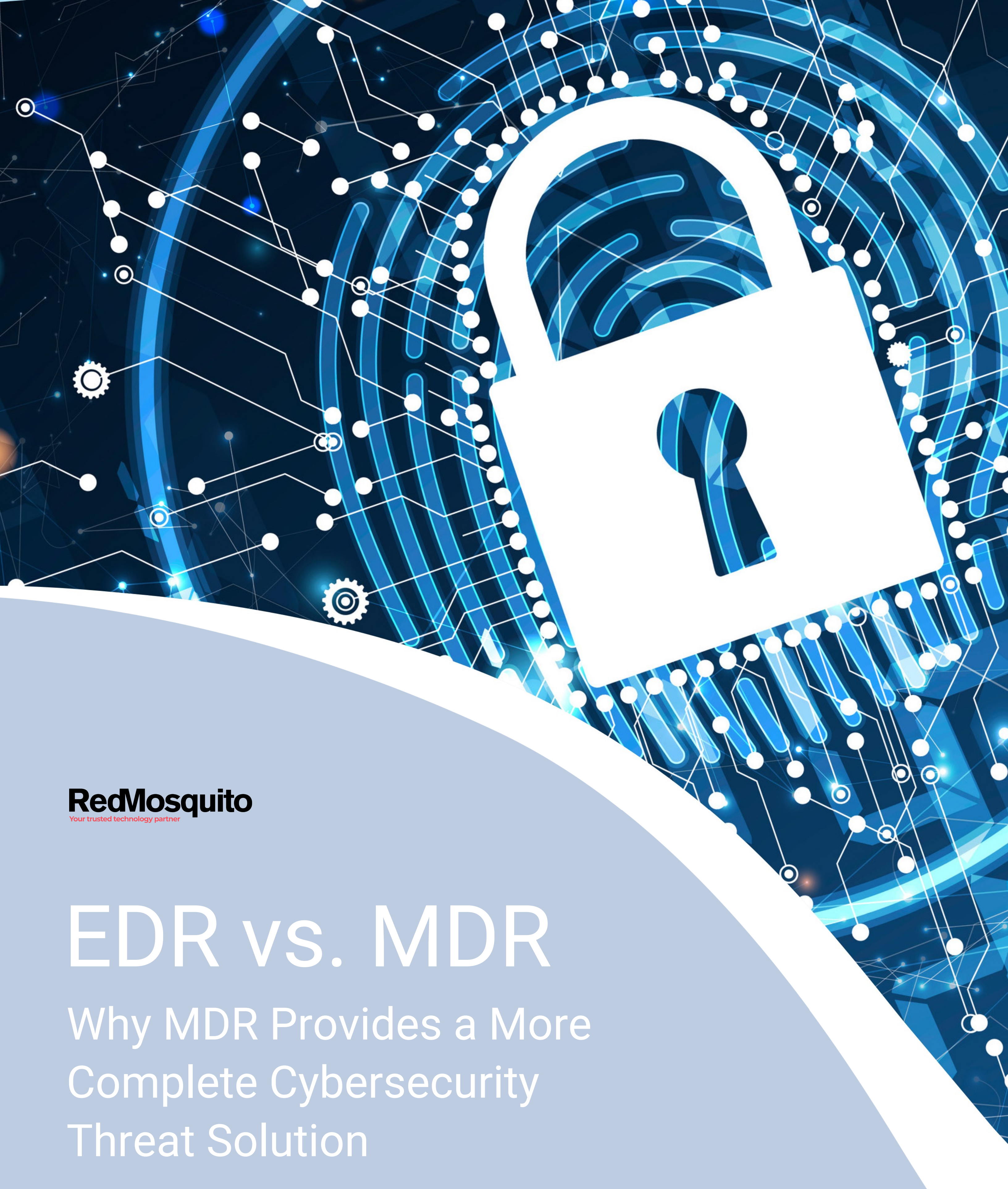


RedMosquito
Your trusted technology partner

EDR vs. MDR

Why MDR Provides a More Complete Cybersecurity Threat Solution

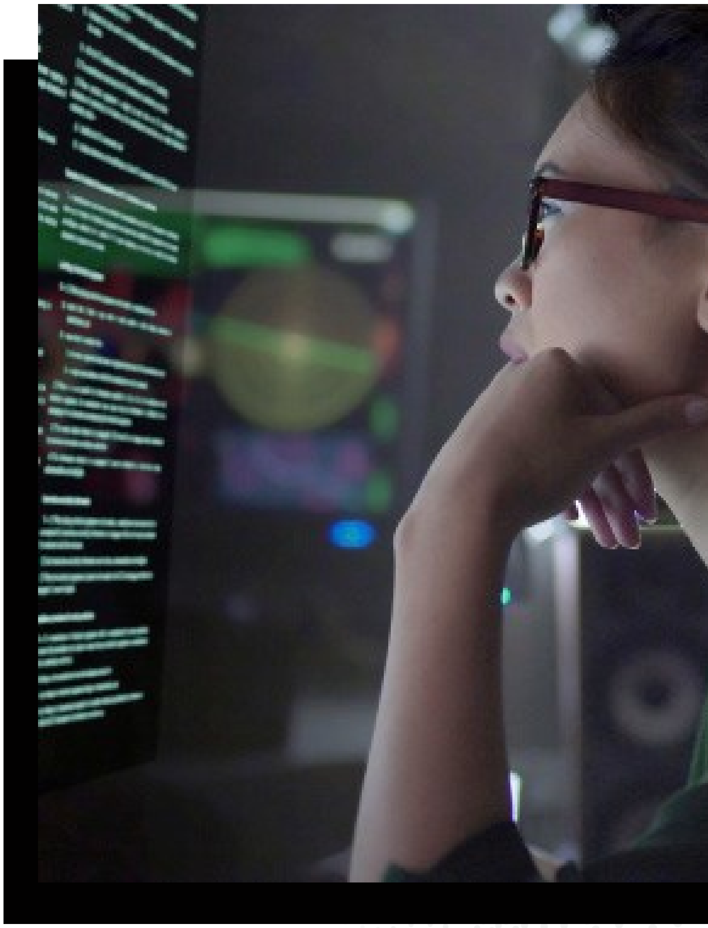
http://redmosquito.co.uk

Contents

Cybersecurity is rapidly becoming one of the biggest threats to businesses today. While massive data incidents at big-name companies continue to make headlines, the real story is the quieter, widespread epidemic of cyberattacks on small and medium-sized businesses (SMBs).

EDR and MDR are acronyms that get kicked around a lot in discussions about cybersecurity, but what do they mean? What do these technologies do? And more importantly, which one can effectively protect your business?

Get answers to these questions and more in this eBook. We'll start with a quick primer on EDR and MDR to help demystify these terms. We'll explore their uses, highlight their differences with a comparison, and show the clear winner.



Two growing trends that put SMBs at greater risk

Threats are more frequent and sophisticated, and the potential attack surface has expanded through cloud, mobile and multiple endpoints.

As enterprises work harder to implement the people, processes and technology to protect their businesses, cybercriminals turn their attention to the perceived soft target: SMBs.

What is EDR technology and how would you use it?

Endpoint detection and response (EDR) solutions are endpoint-focused security technology.

Endpoints are essentially gateways to a network. They include hardware devices such as desktops, smartphones, Internet of Things (IoT) devices, and servers—and they are all prone to vulnerabilities. Malicious actors target endpoints in hopes of infiltrating the network to which they connect.

