

Cyber Security

Stay Ahead of Cyber Threats with Our
Managed Detection and Response Service

canaryit.com.au





Hunt Down Cyberattacks Before They Impact Your Business

In an era defined by relentless cyber threats and evolving attack vectors, safeguarding your organisation's digital assets demands a proactive and vigilant approach.

Ingesting data from your existing cyber security investments, our MDR service offers a proactive approach to cybersecurity. We combine advanced threat detection capabilities with expert response protocols to safeguard your organisation's digital assets.

The Challenge

In the face of sophisticated cyber threats, traditional security measures such as antivirus software and firewalls are no longer sufficient to protect organisations from data breaches and cyberattacks. The challenges organisations face include:

- 1. Advanced Threat Landscape:** Cybercriminals are continuously developing new and sophisticated methods to infiltrate networks, steal data, and disrupt operations.
- 2. Limited Security Resources:** Many organisations lack the internal expertise and resources to effectively detect and respond to cyber threats in real-time, leaving them vulnerable to attacks. Finding, training, and retaining experienced security professionals has become a major obstacle for organisations of every size.
- 3. Detection and Response Time:** Traditional security solutions often focus on perimeter defences, such as firewalls and antivirus software, which may not provide sufficient visibility into internal network activity. As a result, organisations may struggle to detect intrusions and respond to security incidents in a timely manner, allowing attackers to dwell undetected within their networks for extended periods.
- 4. Complexity of Security Tools:** Managing multiple security tools and platforms can be overwhelming for IT teams, making it difficult to correlate and analyse threat data leading to gaps in coverage and delayed response times.

5. Escalating Costs: Staffing an entire SOC to protect an organisation is a costly endeavour and is not feasible for many organisations.

6. Regulatory Compliance: Compliance mandates impose stringent requirements on organisations to protect sensitive data and report breaches promptly placing additional pressure on organisations to implement robust cybersecurity measures to protect sensitive data and avoid penalties.

7. Risk of Data Breaches: The consequences of a successful cyberattack can be severe, including financial losses, damage to reputation, and legal liabilities. With data breaches occurring with increasing frequency, organisations must prioritize proactive security measures, such as MDR, to mitigate the risk of data loss and business disruption.

The Solution

'CanaryProtect' MDR from Canary IT

Introducing CanaryProtect Managed Detection and Response (MDR) service, a comprehensive cybersecurity service engineered to reinforce your defences against the most advanced cyber threats. Remotely delivered, human-led, modern security operations centre (SOC) functions include 24/7 monitoring, rapid incident response, and continuous security enhancements.

Our MDR service empowers your organisation to stay one step ahead of cybercriminals and maintain a resilient security posture in today's dynamic threat landscape.





Safeguard your resources and reputation for a fraction of the cost of an in-house Security Operations Centre.



Network Inspection

Continuous network traffic inspection that detects malicious activity to/from suspicious IP addresses and domains



Cloud Security

Monitors cloud services, SaaS apps, IaaS infrastructure, and SecOps services to identify malicious user activity



Threat Detection

Identifies malicious files/EXEs, malicious traffic, bad IP addresses/domains, and lateral movement through Windows event log and Sysmon monitoring



Managed Containment

Detect indicators of compromise and prevent the spread of threats



24x7 Monitoring

A cloud-based SOC staffed by security analysts who monitor your on-premises and cloud resources 24x7



Leverage Existing Infrastructure

Leverage existing security technologies within your current environment without worrying about vendor lock-in or replacing your existing systems.



Log Analysis and Search

Automatically collects, normalises, analyses, and retains data from existing networks, and applications





Detect | Respond | Recover

Stay Ahead of Cyber Threats with Our Managed Detection and Response Service.

Detect



Develop greater insight into your security posture with broad visibility, 24x7 monitoring, and advanced threat protection.

Broad Visibility

Works with your existing technology stack to discover and profile assets and collect data and security event observations from multiple sources.

24x7 Monitoring

Your environment is monitored for threats and risks around the clock, allowing you to focus on other important areas of your business.

Advanced Threats

Catch advanced threats that are missed with other approaches with a platform that analyses more security data, and an experienced team who knows how to look for them.

Respond



Ensure threats are contained before they can do damage with managed investigation and guided response.

Managed Investigations

We investigate suspicious activity so you don't have to, making alert fatigue and time wasted on investigating false positives a thing of the past.

Incident Response

Every second counts. Detect and respond to critical security incidents within minutes to prevent the spread of threats.

Log Retention and Search

Takes the work out of managing logs, enabling you to easily conduct additional investigations, if needed.

Recover



Learn from incidents and make sure they don't happen again by implementing custom rules and workflows to harden your security posture against future attacks.

Guided Remediation

We work with you on detection, response, and remediation to validate the threat has been neutralised and verifying it hasn't returned.

Root Cause Analysis

Deep investigation into the root cause of incidents to promote the creation of customised rules and workflows that harden your posture.

Personalised Engagement

Regular meetings to review your overall security posture and find areas of improvement that are optimised for your environment.



Canary
Technology Solutions

Brisbane | Canberra | Melbourne

Level 3, 95 Pitt Street
Sydney, NSW 2000

1300 CANARY
connect@canaryit.com.au
canaryit.com.au