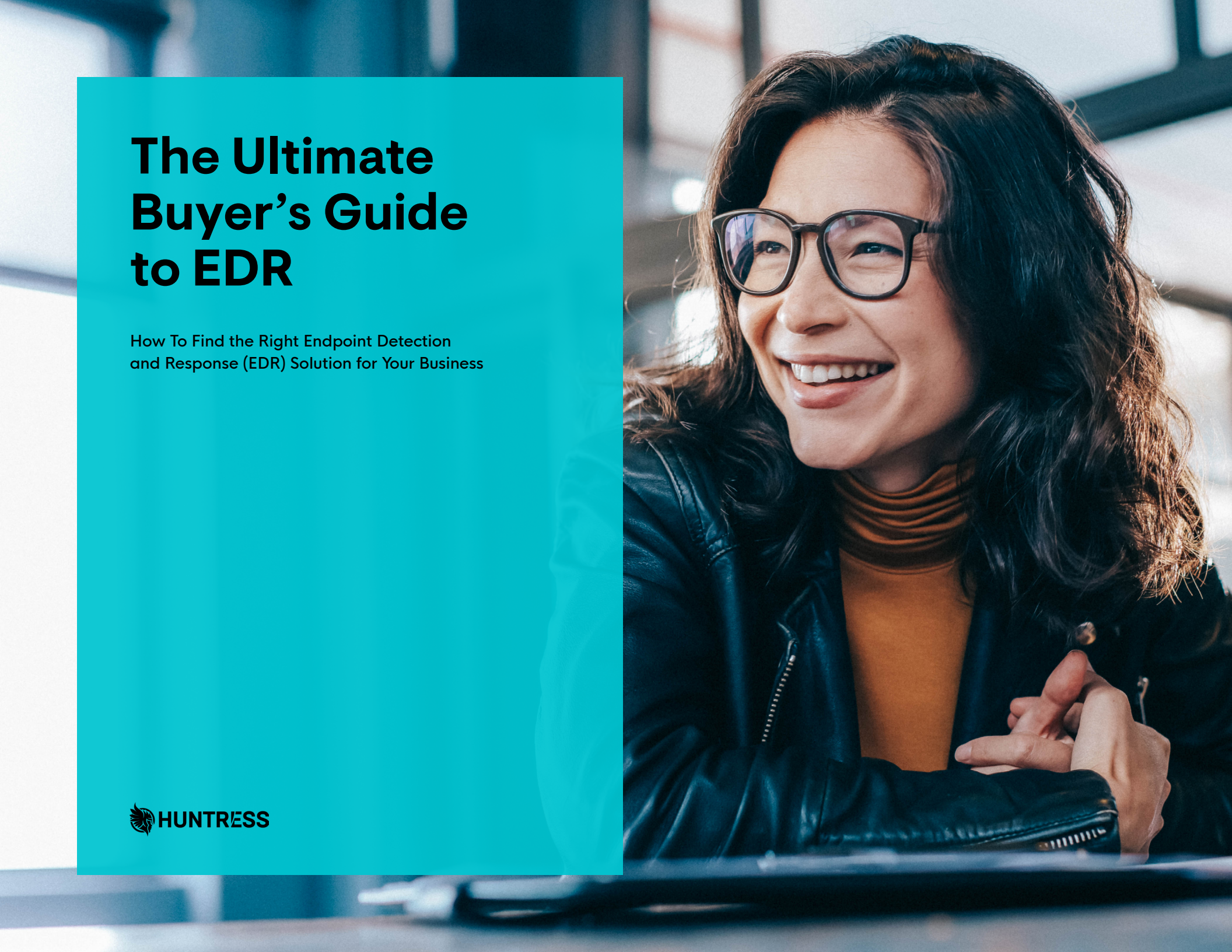
The Ultimate Buyer's Guide to EDR

How To Find the Right Endpoint Detection and Response (EDR) Solution for Your Business



HUNTRESS

Table of Contents

Cybersecurity has always been a game of cat and mouse.

In the past, businesses have turned to perimeter security—like antivirus and firewalls—as their defensive wall against cyber threats. And as new threats have emerged, those walls have become taller and taller to prevent threat actors from climbing over.

But keeping threat actors out is only half the battle.

Today, endpoints have become the new battleground. In order to stand a chance against modern attackers, businesses need the ability to reliably detect known and unknown threats, respond to them and extend the cybersecurity fight across all phases of an attack.

