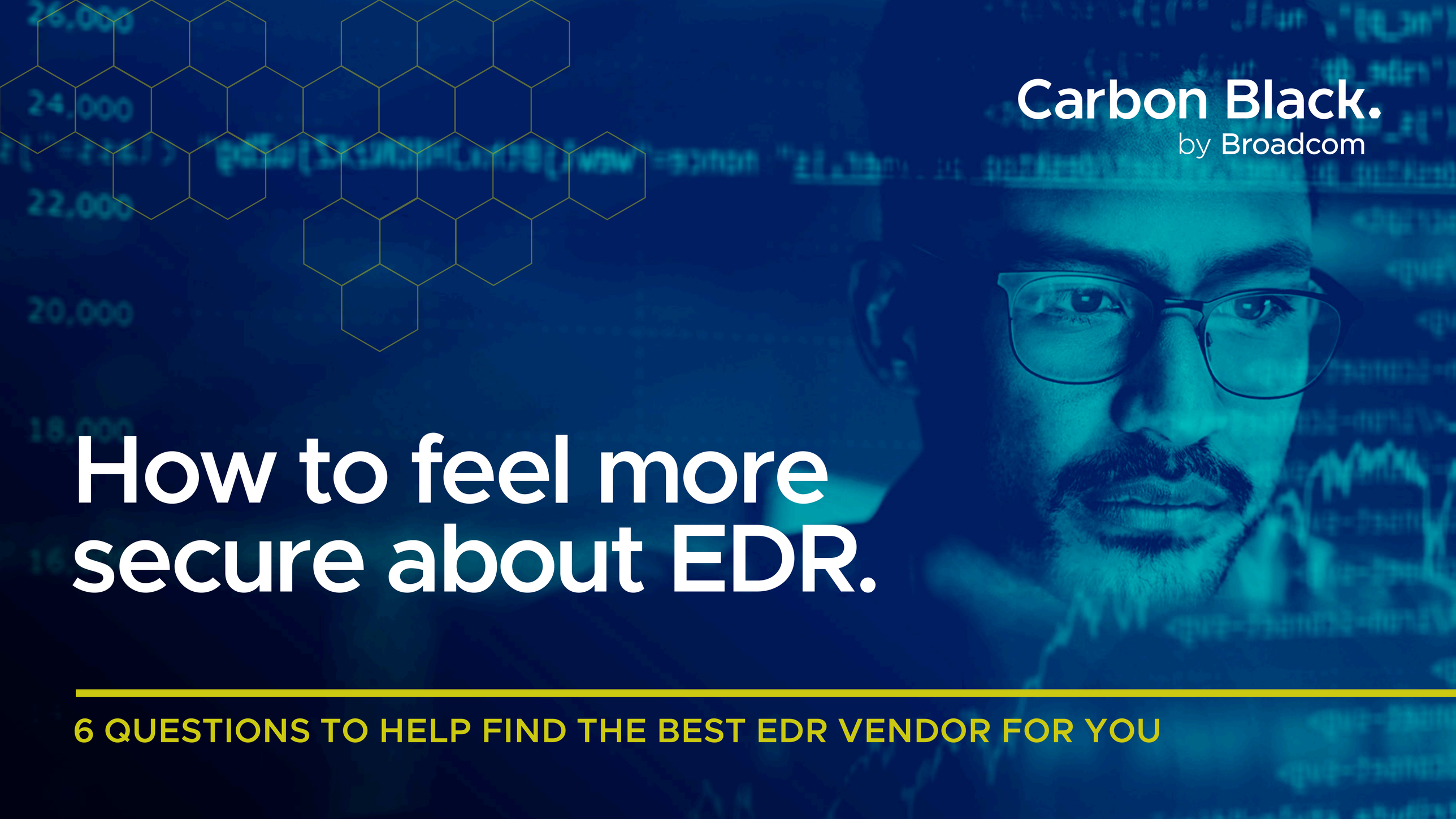
Carbon Black.
by Broadcom



How to feel more secure about EDR.

6 QUESTIONS TO HELP FIND THE BEST EDR VENDOR FOR YOU

More endpoints. More threats. Less control.

Your current cybersecurity challenges.

The cybersecurity landscape has never been more daunting. Complex, targeted attacks are growing in number and sophistication, with attackers now evading frontline antivirus (AV) and even next-gen antivirus (NGAV) defenses. As endpoints multiply in a remote-heavy workforce, ransomware and malware attacks are also on the rise.

