

[Cybersecurity 101: The Fundamentals of Cybersecurity](#) > [Endpoint Security: How Endpoint Protection Works](#) > **What Is Endpoint Detection and Response (EDR)?**

WHAT IS ENDPOINT DETECTION AND RESPONSE (EDR)?

FORRESTER WAVE FOR EDR REPORT

Anne Aarness - January 07, 2025

I What is EDR?

Endpoint Detection and Response (EDR), also referred to as endpoint detection and threat response (EDTR), is an endpoint security solution that continuously monitors end-user devices to detect and respond to cyber threats like ransomware and malware.

Coined by Gartner's Anton Chuvakin, EDR is defined as 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."

I How does EDR work?

EDR security solutions record the activities and events taking place on endpoints and all workloads, providing security teams with the visibility they need to uncover incidents that would otherwise remain invisible. An EDR solution needs to provide continuous and comprehensive visibility into what is happening on endpoints in real time.

An EDR tool should offer advanced threat detection, investigation and response capabilities — including incident data search and investigation alert triage, suspicious activity validation, threat hunting, and malicious activity detection and containment.



LEARN MORE

Download our buyer's guide on endpoint protection to learn the must-have features and capabilities for a modern endpoint protection strategy.

Download White Paper >

I Key EDR functions

I Key EDR functions

Automatically uncovers stealthy attackers

EDR technology pairs comprehensive visibility across all endpoints with IOAs and applies **behavioral analytics** that analyze billions of events in real time to automatically detect traces of suspicious behavior.

Understanding individual events as part of a broader sequence allows CrowdStrike's EDR tool to apply security logic derived from CrowdStrike Intelligence. If a sequence of events matches a known IOA, the EDR tool will identify the activity as malicious and automatically send a detection alert. Users can also write their own custom searches, going back up to 90 days, with Falcon Insight's cloud architecture returning query results in five seconds or less.

Integrates with threat intelligence

Integration with **CrowdStrike Adversary Intelligence** provides faster detection of the activities and tactics, techniques and procedures (TTPs) identified as malicious. This delivers contextualized information that includes attribution where relevant, providing details on the adversary and any other information known about the attack.

Managed threat hunting for proactive defense

Using EDR, the threat hunters work proactively to hunt, investigate and advise on threat activity in your environment. When they find a threat, they work alongside your team to triage, investigate and remediate the incident, before it has the chance to become a full-blown breach.

Provides real-time and historical visibility

EDR **acts like a DVR on the endpoint, recording relevant activity to catch incidents that evaded prevention**. Customers are given comprehensive visibility into everything that is happening on their endpoints from a security perspective as CrowdStrike tracks hundreds of different security-related events, such as process creation, drivers loading, registry modifications, disk access, memory access or network connections.

This gives security teams the useful information they need, including:

- local and external addresses to which the host is connected
- all the user accounts that have logged in, both directly and remotely
- a summary of changes to ASP keys, executables and administrative tool usage
- process executions
- both summary and detailed process-level network activity, including DNS requests, connections, and open ports
- archive file creation, including RAR and ZIPS
- removable media usage

This complete oversight of security-related endpoint activity allows security teams to “shoulder surf” an adversary’s activities in real time, observing which commands they are running and what techniques they are using, even as they try to breach or move around an environment.

Accelerates investigations

CrowdStrike endpoint detection and response is able to accelerate the speed of investigation and ultimately, remediation, because the information gathered from your endpoints is stored in the CrowdStrike cloud via the **Falcon platform**, with architecture based on a situational model.

CrowdStrike endpoint detection and response is able to accelerate the speed of investigation and ultimately, remediation, because the information gathered from your endpoints is stored in the CrowdStrike cloud via the **Falcon platform**, with architecture based on a situational model.

The model keeps track of all the relationships and contacts between each endpoint event using a massive, powerful graph database, which provides details and context rapidly and at scale, for both historical and real-time data. This enables security teams to quickly investigate incidents.

This speed and level of visibility, combined with integrated, contextualized intelligence provides the information needed to thoroughly understand the data. This enables security teams to effectively track even the most sophisticated attacks and promptly uncover incidents, as well as triage, validate and prioritize them, leading to faster and more precise remediation.