They need endpoint detection and response (EDR).

With the growing need to defend our devices from today's attackers, choosing the right EDR solution for the job can be a daunting task. There are so many options and features to choose from, and not all EDR solutions are made with small and mid-sized businesses in mind. So how do you pick the best solution for your business?

Don't worry—we got you. This guide will walk you through how to properly evaluate your EDR needs, plus what capabilities to consider or avoid when searching for your ideal solution.

Why EDR Is a Must

The modern workplace has changed. While the rise of remote and hybrid environments has brought many benefits, it's also drastically increased our attack surface. Employees have introduced more laptops, PCs, tablets and even mobile devices into their day-to-day—all endpoints that are spread out and vulnerable to malicious attacks.

That means it's more important than ever to have the right security layers in place.

Today, EDR is one of those critical layers.

Because of its ability to monitor for and alert you to malicious activity, EDR can be one of the most powerful tools in an organization's cybersecurity arsenal.

EDR is an endpoint security solution designed to detect even the most subtle cyber threats and allow teams to respond to them more quickly. It provides unparalleled visibility and detection capabilities across endpoints, which means it can often catch threats that perimeter security measures—like antivirus and firewalls—might miss.

Typically, EDR solutions should have the ability to track and analyze endpoint activity and enable analysts to respond when suspicious activity is detected. Along with this functionality, a modern and effective EDR solution can bring many advantages, including:

Increased visibility into endpoint activity—we're talking at a granular level that makes it extremely hard for hackers to hide. Through continuous monitoring and data collection, EDR solutions can provide a clear window into all activity on an endpoint.

Protection against known and unknown threats, like zero-day vulnerabilities or threats that can bypass signature-based detection. Rather than just scanning for known malware, EDR solutions can establish behavior patterns and detect when activity deviates from those patterns.

Deeper threat intelligence and analysis. EDR solutions consolidate and correlate a ton of endpoint data, providing in-depth context for all threat activity, attack chains and attack timelines—leading to clear, targeted response actions.

Faster incident response that can help minimize the potential impact of threats. EDR solutions build up a database of detections, enabling them to quickly pick up on suspicious activity, alert on it, and in most cases, provide remediation assistance to remove the threat.

Adherence to many of today's insurance and regulatory compliance requirements. EDR is more commonly a box that businesses have to check for cyber insurance, and it can lead to higher premiums if you don't have it.

How EDR Works

So how does EDR technology function, exactly? And where does it fit in a security stack? As coined by Anton Chuvakin, EDR is a solution that,

> **"Records and stores endpoint-system-level behaviors, uses various data analytics techniques to detect suspicious system behavior, provides contextual information, blocks malicious activity, and provides remediation suggestions to restore affected systems."**

Think of EDR as a stenographer of sorts; it's capturing the relevant events occurring on every endpoint it's installed on. Every login. Every running process. Every bootup and shutdown. All of that (and more) is monitored and logged to provide a full picture of what's happening at the endpoint level.

That granularity also helps create a baseline of expected endpoint activity. And from that baseline, security analysts or machine learning algorithms can help determine what is "normal" behavior for your organization and what appears to be "abnormal" behavior.

FOR EXAMPLE:

If an employee opens a phishing email claiming to be a salary increase for the entire company, downloads a document, and that document runs a program it shouldn't, EDR will step in to flag that behavior and automatically generate an alert to let your team know that something is amiss.