Today's hyperconnected business landscape keeps suppliers, partners, and customers tightly integrated. Vulnerabilities that used to be easily contained can now create a ripple effect, extending out across networks and supply streams. Add the proliferation of IoT devices and other connected endpoints, and perimeters that were once clearly defined become increasingly blurred—and harder to secure. All reasons why it's critical to zero in on the exact right EDR partner.

63%

of organizations have experienced a supply chain attack in the last year.

Source: Gartner

Ransomware attacks have increased 48%

59% of IT and security professionals report an increase in the volume and severity of malware attacks. Source: Thales Group

Human error

and a lack of talent will lead to more than half of significant cyber incidents by 2025.

Source: Gartner

Resources are stretched thin

Security teams are feeling the squeeze due the ongoing talent shortage combined with a worsening skills gap. According to ISC2, the cybersecurity workforce shortage has reached almost 4M, with the gap growing 12.6% year over year. More than half (59%) of cybersecurity professionals said the skills gap can have greater impact than the worker shortage, with cloud computing security, AI/ML, and zero-trust implementation being the most common deficits.

Tightening regulations

In response to ongoing data breaches, federal agencies are increasing regulations to protect public entities and hold businesses accountable for security hygiene and incident response practices—from the forthcoming NIST Cybersecurity Framework 2.0 to new SEC requirements around incident disclosure for public companies. This puts more pressure on organizations to take a proactive security stance.

Time for a new strategy

All of these factors add up to a new era of cybersecurity marked by uncertainty and increasing volatility. The good news is, while threats keep evolving—so can your mitigation approach. Although AV and NGAV solutions are still vital for comprehensive security, they're no longer enough. Security teams must beef up defenses with more advanced solutions.

Securing your endless endpoint environment

Cyberattacks are increasingly complex and sophisticated, while security teams are stretched increasingly thin. Add to this endpoint proliferation and tightening regulations, and security teams need advanced threat detection solutions to stay ahead.

The solution:
Endpoint detection and response

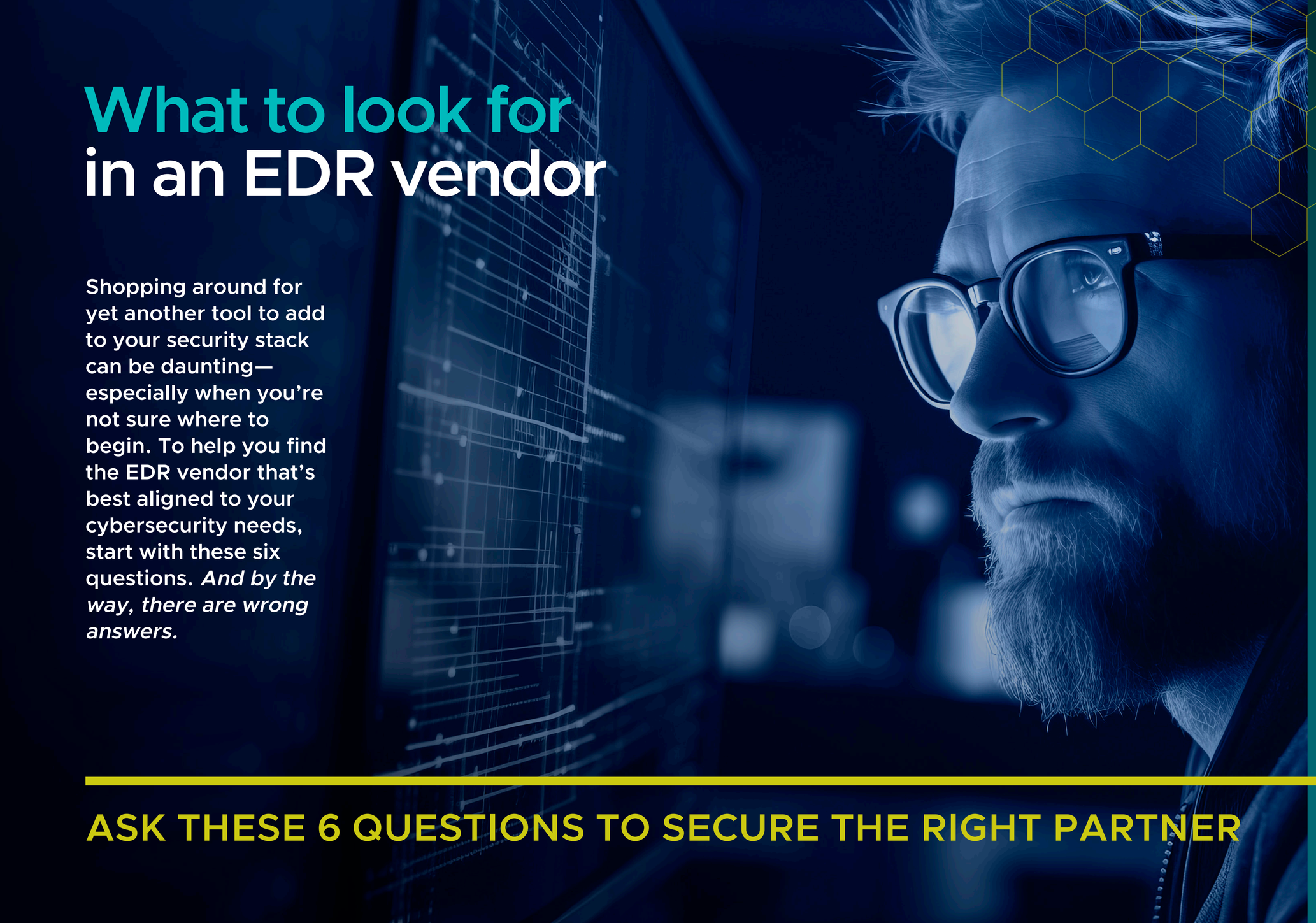
Security leaders are looking to endpoint detection and response (EDR) as a more robust, potent defense in the current climate. EDR is an integrated endpoint security solution that combines continuous, real-time monitoring and endpoint data collection with rules-based automated response and analysis capabilities. If you're struggling to secure your organization across multiple environments, overwhelmed by disconnected tools, controls, and alerts, or feel ill-equipped to prioritize, investigate, and remediate threats, EDR is your lifeline.