EDR technology isn't new—although the term "endpoint detection and response" was only coined in the past decade. EDR technology can serve as a critical layer in an organization's security technology stack. But it's worth mentioning that EDR solutions don't have visibility into the entire network. EDR solutions focus purely on endpoints—monitoring, collecting, and analyzing endpoint activity data to determine what is normal and what isn't.

Modern EDR solutions are cloud-based and use artificial intelligence (AI) and machine learning (ML) for behavioral analysis and threat detection. They can continuously monitor running processes, map them to malicious behavior and identify root causes. Some leading EDR tools can also recognize virus and malware variants.

In the past 12 months, 32% of SMBs have suffered a cybersecurity attack, with an average cost of $104,296.

What are some use cases for EDR technology?

Organizations implement EDR solutions for security threat detection and assessment of endpoint devices accessing their network. With advanced EDR technology, security teams can:

- Benefit from vendor-driven analysis: An EDR platform can collect data from endpoints and transmit that data back to the vendor for analysis.
- Use rollback capabilities: In the event of a threat, a modern EDR tool can quickly roll back files to a previous safe version at an acceptable risk state.
- Query endpoint data quickly: Security teams can swiftly search information collected by the EDR platform to gauge the risk and scope of threats in real-time.
- Contain threats at the endpoint: EDR tools can contain a potential threat, block further events, and alert a security team.
- Monitor and control endpoint device use: Advanced EDR platforms allow organizations to control what applications devices can access while connected to the network.

What is MDR technology and how would you use it?

Managed detection and response (MDR) solutions leverage EDR technology and a security operations center (SOC). The EDR component provides rapid threat detection, and the SOC component provides people, skills, and technology necessary to remediate threats appropriately.