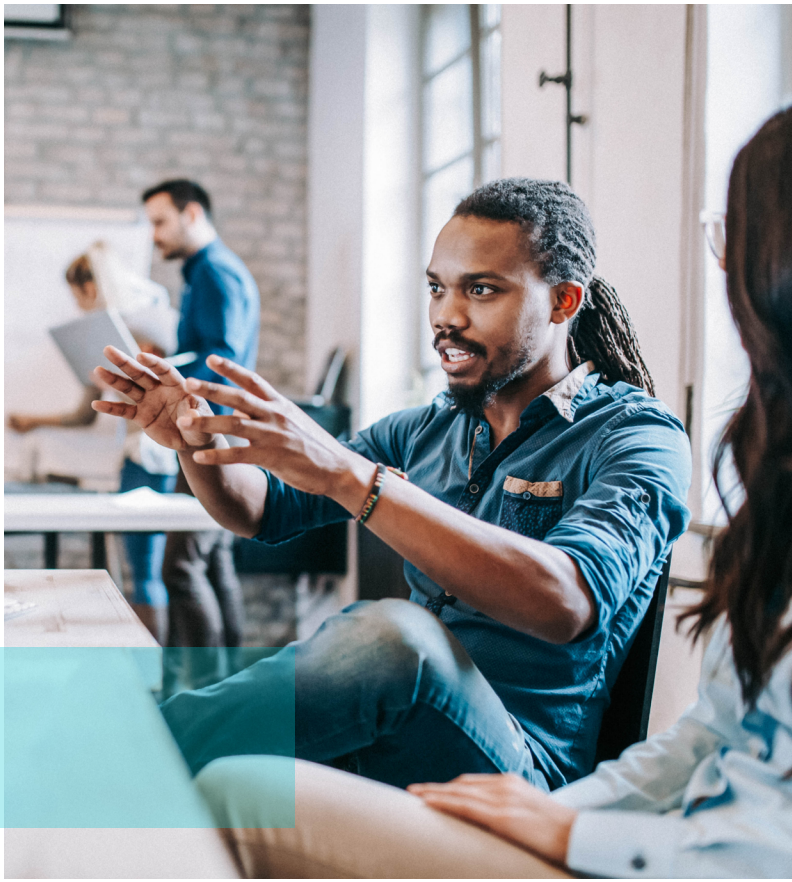
EDR solutions heavily rely on data collection, which gives analysts a lot of helpful context like who, what, where, when and how an attack may have occurred. And depending on configuration, some EDR solutions have the ability to isolate host machines when malicious activity is detected to prevent lateral movement throughout the network.

That's really what sets EDR apart from antivirus solutions and why it's a complementary layer in any security stack.

EDR technology can analyze billions of events in real-time—including comparing indicators of compromise (IOCs), scanning for known threats using traditional malware signatures, and using behavioral detections for threats that might be unknown. And of course, EDR solutions offer the critical ability of enabling threat response.

EDR excels at flagging potential threat actor activity and quickly alerting on it, but it's not a "set it and forget it" kind of tool.

EDR solutions require consistent tuning and close management by security analysts to investigate alerts and verify real threats from false positives.



How To Evaluate Your EDR Needs

The EDR evaluation process is extremely important—but with so many bells and whistles to compare, it can get a little overwhelming.

Whether it's your first time venturing into the realm of EDR or you're looking for a better-fitting solution, asking the right questions can point you in the right direction. Here's what you should consider as you go through your evaluation process.

1. **Determine your organization's needs.**

2. **Determine your technical needs.**

3. **Consider your internal resources.**

1 DETERMINE YOUR ORGANIZATION'S NEEDS

- What kind of threats are you most concerned about?
- Do you have a large number of endpoint devices to manage?
- Will EDR replace or complement your existing endpoint security investments?
- How much expertise or time are you willing to commit to operationalizing an EDR solution?
- What level of support do you need from your EDR solution or vendor?

2 DETERMINE YOUR TECHNICAL NEEDS

- How effective is the solution at detecting the threats you're most concerned about?
- Do you have a process or workflow to continuously review, tune and maintain detection rules?
- What operating systems does the solution support?
- What does the agent update process look like?
- Will the solution have any noticeable impact on your endpoint devices?
- What is the deployment and installation process? Does ongoing maintenance fit within your existing tech stack workflows?
- Are there known conflicts with other tools in your stack?
- Beyond detecting and alerting, does the solution provide the response and remediation capabilities you need?

