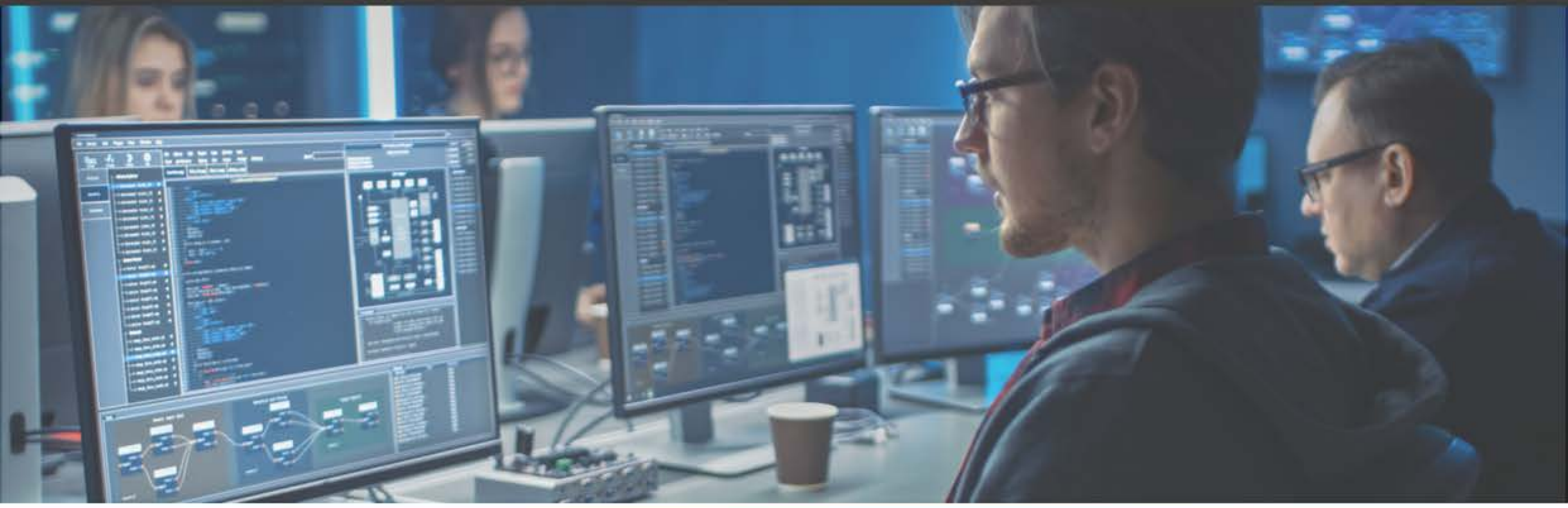
aztech
IT Solutions

MDR | Managed Detection Response
Datasheet



Organisations of all sizes face increasing cyber threats. MDR Managed Detection Response is core to a comprehensive cybersecurity strategy to protect businesses from these threats. MDR provides an extensive layer of defence that can detect malicious activity in real-time and respond quickly to neutralise the threat. MDR solutions are also cost-effective and require minimal maintenance, meaning businesses can trust their MDR systems to be reliable and secure.

AZTech's MDR services is delivered by its CSOC Cyber-Security -Operations Centre team and leverage SentinelOne.

Our Cyber Security Operations Centre will monitor and scan for suspicious activity across your systems, searching and identifying anything that may signify a security breach or compromised system.

Unlike traditional antivirus software that identifies and quarantines files suspected of Malware, AZTech's Managed Detection
and Response is designed to look for and record system activity on your endpoints, providing you with the real-me visibility you need

Organisations are constantly adding to their endpoints, whether it's desktops, smartphones or even the Internet of Things (IoT) - there are now countless ways for cybercriminals to gain access to your data. Endpoint visibility is critical to every organisation, as antivirus software can only protect you so far against cybercrime. Many types of Malware are hard to detect with traditional methods, such as file-less Malware that operates in your computer's memory, hidden from malware signature scanners.

Outsourcing MDR and cybersecurity needs to an MSSP such as AZTech can benefit businesses in several ways. MDR services from AZTech can save time and money for organisations by taking the burden of maintaining an in-house MDR solution off of IT teams.

MDR services can also provide better visibility into security threats and reduce the time it takes to identify, investigate, and remediate incidents. MDR services from AZTech can also offer cost savings by reducing the need to hire and train dedicated MDR personnel and the overall cost of MDR solutions.

Additionally, MDR services provide 24/7 coverage, ensuring that security threats can be identified and addressed quickly and accurately. MDR services can also detect threats that may have been missed by traditional security solutions, further improving an organisation's security posture.

aztech IT Solutions

MDR | Managed Detection Response
Features

Managed Detection & Response (MDR)

Managed Detection and Response from AZTech IT scans your endpoints for abnormal activity and alerts the security team.

This way, any malware, whether hidden from malware signature scanners or easily detected, our CSOC team will be alerted and begin investing further, isolating and removing the issue so that you can continue business as usual.

24/7/365 Detection & Response

With 24/7/365 threat detection and response, our Cyber Security Operation Centre (CSOC) Team gains real-me visibility of cyber threats to your endpoints and network. By utilising multi-layered best of breed security tools and continuous monitoring, any anomaly or suspicious activity will alert our security team to investigate and respond immediately, 24/7.

Threats are evaluated and dealt with accordingly, allowing our team to respond and diffuse directly and for you to focus on your business.

Automated threat detection and response

SentinelOne MDR uses advanced machine learning algorithms to detect and respond to cyber threats quickly, automatically, and accurately.

Monitor

With our MDR Solutions, your endpoints will be monitored daily with real-me visibility to collect activity data that may indicate threats.

Analyse

We can analyse the collected data to identify threat patterns to help detect any breach attempts and stop them immediately.

Fast Response

Fast and accurate response to remove, contain or stop attacks before they become a breach so that you can continue business as usual.

Cost Effective

No capital outlay, Monthly fixed costs based on the number of protected endpoints

Real-Time Visibility

Real-time visibility allows you to act as soon as an anomaly is detected, helping to prevent a breach.

Why is having a CSOC and MDR important?

Every device connected to your network is a potential entry point to your data, making it a target for cybercriminals.

Zero-day attacks and Advanced Persistent Threats are more severe security issues organisations face. With the rise of BYOD (Bring Your Own Device), mobile attacks and advanced hacking techniques have only increased your risk of becoming a victim to a data breach. Your classic anti-virus software can detect malware when there's a matching signature. Still, it cannot determine if the attacker has access to your endpoint just by monitoring the activity.

Cybercriminals have evolved their ways of attacking businesses and individual users, which is why you need Security Operations Centres to react to their new ways of infiltrating your organisation's data.