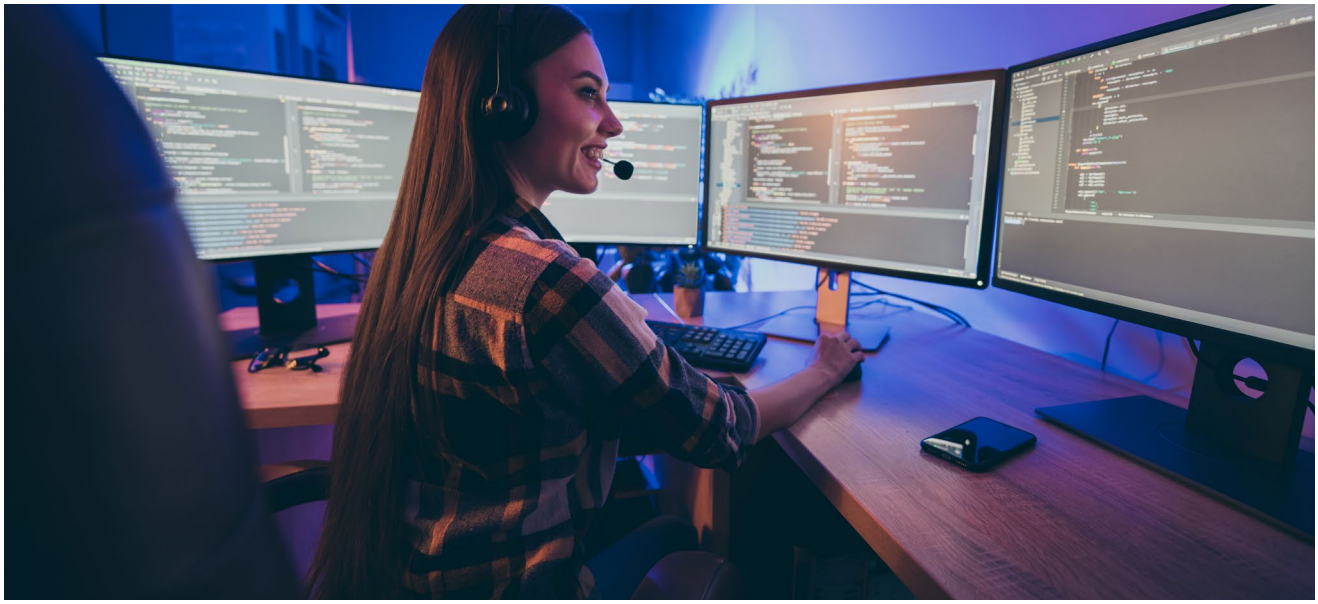
Cyber Detection and Response – Endpoint



More remote users, devices and data make endpoints an easy target. In fact, 70% of cyber breaches originate at the endpoint*.

Telstra's Cyber Detection and Response - Endpoint is a fully managed monitoring service that helps protect your data assets and business operations from malware and ransomware across your endpoints 24x7, whilst providing response and remediation capabilities on your behalf.

What is Cyber Detection and Response – Endpoint?

The Cyber Detection and Response – Endpoint solution enables you to quickly address the escalated frequency and threat level of broadened attack surfaces and increases in both known and unknown vulnerabilities.

It is a 24x7 fully managed monitoring service that helps detect, investigate, and neutralise discovered threats on your behalf. Unlike many solutions, it doesn't just issue notifications; it also helps remediate and remove the threat.

The solution is vendor agnostic utilising Microsoft Defender for Endpoint or Crowdstrike Falcon Insight.

Importantly, your infrastructure doesn't need to be managed by Telstra to use this service.

Features

Replace legacy anti-virus: Automatically block detected malware with expert human oversight to remove false positives

Initial Policy Consultation: Let our experts evaluate your security environment now, and where it needs to be

Continuous false positive reduction: Automate threat reviews and minimise alerts to the ones that count

Manual remediation: Custom policy enforcement utilising 'living off the land' techniques

