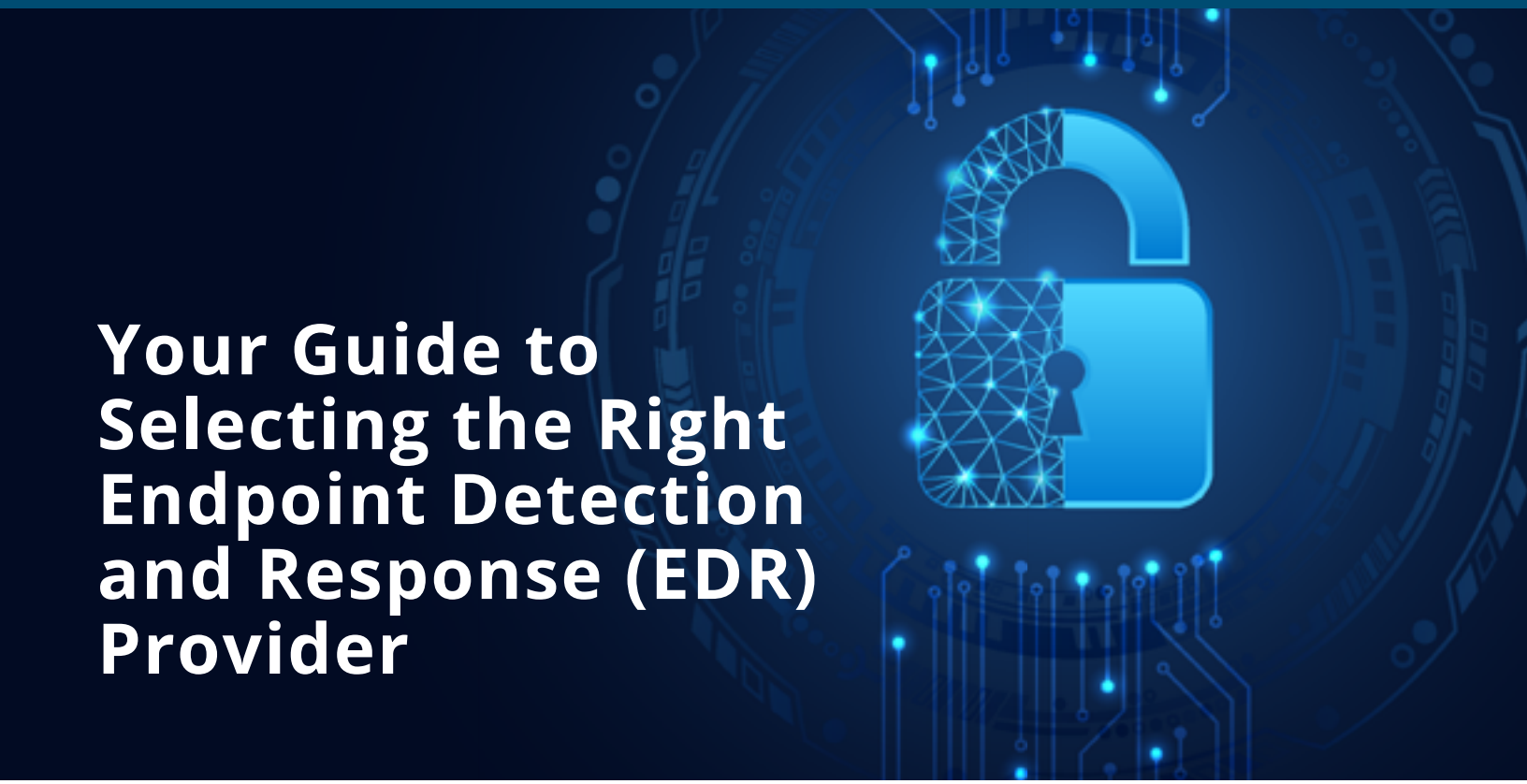
vCom



# Your Guide to Selecting the Right Endpoint Detection and Response (EDR) Provider

As a business leader, you know cybersecurity must take priority among the many moving parts of your organization—yet it is the most intimidating challenge. Each year the statistics get worse while the pressure heightens to establish a successful security strategy. Global ransomware damage costs are predicted to exceed $265 billion by 2031[1]. The use of malware increased by 358% through 2020[2]. The average attack costs $3.86 million[3]. The bad news goes on and on, and the COVID-19 pandemic only made things worse.

While cyber criminals get exponentially more sophisticated year over year, businesses have struggled to keep up. It still takes 280 days to find and contain the average cyber-attack3 —more than enough time for an organization to have suffered irreparable brand damage and costs. The writing is on the wall: cybersecurity cannot wait. But how do you begin to sift through all the security solutions on the market—not to mention all the vendors?

At vCom, we've seen many mid-size businesses like yours grapple with these questions, and we recommend starting with endpoint detection and response (EDR). EDR is an advanced security solution that helps businesses become proactive instead of reactive to cyber threats, and it's seeing massive adoption across all industries for that reason. Read on to get a thorough understanding of what EDR is, how it works, why you need it, and how to take the next step with an EDR provider.

# What is EDR?

Endpoint detection and response is a term suggested by Gartner's Anton Chuvakin[4] to describe security systems that use a high degree of automation to help teams quickly identify and respond to threats, as well as detect and investigate suspicious activities on endpoints. An endpoint is considered any computer system in a network, which can include individual employee workstations or servers as well as mobile devices.