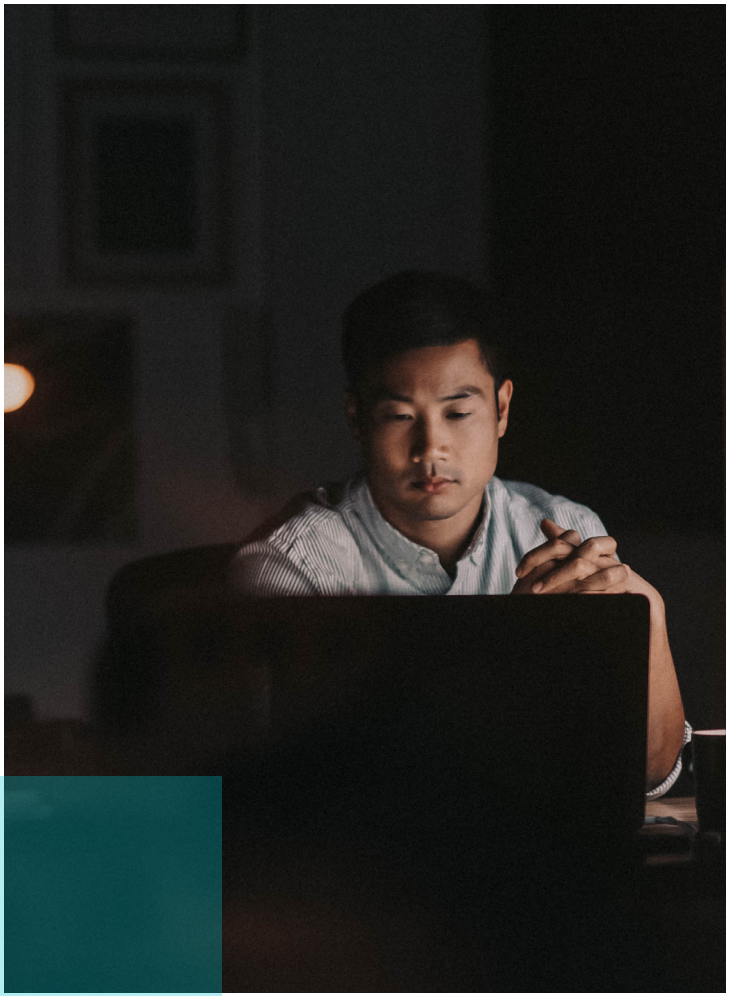
3 CONSIDER YOUR INTERNAL RESOURCES

- Do you need 24/7 coverage?
- Can your team support the level of time commitment that is needed to use and finetune the solution?
- Does your team have the required expertise to deal with threat investigations and incident response?
- Can your organization afford an EDR solution right now?

It's **important** to mention that implementing an EDR product alone does not give your organization EDR capabilities.

Well-trained security professionals are often required to manage EDR effectively and maximize your investment. Without the right team and time commitment, EDR solutions can amass data and alerts, leading to higher costs and overburdening analysts.

That means being brutally honest with yourself about your in-house resources. If your team doesn't have at least one full-time employee dedicated to triaging, investigating and responding to alerts, you might want to consider a managed EDR solution.



Managed EDR vs. Unmanaged EDR

EDR solutions can be either managed or unmanaged, and each option has its own pros and cons.

Unmanaged EDR solutions are typically purchased and implemented by the organization itself. This means that you are responsible for the setup, configuration and management of the solution.

Managed EDR solutions, on the other hand, provide all of the benefits of an EDR solution without the need to set up, configure or manage it in-house—that's typically handled by a third-party vendor. Additionally, managed EDR solutions often provide a team of experts who can help with day-to-day management, investigations and alerts.

UNMANAGED EDR SOLUTIONS

PROS

- ✓ Completely self-managed with EDR functionality at your fingertips
- ✓ Offers a high level of control and customization
- ✓ Provides deep visibility and data for security teams to act on

CONS

- ✗ Requires internal resources for setup, configuration and management
- ✗ Requires security expertise to parse through alerts and drill down to verify signs of a true threat
- ✗ Creates a lot of noise if not tuned or managed properly
- ✗ Can lead to alert fatigue and overload

MANAGED EDR SOLUTIONS

PROS

- ✓ Access to a team of security experts you don't need to build and staff
- ✓ Improved efficiency via experts who know what they're doing
- ✓ Alert fatigue and false positives are reduced as malicious activity is investigated and vetted for you
- ✓ No need to allocate internal resources for setup, configuration or management

CONS

- ✗ Less control and customization than unmanaged solutions
- ✗ Third-party has visibility into internal data and networks

Ultimately, the right choice for your organization will depend on your specific needs and resources.

If you have the internal resources to effectively maintain an EDR solution yourself, a self-managed solution could be the right choice for you. But if you can't support the added time, skill or headcount, a managed EDR solution could be the better option.

What to Avoid

Despite being a significant advancement from traditional security measures, EDR tools are not perfect. Many businesses—especially non-enterprise businesses—struggle to effectively use EDR solutions for several reasons.

COMPLEXITY

EDR solutions can be pretty complex and high-maintenance to manage on their own. They require a decent time commitment to configure and maintain it, the right level of staff to support it and deal with its alerts, and a high level of technical expertise to properly act on the data it produces. For non-enterprise businesses, they simply don't have these necessary resources in-house, which can lead to difficulty in configuring and maintaining the solution, as well as interpreting and acting on the data it provides.