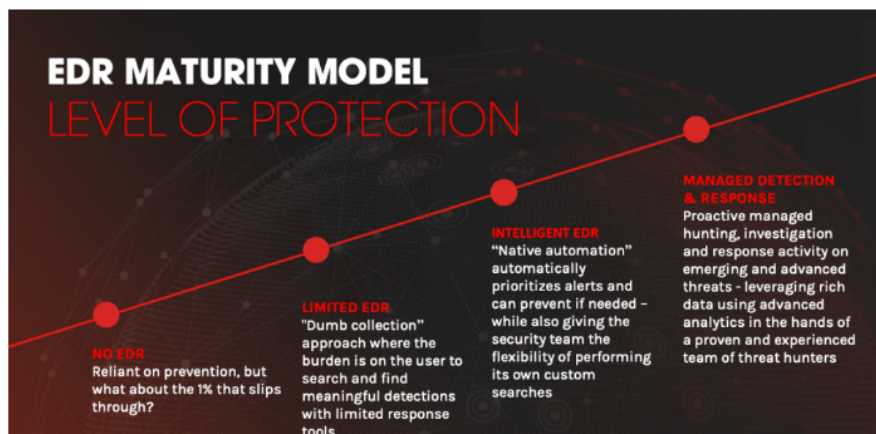
Enables fast and decisive remediation

CrowdStrike EDR can isolate the endpoint, which is called “network containment.” It allows organizations to take swift and instantaneous action by isolating potentially compromised hosts from all network activity.

When an endpoint is under containment, it can still send and receive information from the CrowdStrike cloud, but it will remain contained even if the connection to the cloud is severed and will persist with this state of containment during reboots.

CrowdStrike EDR includes Real Time Response, which provides the enhanced visibility that enables security teams to immediately understand the threats they are dealing with and remediate them directly, while creating zero impact on performance.

What should you Look for in an EDR solution?



Understanding the key aspects of EDR security and why they are important will help you better discern what to look for in a solution. It's important to **find EDR security solution that can provide the highest level of protection while requiring the least amount of effort and investment** — adding value to your security team without draining resources. Here are the six key aspects of EDR you should look for:

1. Endpoint visibility:

Real-time visibility across all your endpoints allows you to view adversary activities, even as they attempt to breach your environment, and stop them immediately.

2. Threat database:

Effective EDR requires massive amounts of telemetry collected from endpoints and enriched with context so it can be mined for signs of attack with a variety of analytic techniques.

Effective EDR requires massive amounts of telemetry collected from endpoints and enriched with context so it can be mined for signs of attack with a variety of analytic techniques.

3. Behavioral protection:

Relying solely on signature-based methods or indicators of compromise (IOCs) lead to the “silent failure” that allows data breaches to occur. Effective endpoint detection and response requires behavioral approaches that search for **indicators of attack (IOAs)**, so you are alerted of suspicious activities before a compromise can occur.

4. Insight and intelligence:

An endpoint detection and response solution that integrates **threat intelligence** can provide context, including details on the attributed adversary that is attacking you or other information about the attack.

5. Fast response:

EDR that enables a fast and accurate response to incidents can stop an attack before it becomes a breach and allow your organization to get back to business quickly.

6. Cloud-based solution:

Having a cloud-based endpoint detection and response solution is the only way to ensure zero impact on endpoints, while making sure capabilities such as search, analysis and investigation can be done accurately and in real time.

I Why is EDR important?

All organizations should know by now that with enough motivation, time and resources, adversaries will eventually devise a way to get through your defenses, no matter how advanced. The following are some compelling reasons EDR should be a part of your **endpoint security strategy**.

Reason #1: Prevention alone can't ensure 100 percent protection

When prevention fails, your organization can be left in the dark by its current **endpoint security solution**. Attackers take advantage of this situation to linger and navigate inside your network.

Reason #2: Adversaries can be inside your network for weeks and return at will

Because of silent failure, attackers are free to move around in your environment, often creating back doors that allow them to return at will. In most cases, the organization learns about the breach from a third party, such as law enforcement or its own customers or suppliers.

Reason #3: Organizations lack the visibility needed to effectively monitor endpoints

When a breach is finally discovered, the victim organization can spend months trying to remediate the incident because it lacks the visibility required to see and understand exactly what happened, how it happened and how to fix it — only to see the attacker return within a matter of days.

Reason #4: Access to actionable intelligence is needed to respond to an incident

Organizations may not only lack the visibility required to understand what is happening on its endpoints, it may not be able to record what is relevant to security, store it and then recall the information quickly enough when needed.

Reason #5: Having the data is only part of the solution

Organizations may not only lack the visibility required to understand what is happening on its endpoints, it may not be able to record what is relevant to security, store it and then recall the information quickly enough when needed.

Reason #5: Having the data is only part of the solution

Even when data is available, security teams need the resources required to analyze and take full advantage of it. This is why many security teams find that soon after they've deployed an event collection product, such as a SIEM, they are often facing a complex data problem. Challenges around knowing what to look for, speed, and scalability begin cropping up and other problems surface before their primary objectives can even be addressed.