While NGAV protection offers a critical first line of defense against threats, sophisticated attackers may still break through—and roam your network undetected. EDR serves as a powerful second line of defense, allowing you to hunt threats proactively, investigate faster, and respond rapidly. Contain threats and minimize damage while gaining insight from each event to help prevent similar attacks in the future.

Securing your perimeter with a more robust defense

NGAV offers critical front line protection against cyber threats while EDR adds a powerful second line of defense, helping to improve your security posture with proactive threat hunting, rapid investigation and response, and minimized damage.

What to look for in an EDR vendor



Shopping around for yet another tool to add to your security stack can be daunting—especially when you're not sure where to begin. To help you find the EDR vendor that's best aligned to your cybersecurity needs, start with these six questions. *And by the way, there are wrong answers.*

It's not a question of moving beyond NGAV, it's how you get there

Just like EDR is proactive security, you want a proactive partner to guide you to the next level of your cybersecurity defense. Welcome to the beginning of the end of endpoint vulnerability.

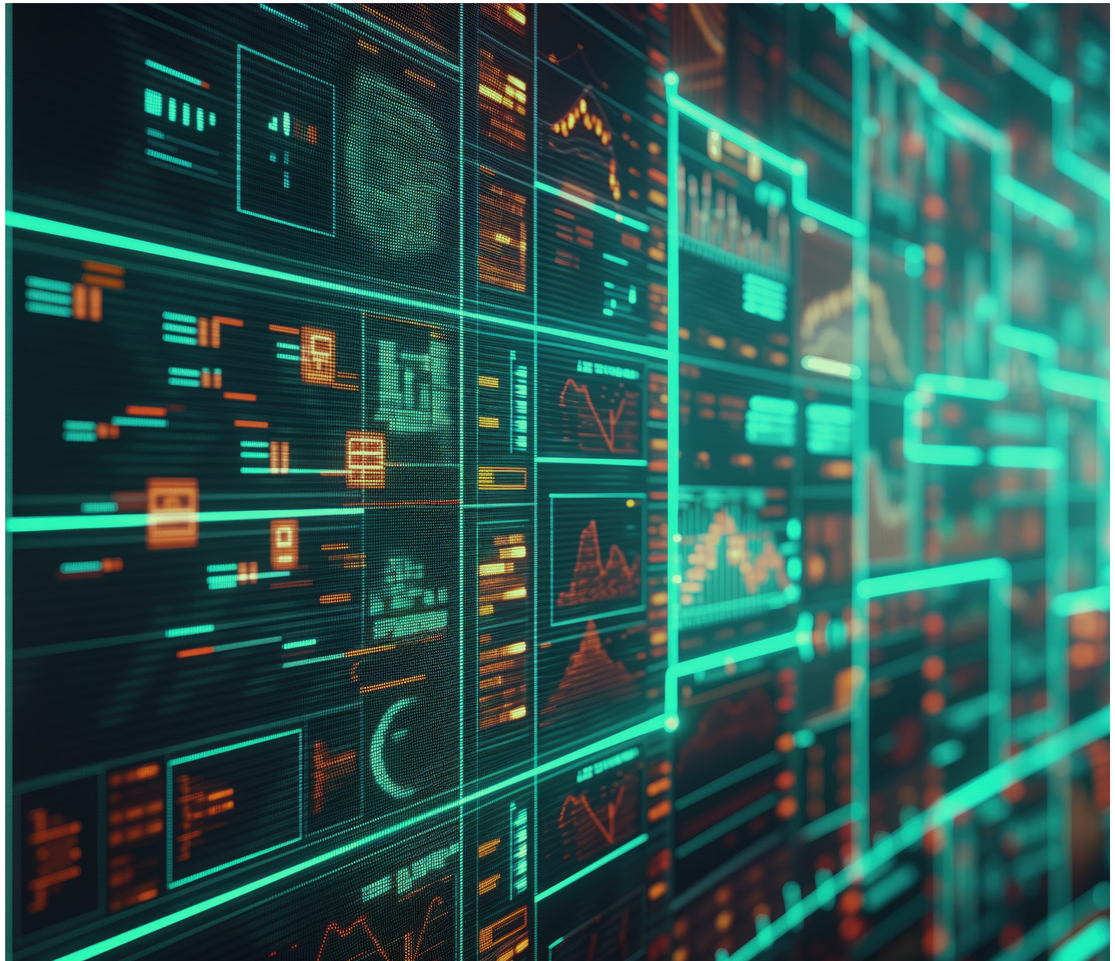
ASK THESE 6 QUESTIONS TO SECURE THE RIGHT PARTNER

1 What kind of intel does the solution provide?

The first thing you need to know is exactly what information you'll get from the EDR solution. Does it go beyond basic threat detection to offer deeper insight into what's happening in your environment? This should include unimpeded visibility that lets you account for each facet—including all endpoints across every environment.

Context is critical. Spotting potential threats is only the first step—you really need to understand what the threat means for your organization and environment, so you can come up with an appropriate plan of action. Be sure to vet vendors as to how much context they'll provide so you can take steps to mitigate threats and prevent attacks.

An optimal EDR solution will also offer in-depth analysis in the event that breach does occur. Understanding attacker behavior and what led to the incident will empower your team to respond and remediate in real time, stopping attacks in their tracks and enabling you to repair damage quickly, minimizing the impact.