MDR technology is one of the fastest-growing security market segments, and it's easy to see why. MDR solutions use the power of EDR technology to find and respond to active threats, plus they include SOC's 24/7 monitoring services with cybersecurity experts who can investigate, contain, and eliminate threats.

More than half of respondents (51%) in a survey reported that their organization is already using MDR services, while 42% have either plans or interest in MDR services.

MDR provides comprehensive coverage:

- Complete visibility across endpoints, servers, network devices, DNS, and more
- Proactive cybersecurity experts
- Threat intelligence and analytics

Because MDR unifies cybersecurity tools and centralizes visibility and contextual information into a single repository, it drives faster and better outcomes than multiple, siloed tools. It provides the information security teams need to act and respond to potentially catastrophic events.

What are some use cases for MDR technology?

Organizations implement MDR solutions for comprehensive security threat detection, assessment, and human remediation across their entire IT infrastructure. With advanced MDR technology, security teams can:

Proactively protect data: A robust MDR platform protects critical and sensitive data such as financial, customer, and employee information, as well as applications and intellectual property.

Benefit from end-to-end visibility: MDR solutions offer fully integrated visibility across all cybersecurity services and tools.

Respond to threats faster: Enhanced automation and a 24/7 SOC manned by certified technicians add up to fast incident response and less potential damage to your business.

Lower risks: MDR solutions reduce risks of financial and reputational loss and noncompliance penalties for highly regulated industries like healthcare and finance.

Provide peace of mind: MDR solutions offer increased confidence in your ability to identify, block, and defend against the most sophisticated cybersecurity threats.

A quick comparison of capabilities: MDR vs EDR

MDR

- Focuses on the entire IT infrastructure
- Filters out false alerts dramatically reducing alert fatigue
- Enhances threat response through behavior-based analysis and threat intelligence feeds
- Features integrated views across tools for proactive security risk detection
- Integrates information security teams for quick response

EDR

- Focuses only on endpoints
- Detects endpoint events (e.g., file written, file executed)
- Responds to threats automatically or with cybersecurity team intervention
- Features built-in machine learning and behavioral analysis capabilities
- Allows cybersecurity experts to proactively threat hunt

2 u h v v 7 x 1 4 y 8 z A
8 CYBER ATTACK 2 t h 9 v 6
x 4 l z y m b 8 1 5 6 c d d

How MDR protects businesses more effectively

Cybersecurity experts know prevention isn't enough to stop all threats.

For example, EDR solutions are limited in their ability to detect and deflect highly sophisticated fileless malware. This malware is dangerous, as it exploits vulnerabilities that can give attackers administrative control and the ability to gather data to use in future attacks—like a highly targeted phishing attack.

The fileless malware threat is another reason more businesses are turning to MDR solutions. The additional SOC component provides the people, skills, and advanced technologies that add up to an invaluable layer of defense.

EDR solutions can detect, block, contain, and remediate threats targeting endpoints. They can also analyze and investigate threats, and, if needed, roll back files to "safe" versions. On the other hand, MDR solutions include the full range of EDR functionality plus full visibility into an organization's IT infrastructure and a SOC.

Companies that need to meet compliance and regulatory mandates can also benefit from the comprehensive reporting features built into MDR. Clients with highly valuable data, like sensitive financial information and intellectual property, are better protected, too, because MDR technology can flag unusual patterns and behaviors.

These additional layers of security—and 24/7 expert monitoring services—make MDR the clear winner.

Develop a complete security defense with MDR

MDR uses EDR solutions and a SOC to provide a more complete cybersecurity defense. An MDR solution is an important part of an organization's overall security strategy, which includes an array of other security controls (technological, physical and logical), adopting best practices and leading frameworks, implementing and enforcing effective policies, creating and testing business continuity management plans, providing relevant end-user training, and much more.

Even though an EDR solution can effectively detect and isolate threats on endpoint devices, a well-designed MDR platform will outperform an EDR tool in detection, prevention, and remediation across the entire IT infrastructure.

A case for MDR

So, what can happen when you don't have an MDR tool in place? Consider the following real-world example of a missed opportunity to contain a threat fast: An organization's web servers were hit with web shells—malware that enables remote access and control—leading to defacements.

The organization had an EDR platform. But because that tool can only detect when something happens on the endpoint, like the execution of a file, it only detected the threat and triggered an alert after the attacker tried to escape the website.
If the organization had a robust MDR platform in place, its SOC team could have detected the malicious traffic as soon as the initial exploit occurred and moved quickly to reduce its impact.

Take the next step

Partner with a managed services provider who can offer an MDR solution to protect your business. Contact us today!

Let's talk about your needs and how we can help!

RedMosquito
Your trusted technology partner

0141 348 7950

http://redmosquito.co.uk