Reason #6: Remediation can be protracted and costly

Without the capabilities listed above, organizations can spend weeks trying to discern what actions to take — often the only recourse is to reimage machines, which can disrupt business processes, degrade productivity and ultimately cause serious financial loss.

Want to see an EDR solution in action? Click the button below to watch an on-demand demo of the CrowdStrike endpoint protection platform.

WATCH NOW



ENDPOINT DETECTION AND RESPONSE (EDR) FAQs

Q: What is endpoint detection and response (EDR)?

A: EDR is an endpoint security solution that continuously monitors end-user devices to detect and respond to cyber threats like ransomware and malware.

Q: How does EDR work?

A: EDR security solutions record the activities and events taking place on endpoints and all workloads, providing security teams with the visibility they need to uncover incidents that would otherwise remain invisible.

Q: What should you look for in an EDR solution?

A: Six key aspects of EDR you should look for are endpoint visibility, threat database, behavioral protection, threat intelligence, fast response, and the solution being cloud-based.

Q: How is EDR different from antivirus?

A: One of the key differences is that antiviruses focus on known threats, while EDR solutions leverage intelligence features to uncover unknown threats.

Q: Why is EDR important?

A: EDR is important because it protects you from those adversaries that, with enough motivation, time and resources, will devise a way to get through your defenses, no matter how advanced.



Anne Aarness is a Senior Manager, Product Marketing at CrowdStrike based in Sunnyvale, California.



Anne Aarness is a Senior Manager, Product Marketing at CrowdStrike based in Sunnyvale, California.

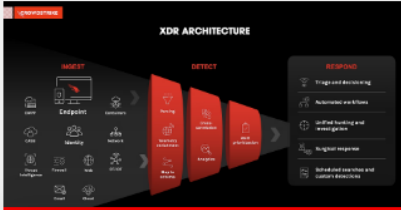
Featured Articles



EDR vs NGAV



EPP vs. EDR



Extended Detection and Response (XDR)

Try CrowdStrike free for 15 days

Start free trial →

Contact us →

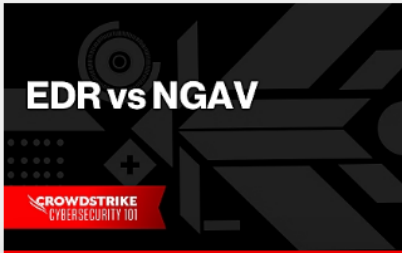
View pricing →



Get Started	Company	Partners	Existing Customers	Support
Pricing Sale	About Us	Partner Programs	Support Portal	Call 1-888-512-8906 (US)
Free Trial Guide	Executive Leadership	Service Providers	Developer Portal	Experienced a Breach?
Falcon Flex	Board of Directors	Strategic Technology		Contact Us
Financing	Newsroom	Channel & Distributors		Schedule a Meeting
CrowdStrike Marketplace	Investor Relations	Become a Partner		FAQs
Cyber Monday Deals	CrowdStrike Racing & F1			
	Sustainability			

Anne Aarness is a Senior Manager, Product Marketing at CrowdStrike based in Sunnyvale, California.

Featured Articles



EDR vs NGAV

CROWDSTRIKE
CYBERSECURITY 101

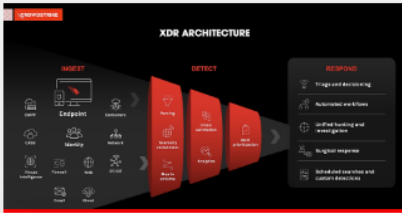
EDR vs NGAV



EPP vs EDR

CROWDSTRIKE
CYBERSECURITY 101

EPP vs. EDR



XDR ARCHITECTURE

DETECT

RESPOND

Extended Detection and Response (XDR)

Try CrowdStrike free for 15 days

Start free trial →

Contact us →

View pricing >

Get Started	Company	Partners	Existing Customers	Support
Pricing Sale	About Us	Partner Programs	Support Portal	Call 1-888-512-8906 (US)
Free Trial Guide	Executive Leadership	Service Providers	Developer Portal	Experienced a Breach?
Falcon Flex	Board of Directors	Strategic Technology		Contact Us
Financing	Newsroom	Channel & Distributors		Schedule a Meeting
CrowdStrike Marketplace	Investor Relations	Become a Partner		FAQs
Cyber Monday Deals	CrowdStrike Racing & F1			
	Sustainability			