EDR combines real-time continuous monitoring and collection of endpoint data with rules-based automated response and analysis capabilities, according to security giant McAfee. As a software solution, EDR is deployed on a business' network by installing agents on endpoints that your security team either manages through on-premise software or a cloud-based portal.

# Why EDR?

You might be thinking, "I have antivirus and firewalls, why do I need yet another security solution?" Yes, firewalls and antivirus solutions are imperative for your business to maintain as part of a cybersecurity strategy, but they are not enough alone. Cyber criminals find ways to by-pass firewalls every day, which is why any strong security strategy needs EDR.

EDR solutions can identify threats that are de-signed to bypass common antivirus software. EDR uses monitoring tools to collect data from endpoints across your organization that could indicate threats, analyzes the data, documents any patterns, automatically responds to iden-tified threats, notifies security teams, and pro-vides toolsto enable your team to better search potentially malicious activity.

It's no wonder more than 50% of enterprises will replace their legacy security software with EDR by the end of 2023[5].

# How Does a Business Use EDR?

There are several use cases for EDR in any organization:

1

## Improving investigative capabilities

Threat hunting can soak up valuable time and resources—and even turn up zero results—if your team doesn't know where to look or doesn't have the right tools to hunt properly. Staying ahead of the cyber threat game is a constant challenge, which is where EDR's alert capabilities help. You'll be able to speed up investigations through high-value alerts that improve detection and response times.

2

## Migrating to the cloud

No doubt your organization is in the process of digitally transforming by onboarding new cloud solutions and strategizing how to move existing solutions off-premise wherever possible. While a move to the cloud is one of the smartest decisions a business can make, it comes with natural security challenges that EDR addresses. EDR includes behavioral monitoring that observes device behaviors throughout your network and issues alerts if devices deviate from approved behaviors.

3

## Ensuring mobile security

If your business was one of many that plunged into remote work in 2020, you need a sophisticated solution to secure all the mobile devices on your network. Each one is an endpoint, and they—especially if they are personal devices—require different, more advanced monitoring compared to corporate devices. Even if you had legacy endpoint security in place prior to your move to remote work, personal devices don't adhere to those protections. EDR blankets your mobile endpoints with a layer of security that keeps them visible and monitored.

# How to Select the Right EDR Provider

Once you have a grasp on how EDR can elevate your security posture, you'll need to sift through the thousands of EDR providers out there to pick the right solution for your business. While that may seem like an insurmountable task, there are several clear steps to take and questions to ask that will lead you to the right EDR solution for your business.

## Ask the Right Questions During Your EDR Selection Process

Compile a list of questions that will help you winnow down your pool of potential EDR providers. We recommend starting with the following:

- Is the EDR solution easy to manage and deploy? Simplicity should be implicit.
- Is the solution, in terms of its ability to update itself, based on the latest threats to your industry? It should be sophisticated enough to update itself often.
- How much of an additional burden will this solution introduce to your company? It's important to gauge the load the EDR solution will introduce to your enterprise.
- How scalable is the solution for both your current infrastructure and your future infrastructure? As your business evolves to sustain a remote or hybrid-remote network, looking ahead to what your EDR will need to support is key.

# Keep Eyes and Ears Out for Best Practices and Red Flags

The right EDR provider for you should make sure to do two things:

- **Outline what solutions they cannot handle.** No EDR provider can do it all, and *anyone that pretends otherwise should be flagged*. An honest provider will look at your set of benchmarks and admit they can't handle a percentage of those requirements.

- **Conduct a penetration test.** Any worthy EDR provider will conduct either a black box test, white box test, or a grey box test to get an accurate picture of your vulnerabilities. This phase occurs before you've made your choice.

## Consider These Other Qualifiers

- **Keep in mind the needs of your unique vertical.** For example, if your organization is in healthcare, Health Insurance Portability and Accountability Act (HIPAA) compliance will be a factor. If you're in consumer retail, Payment Card Industry (PCI) compliance applies instead. These industry-specific needs will affect your EDR choice.

- **Look to providers who have had wide exposure to customers in your industry.** While startups are definitely worthy market players, they do not have the seasoned experience of EDR providers who have a roster of industry-specific customers. The more a provider can demonstrate a history of customer success, the more assured you are of their ability to expose vulnerabilities and survive cyber attacks.

## Leverage Third-Party Experts to Finalize Your EDR Selection

Rarely does a modern business have the time to successfully investigate, interrogate, analyze, and finalize their EDR provider alone. Your chief information security officer (CISO) already has enough on their plate, which is where expert guides like vCom come in. Our industry veterans and security experts help businesses like yours sift through the thousands of EDR vendors to not only select the best-fit for your organization but help you manage the solution as well.

**Our software platform enables you to manage all your IT spend so you can gain visibility into how to lower your costs, maximize your investments, and onboard new technologies where you need them most. For guidance in elevating your security posture through EDR, reach out to vCom today or schedule a demo. We're standing by to lend our expertise to your organization.**


**Sources:**

1. https://cybersecurityventures.com/global-ransomware-damage-costs-predicted-to-reach-250-billion-usd-by-2031/
2. https://www.helpnetsecurity.com/2021/02/17/malware-2020/
3. https://www.ibm.com/account/reg/us-en/signup?formid=urx-46542
4. https://www.mcafee.com/enterprise/en-us/security-awareness/endpoint/what-is-endpoint-detection-and-response.html
5. https://www.gartner.com/en/newsroom/press-releases/2020-09-15-gartner-survey-finds-the-evolving-threat-landscape-is-top-priority-for-security-and-risk-management-leaders