

Why ActZero MDR?

There are a lot choices when it comes to a Managed Detection and Response service. ActZero includes the Technology + People + Processes in one SKU, starting with leading EDR solutions like **CrowdStrike** or **Defender** and **Stellar Cyber XDR**, without the complexity or expense of other MDR services.

Coverage across entire IT environment

Collect data from all endpoints, network, mobile devices, cloud, identity, and email accounts, using tools such as EDR, XDR, NGAV, SIEM, CSPM, log management, and vulnerability scanning to detect threats effectively.

Better block rate with top EDR

ActZero MDR service includes CrowdStrike EDR and NGAV licenses enhanced by our own AI/ML capabilities with an **88% block rate**.

Fewer alerts

AI engine generates detections and unifies telemetry across multiple security stack components, for real-time endpoint and account attack blocking, resulting in fewer false positives with fewer than **6 alerts per month**.

Quick response

AI works across platforms to contain threats in **~10 milliseconds** and inform human threat hunters and enable proactive measures resulting in faster response. **<6 min Mean Time to First Response** compared to industry average of 30 minutes.

Bundled MDR service

ActZero offers a complete MDR service bundled for easy pricing and fair pricing by endpoints per month with a single SKU, simplifying the procurement process for customers.

Round-the-clock coverage

24/7 SOC analysts available to review detections, triage, and respond to prevent incidents.

Incident Response Retainer

ActZero offers quarantine, elimination, and recovery services as part of our package, simplifying incident management.

Fast Deployment & Self Onboarding

Quick remote deployment and self-onboarding within hours to a few days, saving time and securing the environment faster.