

MANAGED DETECTION & RESPONSE (MDR)

THE GCX APPROACH



GCX recognises that there are many customers today that are rapidly migrating to a digital world, which leads their attack surfaces to expand, and often with less centralised control, the need to detect threats before they cause irreversible damage is greater than ever. Many organisations are struggling with the increase of cybersecurity tools and technologies, striving to filter large amounts of data quick enough to detect and respond to critical cyber threats. Our MDR helps organisations improve threat visibility by providing targeted, timely telemetry for reliable detection, simplified investigation, and precise responses to contain and mitigate threats.

GCX MDR combines the critical elements required to introduce enterprise-class cyber security to businesses. Our solution adapts to your business, designed to deliver quality cyber security that is always improving.

EFFECTIVE SECURITY

Our next generation security platform is fully aligned to the MITRE framework and is designed from the ground-up to detect and prevent new and sophisticated threats, as well as known threats:

- Sophisticated behavioural and machine learning-driven threat protection- improved accuracy, efficiency, and decision-making
- Extensive detection and prevention of ransomware, zero-day exploits, privilege escalation and more
- No daily updates required – signature-less threat protection
- Attack timeline visibility and context – identifying commonality of infection points
- Light incident response – threat containment and remediation

BUSINESS SECURITY

An all-encompassing unified solution designed from the ground-up to provide a multitude of security solutions, combining people and security orchestration designed to secure and continually improve your entire business security against today's threats, including:

- 24/7 Follow the Sun Managed Detection and Response (MDR) – Cyber criminals never sleep
- Tailored Threat Hunting & Threat Intelligence – Flexible to meet your needs
- Security Orchestration, Automation and Response (SOAR) - Speed up incident resolution
- Business 'Defence in Depth' Assessment, Plan and Roadmap- to protect the Confidentiality, Integrity and Availability of your network and the data within
- End point detection and response (EDR)

GCX MANAGED DETECTION | THREAT HUNTING | THREAT INTELLIGENCE | INCIDENT RESPONSE

Around the clock our Global CSOC services are providing a threat monitoring managed detection, threat hunting, threat intelligence and incident response service. To defeat sophisticated adversaries focused on breaching your organisation, you need a dedicated team working for you to proactively identify and mitigate attacks.

- A global team of expert threat hunters, watching your back around the clock
- Augment your existing in-house resources, to improve operational efficiency
- Real-time threat correlation with the 'power of the crowd' to identify new and emerging threats
- Attack attribution and identification of unique adversary TTPs (tactics, techniques, and procedures)
- 40+ threat intelligence sources tracked and correlated around the clock
- Containment of threats from spreading on the network
- Remediation of threats by restoring endpoints to a form of 'known good'
- Investigation and situational awareness of endpoint activity in real-time
- Response Reduce alert fatigue with proactive notification and actionable alerts

CLOUD ARCHITECTURE

By using our cloud based MDR architecture, our customers reduce overheads, friction and cost while benefitting from the most comprehensive security solution available today with an entirely new cloud-based architecture. The simplicity of the architecture provides the freedom to replace and retire the complicated, performance - robbing security layers that clutter security environments.

- Turnkey solution – fast & easy deployment without disruption on the endpoint, lightweight sensor with no reboot required
- Immediate time to value — no hardware, additional complex software or configurations required
- Complete protection for Windows desktop and servers, Mac OSX and Linux, even when off the network
- Rapid scalability through our cloud based platform

WHY CHOOSE GCX?

GCX provide a flexible range of global services that can be as simple as assisting you to deliver and support your own self-build network through to providing a fully managed outsource service. Our solutions are backed by a team of expert consultants who can assist on every step of your data journey, whether it is design concerns like resilience or security, OEM and carrier selection, deployment, and management we are there all the way with approaches that adhere to best practices and are standards led wherever possible.

Our global presence ensures that we can deliver and support whenever, wherever.