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.

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.

XDR provides visibility into the entire attack

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



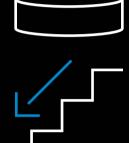
Faster incident response

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

Prevents the spread of threats and minimises impact

What this means for your business:





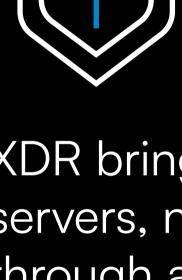
Reduces the risk of reputational harm

Lowers the chance of data loss

below to find out. How long does it typically take for resolution

But how much faster is XDR? Have a look at the table

	Willioul ADR	WIIII ADR
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
Extortion resolution without XDR	Variable	< 24 hours

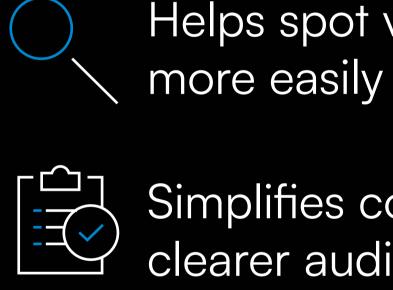


XDR brings together all your systems' telemetry from servers, networks, cloud, email and endpoints into view through a single pane of glass, breaking down siloes.

Improved visibility across your

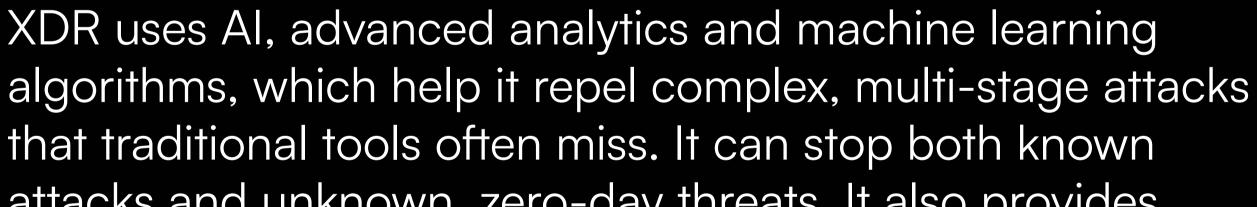
security environment

What this means for your business: Offers complete oversight of the attack surface



Simplifies compliance and reporting thanks to clearer audit trails

Helps spot vulnerabilities or misconfigurations



attacks and unknown, zero-day threats. It also provides contextual insights instead of isolated alerts, providing details on attack types and techniques.

3.
Smarter threat detection

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)



Lower security costs

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

Reduced duplication of payments towards



security tools

What this means for your business:



ROI on security investment is maximised

Budget is freed up to invest elsewhere



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.