

THE BIGGEST BENEFITS OF XDR

XDR solutions reflect the continued evolution of cybersecurity products. In fact, XDR is a culmination of cybersecurity product evolution, going far beyond the scope of endpoint detection and response (EDR) and managed detection and response (MDR) products.

XDR provides visibility into the entire attack surface, encompassing both cloud and on-premises environments. With XDR, businesses gain enhanced threat detection and protection, making precise, real-time determinations based on datapoints collected and consolidated across an array of threat entry points.

Here are four of the biggest benefits of XDR, and what they mean for your business.

1. Faster incident response

XDR helps businesses identify and respond to threats more quickly thanks to its advanced analytics capabilities.

What this means for your business:

- Prevents the spread of threats and minimises impact
- Lowers the chance of data loss
- Reduces the risk of reputational harm

But how much faster is XDR? Have a look at the table below to find out.

How long does it typically take for resolution

	Without XDR	With XDR
Typical BEC resolution (gateway only)	1-2 months	1-2 hours
Identity theft resolution	3-4 weeks	1-2 hours
Malware infection resolution	3-4 weeks	~ 1 hour
Insider threats resolution	3-6 months	~ 4 hours
Extortion resolution without XDR	Variable	< 24 hours

2. Improved visibility across your security environment

XDR brings together all your systems’ telemetry from servers, networks, cloud, email and endpoints into view through a single pane of glass, breaking down siloes.

What this means for your business:

- Offers complete oversight of the attack surface
- Helps spot vulnerabilities or misconfigurations more easily
- Simplifies compliance and reporting thanks to clearer audit trails

3. Smarter threat detection

XDR uses AI, advanced analytics and machine learning algorithms, which help it repel complex, multi-stage attacks that traditional tools often miss. It can stop both known attacks and unknown, zero-day threats. It also provides contextual insights instead of isolated alerts, providing details on attack types and techniques.

What this means for your business:

- Keeps you ahead of attackers’ complex tactics
- Reduces alert fatigue by automating detection
- Provides better understanding of attackers’ tactics, techniques and procedures (TTPs)

4. Lower security costs

Because XDR streamlines your toolsets and uses automation, it makes your security operations more efficient and less expensive.

What this means for your business:

- Reduced duplication of payments towards security tools
- Budget is freed up to invest elsewhere
- ROI on security investment is maximised

These are by no means the only benefits of XDR. To find out more about XDR’s benefits and how it works, download our eBook XDR explained: A strategic approach to threat management.

