANY PARTY.