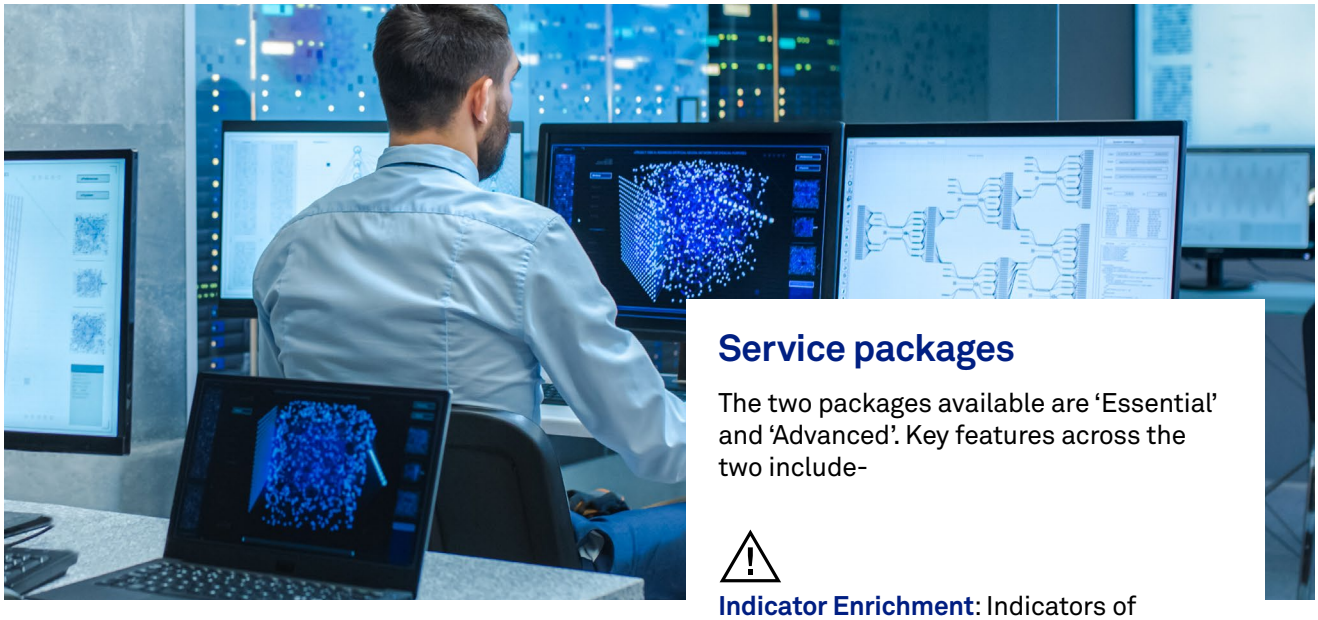
Continuous policy adaption: Evolve and rewrite policies as your needs change

Root cause analysis: Remote investigation of all positively identified malicious activity

Real time response: Manually interact with endpoints to push custom scripts or extract forensic data

Threat hunting: Deploy analytics to help identify activity that may have bypassed traditional detection methods

* Source: IDC



Key Benefits

1. **Helps defend against increasingly frequent and sophisticated cyber attacks**

   Analysts monitor your endpoint security posture 24/7 and respond to incidents.

2. **Expands your cybersecurity capabilities via a 24/7 managed monitoring service**

   The solution leverages expertise and resources that are not readily available 24x7 to many organisations. Unlike many solutions, Cyber Detection and Response Endpoint doesn't just issue notifications. Instead, it can help remediate and remove the threat.

3. **Provides the support of world-class security expertise**

   Telstra Cyber Detection and Response Endpoint isn't simply a reactive solution responding to threats as they appear: it combines cutting edge technology with an elite team of security analysts to extend your existing technologies and team. In addition, our experienced security professionals can assist in deployment and provide ongoing security assurance services where required.

Service packages

The two packages available are 'Essential' and 'Advanced'. Key features across the two include-

Indicator Enrichment: Indicators of compromise associated with detections within the monitored environment are automatically extracted, scored, and enriched, leveraging open source and proprietary threat Intelligence tools.

Endpoint Response: Telstra will take a specific set of actions at the completion of an investigation: quarantine, delete, whitelist, monitor, or blacklist. If an advanced investigation with live/real-time response is needed, remote intrusion response activities are also available.

Threat Detection: Advanced endpoint software is used to expand enrichment and enhance behavioural correlations. The result is that advanced threats can be isolated, in particular those that might evade many existing security solutions.

Advanced Threat Hunt: Part of the 'Advanced' service offering, this feature proactively and iteratively searches through events to help detect and isolate advanced threats that might evade many existing security solutions. It also enables remote hunt missions on a regular basis that perform manual and semi-automated activities for targeted data analysis to search for signs of advanced adversaries.