Understanding your environment

Look for a solution that provides deep threat insight and full context to help you understand what it means for your environment and how you should respond. In-depth analysis of any breach incidents is also key to minimizing damage.

2 What type of endpoint and attack data does the solution capture?

It's important to choose an EDR solution that continuously collects and stores threat data in a centralized location where you can access it easily. Up-to-date intel allows you to take a proactive security stance, shutting down potential threats in your environment, minimizing damage, and preventing similar future attacks. If the data that's collected or your access to it is limited, your ability to hunt threats in real time will also be limited.

Look for a solution that provides a visual representation of all events associated with an alert. You should be able to drill down into individual processes or events and see actionable information such as reputation, command line used, and tactics, techniques, and procedures (TTPs), as well as where prevention was applied, source, and what the attacker may have been attempting. Contextualized data about network connections, file modification, and identity intelligence, such as Windows authentication events, should also be accessible.

After an attack occurs, the solution should provide the telemetry to find out what happened and enable you to close security gaps so it doesn't happen again. Learning from every new attack is critical to continually improving your security posture.

Alert visualization should include access to event information, including:

- Reputation
- Command line used
- Tactics, techniques, and procedures (TTPs)
- Source
- Where prevention was applied
- What the attacker may have been attempting
- Network connection data
- File modification data
- Identity intelligence

Accessing actionable endpoint and attack data

Continual data collection and easy accessibility are vital to your ability to hunt threats in real time. Choose a solution that lets you see all events associated with an alert, drill down deeper, and take appropriate action to prevent similar future attacks.