TOO MANY ALERTS OR FALSE POSITIVES

EDR solutions can generate a high volume of alerts, which can be overwhelming for organizations to manage. This is particularly true for organizations that have not implemented proper security protocols and incident response plans. Without the proper processes and staffing in place, these alerts can be ignored or overlooked, reducing the effectiveness of the solution. If not continuously tuned and tightened, EDR solutions can also generate a high number of false positives, which can make it difficult for organizations to identify true threats. This can lead to wasted time and resources, as well as potential misdirection of incident response efforts.

DEATH BY BUNDLES

Bundles usually mean you are saving money. But unfortunately, bundles can be used to wall off key features and functionality. Some security vendors will price and package their services at different levels, sometimes grouping endpoint detection and response separately. This means that essential services like managed response, 24/7 coverage and remediation assistance are sold as additional services—leading you to pay more for the features you need. If you find yourself getting nickel and dimed, it's probably best to steer clear and instead go with a vendor that has key functionality and support baked into their price.

EXTRA BELLS AND WHISTLES

Another common pitfall when shopping for EDR solutions is the tendency to prioritize flashy features and capabilities over the needs of your business. Remember those evaluation questions a few pages ago? It's important to carefully assess and stay true to your needs. That way you're more likely to choose an EDR solution that meets those needs, rather than being swayed by features that may not be relevant or may cause more headaches than you bargained for.

What To Look For

Now that you know what *not* to do, what are the key EDR capabilities you *should* look for?

Here are some factors that your peers and other EDR users find important in their current solution:

"It has to have machine learning and state-of-the-art technology to prevent malware attacks."

"Easy to configure and manage."

"Frequent updates issued in order to keep up with new threats."

"Knowledgeable Sales Engineers and up-to-date documentation."

"Access to good support and a strong knowledge base."

When you're evaluating modern EDR solutions, there are a few must-have criteria to consider.

VISIBILITY

EDR solutions must be able to collect crucial information across endpoints and provide a clear picture of what's happening at any given point in time. This includes continuously monitoring relevant activity on endpoint devices, application-level events and processes that are running. A good EDR solution should also allow you to "wind back the clock" and provide visibility into the entire lifecycle of an attack, from initial compromise to exfiltration of data.

REAL-TIME DETECTION AND ALERTING

EDR that isn't detecting in real time is too late to the game. An EDR solution should be able to pick up on threat activity and present the right data at the right time, allowing security teams to quickly respond to threats and minimize their potential impact. This includes the ability to identify anomalies and suspicious activity, as well as detect known threats using signature-based detection. Plus, the best solutions are the ones you can trust. Look for an EDR that uses an element of AI, signature-based detection and human validation in its detection and alerting—that extra vetting usually means higher fidelity alerts and less time wasted chasing down false positives.

EASE OF USE

An ideal EDR solution should be easy to roll out and use, with a user-friendly interface and intuitive navigation. This also includes the ability to easily deploy to numerous endpoints in a scalable and cost-effective way.

When you're evaluating modern EDR solutions, there are a few must-have criteria to consider.

RESPONSE AND REMEDIATION

Threat detection is necessary, but it shouldn't stop there. Timely response and mitigation must be an integral part of any EDR solution. This means the solution should be able to accurately identify and classify threats—but equally important, it should provide actionable intelligence and offer an easy way to mitigate a threat once it is uncovered. In some cases, this includes the ability to kill processes, quarantine files, remove persistence mechanisms or isolate endpoints.

COMPATIBILITY AND INTEGRATION

EDR should be an additional layer to your security stack, so it's important to consider how it will function alongside the other tools in your environment. Integration into your existing setup shouldn't require hours of frustrating tuning and tweaking. Similarly, nearly all EDR solutions use an endpoint agent that is tightly tied to the endpoint's operating system, meaning it can have serious performance ramifications if not well-designed and tested. Look for a solution that plays nice with your other tools, can easily install or uninstall and will have minimal or no impact on endpoint users.

AUTOMATION AND ANALYTICS

A good EDR solution will allow your analysts to create their own custom searches and rules to help tune out the noise. If you have an EDR solution that isn't collecting valuable analytics or tuning detections, you are setting your analysts up for failure and most likely missing malicious activity.

When you're evaluating modern EDR solutions, there are a few must-have criteria to consider.

THREAT HUNTING

Rather than just reacting to alerts, the best EDR solutions should provide the ability to proactively hunt for threats beyond the solution's detection capabilities. That could mean the solution offers a large library of prebuilt detections, or it's backed by a dedicated team of experts who can track down potentially malicious activity on your behalf.

