



Managed Detection and Response (MDR)

In today's cyberthreat environment, small to medium-sized businesses are finding themselves in the crosshairs of cyber criminals. Immunity to cyber threat doesn't exist, so staying agile and building a proactive defence is critical in protecting your operations

With the rate of cloud adoption and remote working increasing, the need for robust security tailor-made for cloud technology does so too. Cloud environments are not immune to cyber threats with companies top challenges including data loss, compromised credentials and resources, privacy and compliance issues.

Traditional cyber technologies such as anti-virus or antimalware are not enough. That is why Kaizen have teamed up with cyber security experts Blackpoint Security Operation Centre (SOC). Their 24/7 SOC team is focused on catching breaches and rapidly responding to contain them. Made up of former US intelligence cyber experts with real-world experience, their only mission is to monitor your networks and detain advanced threats before lateral spread compromises your livelihood.

When an attack occurs within your business, detection and response times often determine whether malicious actors succeed in their efforts to execute and install scripts or dangerous software throughout your network and satellite staff.

Designed with MDR objectives and workflows in mind, the Blackpoint ecosystem can detect breaches faster than any other current solution on the market with true 24/7 protection.

Harnessing metadata around suspicious events, hacker tradecraft, and remote privileged activity.

When an attack occurs within your business, Blackpoint MDR isolates compromised business endpoints, its technology terminates malicious processes and stops the threat from moving laterally into other systems.

Monitor - Blackpoint hunts proactively for evolving threats 24/7, maintaining full visibility of your entire network. The experienced team leverages leading-edge, proprietary technology to monitor for indicators of compromise, malicious behaviour and open risks.

Detect - Every second counts when it comes to detecting the first signs of breach. Blackpoint detects and isolates developing threats before they can spread laterally. We investigate suspicious activity on your behalf and eliminate alert fatigue and time spent on false positives.

Respond - The fastest response times seen by the industry, Blackpoint isolates and stops malicious processes. We take action to neutralise threats in real-time rather than sending you instructions to action yourself. Get alerted after the risk is eliminated and we've secured your environment.

- Realtime threat detection with active 24/7/365 SOC (Security Operations Centre)
- Cross platform Managed Detection and Response (MDR) application
- Contextually aware breach detection and response
- Cross platform Managed EDR (Endpoint Protection and Response) integration with Windows Defender for Endpoint, SentinelOne, BitDefender and others
- Cloud Response for M365 and Google cloud platforms - account isolation and compromise protection