3 Are APIs available to integrate into your security stack?

Before you invest in any EDR solution, make sure it will work with your existing tech stack. While flexible out-of-the-box integration allows for speed and ease, APIs enable security teams to build out a security posture that fits more specific needs.

Working with a vendor that can deliver robust EDR within a single agent and console will empower your team and streamline processes, allowing you to thwart attacks and strengthen your security maturity. A universal console lets you consolidate endpoint agents and manage all of your prevention needs via a unified platform—keeping all your data and policy requirements in one place.

To make it easier for security teams to push data into connected solutions without having to use APIs, Carbon Black offers a unique data forwarder capability at no added cost.

Integrating with your existing tech stack

Before you invest, make sure the EDR solution offers flexible integration—either out of the box or via APIs for full customization. Working within a single agent and console enables you to keep all your data in one place, empowering your security team.

4 How does the EDR solution protect my containers?

Containers are often overlooked—but if a threat actor worms their way into your environment, they can use containers as a sort of virtual foxhole to hide in. If the container isn't included in your security strategy, it becomes a ticking time bomb.

Be sure to find out if EDR solutions allow you to integrate container alerts and events into existing endpoints and workloads. This will allow you to see more—and stop more, across all your environments.

Including container alerts and events

Don't give threat actors a place to hide—make sure your EDR solution lets you integrate container alerts and events into existing endpoints and workloads. See more and stop more threats across all environments.

5 How customizable is the EDR solution?

In today's dynamic and fast-moving digital environment, one-size-fits-all security tools won't cut it. You need a vendor that will help you get started quickly with suggested detections, and then allow you to customize things like watchlists and policies to fit your unique needs.

Why is this so important? Let's look at watchlists, as an example. Watchlists provide continuous monitoring of your environments for potential threats and suspicious activity. Custom watchlists enable set-and-forget searches, so you can quickly sift through high volumes of endpoint data and surface need-to-know activities to focus on. You can trigger alerts for things like an endpoint connecting to a specific IP/domain and trying to execute a banned hash or any launch of a suspicious process, as well as filtering out alerts for expected but unwanted processes.

With full visibility across your entire fleet of monitored endpoints, you should be able to customize your detection parameters for precise protection and comprehensive defense.

Customize watchlists to look at your environment from different angles

- Combine threat reports from multiple sources, proactively tracking the indicators of compromise (IOCs) that matter most to your organization
- Deepen your insight by evaluating past data associated with an alert—usually available for up to 30 days
- Use an API to manage watchlists through creation, updates, and removal
- Identify abnormal processes and generate hits and alerts for unexpected or unwanted activity
- Create new report watchlists and add/remove/disable/enable new or existing reports
- Configure or disable existing watchlists including generating hits and reports
- Configure, delete, or disable individual reports and their included IOCs

Tailoring the solution to your environment

Choose a vendor that allows you to customize the EDR solution to meet your precise needs. Customizing watchlists, for example, allows you to create set-and-forget searches with specific parameters, sifting through high volumes of endpoint activity data to surface need-to-know activities and IOCs.

6 What skill level is required to deploy and manage the EDR solution?

Adding a new security tool to your tech stack shouldn't require your team to learn a new skillset. The right EDR solution should be accessible to whoever needs to use it, not only the most tech savvy team members.

Depending on your current security posture, adopting EDR might be an easy step, or it could be a huge leap. Find out what kind of support is available from the vendor during implementation and beyond. Ongoing support will allow you to get maximum value from your investment while still focusing on what really matters—protecting your environment and optimizing your security posture.

Ease of use/Accessibility

Making the most of your EDR solution

Before you select a new security tool, make sure it's accessible to the team members who need it most. Find out what support vendors offer during deployment and what ongoing services are available to ensure you get maximum value from your investment.

Extend your security stack with Carbon Black

Security teams today are struggling with too many alerts requiring too much time to analyze and remediate incidents, and disconnected tools that slow them down. What you need is a single tool that lets you prioritize high-quality data by detecting and responding to threats in real time, stopping active attacks in their tracks and quickly repairing any damage.

Carbon Black Enterprise EDR delivers everything your security teams need to succeed—customizable defenses, continuous visibility, and advanced threat hunting. Prioritize data quality over quantity and empower your teams to defend your environment against sophisticated attacks.

