Why EDR?

Endpoint Detection and Response (EDR) combines artificial intelligence, next-gen antivirus, and other technologies into a single, integrated cybersecurity solution. EDR detects, contains, and mitigates both known and unknown threats originating from any endpoint connected to your network.

The Big Picture:	The Weeds:			
Older tools leave you vulnerable	Hacker methods and goals have changed — it's not just about money anymore	You have multitudes of endpoints, any of which can be the easiest attack surface for hackers	Older tools lack visibility, which impedes threat detection	Today's hackers use legitimate applications for their malicious activity instead of malware and viruses
Advanced tech stops advanced attacks	EDR's next-gen antivirus quickly contains and mitigates known threats	AI proactively hunts for unknown threats to find and analyze Indicators of Compromise (IoC)	EDR flags IoC's for your team to review and take action if needed	EDR capabilities inform your team how attackers gained access which enables you to prevent future attacks
You can rewind chains of events to reverse attack damage	EDR logs all activities on every endpoint connected to your network and creates maps for forensics	Mapping capabilities enable you to go back in time and undo the chain of events triggered by a threat	EDR can reverse ransomware encryption — no need to pay a ransom	Rollback functions vary by EDR tool so you can choose the tool that best matches your needs
You can customize EDR to your specific needs	Your security team can write EDR rules for your specific industry, organization, and objectives	Fine-tuned configurations define algorithm functions, reduce noise, and improve detection accuracy	Custom detection rules define which activities trigger which automated responses and alerts	Improved accuracy enables your security team to focus on the activities that are most likely to pose a threat
Better for business and digital transformation	Running an EDR tool typically costs a fraction of the costs related to downtime and remediation following an attack	Stakeholders, clients, and partners are more confident you're protecting their interests	EDR helps pave the way for additional cloud adoption and digital transformations	Cyber insurance providers are requiring EDR because it reduces the number of claims and claim dollar amounts

Infrastructure first! To benefit from EDR or any advanced technology, you need the infrastructure to run it. The key is to build the strong foundation you need before you want to implement new technologies. By planning ahead, you'll be ready to leverage innovations that help you grow, prosper, and stay secure.