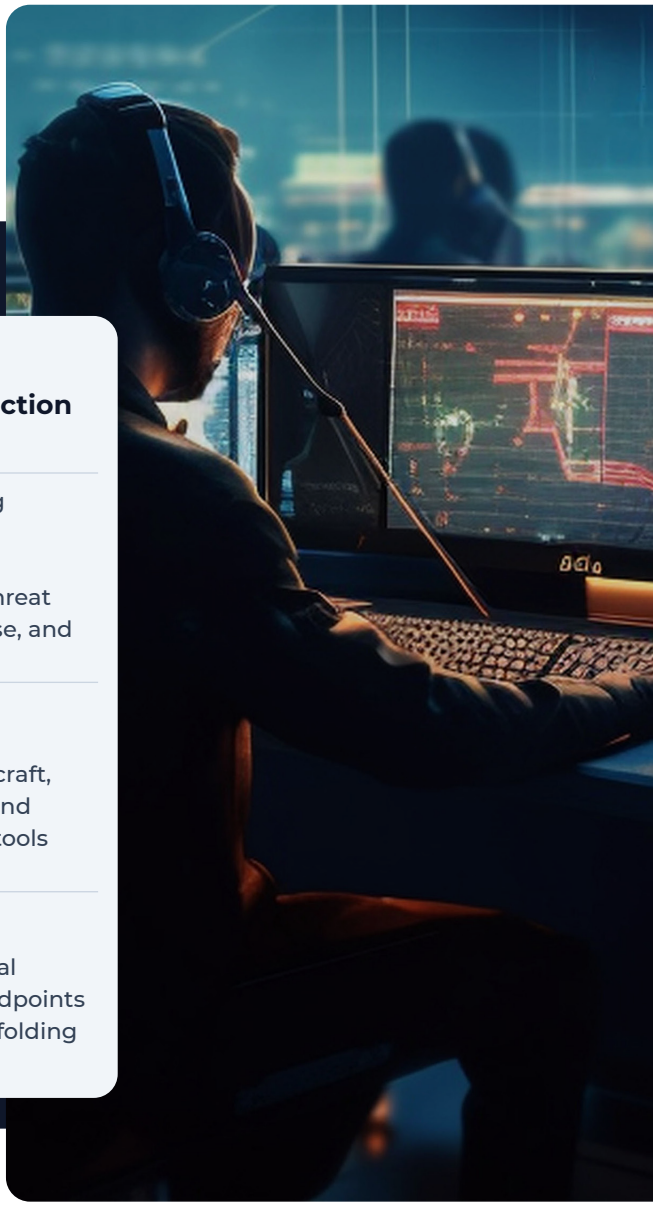
AccuTech™ International

Why do I need MDR on top of EDR?

The Value of Continuous Monitoring and Response to Cyberthreats

EDR is a critical part of our security service to you, but it's only one component of a layered security program. MDR uses human analysts to detect and respond to attacks that bypass EDR and other automated security tools.



At a Glance: EDR and MDR

	EDR (Endpoint Detection & Response)	Our MDR (Managed Detection & Response)
WHAT IT IS	Automated detection tool that can also assist with isolating and responding to threats	Service combining technology with human experts to offer full-service threat detection, response, and investigation
WHAT IT DETECTS	Known malware and bad behavior	Stealthy attacker behavior, or tradecraft, that evades EDR and other automated tools
SCOPE OF PROTECTION	Isolated endpoints (desktops, laptops, servers)	Live network map provides contextual visibility across endpoints to stop attacks unfolding in real time

The Attacker Evolution

Because EDR systems are good at stopping known malicious software and code, hackers have adapted. They've learned they can evade EDR by using techniques that help them blend in and look like an IT administrator working within a network. This means they use legitimate tools and processes already in the victim environment, at least until the final attack stages. In fact, a recent report found a 1400% increase in fileless attacks exploiting existing software, applications and protocols in 2023.*

**Source: Aqua Security*

The Value of MDR

RESPONDS EARLY

It's all about eliminating adversaries from the network early, before your critical assets are affected, or malware is deployed. We offer MDR with the fastest detection and response times in the industry: Once an attack is detected, it's contained in less than 20 minutes on average.

PROVIDES BACKUP

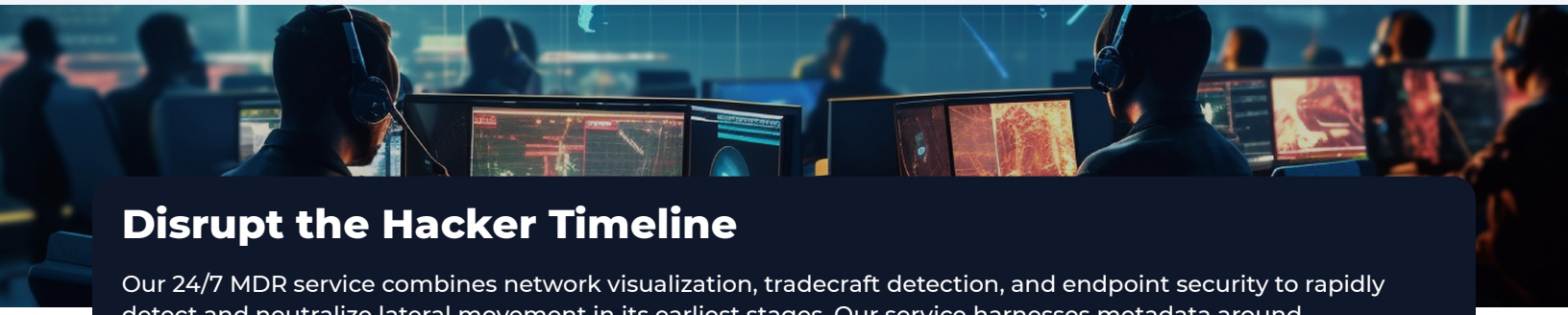
MDR can validate whether EDR has done its job correctly. In one instance, an EDR tool reported that it had blocked malware from a USB device. Our MDR found that was not the case. Instead, the malware had actually run and carried out commands, but had simply hidden its tracks from the EDR. Thankfully, our 24/7 SOC isolated the device and prevented further activity.

DETECTS WHAT EDR DOESN'T

Our MDR catches stealthy hacker activity that EDR can't detect. In 2022, we found that 86% of the time, EDR tools had failed to detect the attacks its security team detected and responded to. Perhaps EDR would have detected the attack later, once malware was in use, but in that case the impact of the breach would have been higher.

COVERS COMPREHENSIVELY

While EDR is limited to comprehending activity on isolated devices, or endpoints, our MDR understands the network holistically based on behavior between endpoints, providing the context and visibility to track hackers' movements through an entire network.



Disrupt the Hacker Timeline

Our 24/7 MDR service combines network visualization, tradecraft detection, and endpoint security to rapidly detect and neutralize lateral movement in its earliest stages. Our service harnesses metadata around suspicious events, hacker tradecraft, and remote privileged activity to catch what others miss and take action before cyberthreats can spread.

Take a proactive, offensive approach to stay ahead of cybercriminals by adding continuous monitoring, real-time threat detection, and active response to defend your digital estate.

▶ Get started with MDR by contacting us today.

AccuTech™ International

866-248-0250 | info@accutech.com | accutech.com