PRICE

An EDR solution should not break the bank. Some solutions are made for enterprise-sized wallets, so don't be afraid to shop around and select one that fits your budget. Just because something is expensive does not make it better, and conversely, something less expensive does not necessarily denote lower quality.

MANAGEMENT AND SUPPORT

It's important to consider what level of support and management you would need from your EDR vendor—it affects everything from upfront cost down to how well you're able to deploy, troubleshoot, optimize and maintain the solution. Because EDR solutions require a lot of time and attention, more businesses are opting for a fully managed solution. With managed EDR solutions, you get all the EDR functionality without the headaches and growing pains. Managed EDR solutions typically include access to a team of security experts, which can help reduce alert fatigue and false positives, and can offer enhanced visibility and threat hunting capabilities.

The Power of Managed EDR

To address the staffing, expertise and resource challenges that come with many of today's EDR solutions, businesses and IT teams are turning to managed EDR solutions instead of the traditional self-managed approach.

A managed EDR solution is typically provided as a service, with a vendor managing the EDR infrastructure and providing ongoing monitoring, analysis and response assistance.

One of the main benefits of a managed EDR solution is the ability to offload the burden of managing the solution to a team of security experts.

Hackers don't work 9 to 5, and neither should your security team.

Managed EDR solutions are often backed by a security team who can provide 24/7 coverage—not to mention they can help with day-to-day management, like triaging alerts, threat investigations and incident response. Plus, they have the technical know-how to investigate suspicious activity, offer mitigation guidance and deal with threats in real time—giving you direct access to their expertise without needing to find and retain that talent in-house.

Another major benefit of a managed EDR solution is the ability to reduce alert fatigue and false positives. A managed EDR solution typically includes advanced analytics capabilities or an element of verification from a team of analysts, which can help filter out false positives and prioritize the most critical alerts before it even crosses your desk. This can help security teams more effectively identify and respond to threats, rather than being overwhelmed by the irrelevant noise that can come with self-managed solutions.

Depending on your business' needs and current resources, managed EDR may be an option you'll want to consider.

Overall, a managed EDR solution can provide non-enterprise businesses with an effective and efficient way to detect and respond to threats, while also addressing common challenges and pitfalls associated with unmanaged EDR solutions.

About Huntress Managed EDR

At Huntress, we strongly believe that managed EDR should alleviate your biggest security obstacles, not create more for you. That's why we built Huntress Managed EDR with small businesses and IT teams in mind.

Huntress Managed EDR is a powerful and effective managed EDR solution backed by a 24/7 team of cyber experts. By combining extensive detection technology with real human experts, we help uncover, isolate and contain the threats that are targeting your business—all without the impossible cost, expertise and personnel burdens created by other platforms.

What makes us different? To put it simply: We're not made for the enterprise, we're made for you.

Huntress Managed EDR is built to support you where you need it most. That means we have you covered from red flag to remediation. Our powerful detection technology is backed by our experienced ThreatOps team who provide 24/7 follow-the-sun coverage to investigate and verify all suspicious activity in your environment. But we don't stop there. We make threat remediation actionable and easy by delivering easy-to-follow mitigation steps or one-click approval for automated actions—so you can act quickly and stop attacks in their tracks.

But don't just take our word for it! See why Huntress partners and customers love working with us and having Huntress Managed EDR in their stack.

I feel much more confident in our organization's security with Huntress on our side. Huntress has a clean, easy-to-use interface that only shows me the most essential information.

I trust Huntress's team to filter out the noise and only alert us when necessary. And when they do need to contact us, they already have an action plan in mind."

ALEXANDER S.
SECURITY ANALYST

"With Huntress ThreatOps, we have some of the best minds of cybersecurity at our disposal.

They help us validate incidents, handle them and also level up our own knowledge. With the context and information included in their personalized reports, any tier one technician can easily understand what threats have been detected and take the appropriate next steps—it's been a great force multiplier for us."

ANTHONY C.
CISO

Let's Talk.

Need help evaluating an EDR solution?
Want to learn more about managed EDR?

We're always happy to chat.
Send us a ping or email us at **hello@huntress.com.**

CONTACT US

Want to see Huntress Managed EDR in action?
Schedule a demo to ask questions, chat live with our team and see the value Huntress can bring to your organization.

BOOK A DEMO

HUNTRESS