By continuously collecting data and sending it to the Carbon Black Cloud, Enterprise EDR gives you immediate access to a broad, contextual view of any attack. Slash investigation times from days to minutes and get complete peace of mind knowing you have a comprehensive, proactive strategy to defend your environment against whatever comes next.

“Carbon Black significantly reduces the time spent on investigations down to an instant.”

—Shuichiro Shimizu, Security Engineer, COLOPL, Inc.

“I am very pleased at how minimally invasive yet intuitive Carbon Black is, and how quickly it can stop potential threats.”

—Christophe St. Luce, IT Director, City of Venice

Carbon Black enables you to:

- Investigate attacks with speed and precision
- Take control of endpoint data and reduce complexity
- Understand what’s happening in your environment
- Make data-backed decisions—quickly and confidently

See How EDR Solutions Stack Up

	Carbon Black	CrowdStrike	SentinelOne	Microsoft
Deployment Options	✓ **In-the-cloud or on-premises flexibility**	! Cloud only	✓ Comparable deployment	! No support for on-premise deployments of Defender console
Endpoint Performance Impact	✓ **Minimal impact on endpoints**	✓ Comparable impact on endpoints	! Testimonies of significant impact on assets, especially older infrastructure	✓ Comparable impact on endpoints
Customizability & Configuration	✓ **Granular control & customizability for power users**	! Toggle functionality only	! Toggle functionality only	! Complex configurability
Native Network Threat Detection	✓ **Native network telemetry & detection**	✗ Nothing native; relies on 3rd party for network detection	✗ Nothing native; relies on 3rd party for network detection	! Limited native network telemetry & detection
Threat Investigation	✓ **Ability to "Live Query" any device across 2000 attributes with more than 100 out-of-the-box queries**	! Queries limited to what Windows supports & often only functions if certain .net framework components are installed	! Limited live query abilities	✓ Comparable query capabilities
Managed Services	✓ **Light-touch managed services & network of expert partners**	! Heavy-handed services that remove control from security team	✓ Comparable managed services	✓ Comparable managed services
Pricing Flexibility & Transparency	✓ **Transparent & predictable pricing that simplifies budgeting**	! Complex pricing with potential unexpected costs at renewal	! High purchase price and add-ons required to reach parity	! Highly complex pricing structure
Total Economic Impact*	**427%**	**316%**	**353%**	**207%**

*The Total Economic Impact™ Of Carbon Black, a commissioned study conducted by Forrester Consulting on behalf of Carbon Black. Results are based on a composite organization.

Additional Offerings

	Carbon Black	CrowdStrike	SentinelOne	Microsoft
Upgrade to XDR	✓ **Activate in minutes (simple feature flag activation within Carbon Black EDR)**	! Module-based approach to achieving full XDR	! High cost associated with full XDR	! Jumbled mix of disparate tools and licenses needed to achieve XDR
Application Control	✓ **Dedicated Application Control with broad & deep capabilities**	✗ No native application control	! Limited version for cloud workloads only	! Notoriously complex dedicated solution with limited support

Comparison data accurate as of February 2024.

Quick Access Glossary

Term	Definition
EDR	An endpoint detection and response (EDR) is an integrated endpoint security solution that combines real-time continuous monitoring and collection of endpoint data with rules-based automated response and analysis capabilities.
Data Repository	A data storage entity in which data from multiple sources has been isolated for analytical or reporting purposes
Threat Intelligence	Evidence-based knowledge, including context, mechanisms, indicators, implications, and actionable advice, about an existing or emerging menace or hazard to assets that can be used to inform decisions regarding the sub
Native and Third-Party Telemetry Sources	Sources of data that automatically provide data that is stored in the data repository
Analytics / Correlation Engine	Software that programmatically aggregates, normalizes, and analyzes event log data, using predictive analytics and fuzzy logic to alert the systems administrator when there is a problem
Response Actions and Workflow Automation	Enables organizations to take inputs from a variety of sources and apply workflows or automation scripts aligned to processes and procedures
Incident Response	A set of information security policies and procedures to identify an attack, minimize its effects, contain damage, and remediate the cause to reduce the risk of future incidents


Take the next step in
your security evolution
See what Carbon Black Enterprise EDR
can do for your organization.
Learn More
Carbon Black.
by Broadcom