Cyber Vigilance
We've got your back...

Service Description
Managed Threat Detection

Cyber Vigilance's Managed Threat Detection Service is a foundational element of our 'Technology' pillar of Cyber Security Managed Services.

Service Features

Cyber Vigilance's Managed Threat Detection Service, powered by SentinelOne, continuously analyses all activity signals from your protected devices to provide threat protection of unmatched accuracy coupled with automated remediation workflows for all core attack vectors eliminating the need for complex multi-product security stacks, making robust breach protection available to our customers, regardless of their size or level of security skills. The Managed Threat Detection Service offers three levels of features/functionality.

This service offers the following Managed Endpoint Detection and Response (EDR) capabilities:

- Next Generation Anti-virus (NGAV) Static AI & Behavioural AI
- Remediation & Recovery
- Network & USB/Bluetooth Device Control
- Rogue Device Discovery
- Deep Visibility and Threat Hunting
- MITRE ATT&CK Integration
- 24x7 SOC Services

Cyber Vigilance continuously monitors and analyses your endpoint and network activity for threats and suspicious activity.

Cyber Vigilance
We've got your back...

Service Description
Managed Threat Detection

Singularity Core

Our entry-level service is built on SentinelOne's Singularity Core. Singularity Core is suitable for organisations that want to replace legacy Anti-Virus or NGAV with endpoint protection (EPP) that is more effective. Core also offers basic EDR functions demonstrating the true merging of EPP+EDR capabilities. Singularity Core features include:

- **Built-in Static AI and Behavioural AI** - analysis prevent and detect a wide range of attacks in real-time before they cause damage. Core protects against known and unknown malware, Trojans, hacking tools, ransomware, memory exploits, script misuse, bad macros, and more.
- **Sentinels are autonomous** - which means they apply prevention and detection technology with or without cloud connectivity and will trigger protective responses in real-time.
- **Recovery is fast** - and gets users back and working in minutes without re-imaging and writing scripts. Any unauthorised changes that occur during an attack can be reversed with 1-Click Remediation and 1-Click Rollback for Windows.

Singularity Control

Control is for organisations seeking the best-of-breed security found in Singularity Core with the addition of "security suite" features for endpoint management. Control includes all Core features plus:

- **Firewall Control** - for control of network connectivity to and from devices, including location awareness.
- **Device Control** - for control of USB devices and Bluetooth/BLE peripherals.
- **Rogue visibility** - discover devices on the network that need SentinelOne agent protection.
- **Vulnerability Management** - in addition to Application Inventory, for insight into 3rd party apps that have known vulnerabilities mapped to the MITRE CVE database.
- **Secure remote shell** - enabling remote access to a managed SentinelOne device from the Singularity cloud console.

Singularity Complete

Complete is for enterprises that need modern endpoint protection and control plus advanced EDR features that we call ActiveEDR. Complete also has patented Storyline technology that automatically contextualises all OS process relationships [even across reboots] every second of every day and stores them for your future investigations. Singularity Complete automatically correlates telemetry mapping it into the MITRE ATT&CK framework. Complete includes all Core and Control features plus:

- **Patented Storyline** - for fast Root Cause Analysis and easy pivots.
- **Integrated ActiveEDR** - visibility to both benign and malicious data.
- **14-day data retention**.
- **Hunt by MITRE ATT&CK Technique.**
- **Mark benign Storylines as threats** - for enforcement by the EPP functions.
- **Custom detections and automated hunting** - rules with Storyline Active Response (STAR).

Cyber Vigilance
We've got your back...

Service Description
Managed Threat Detection

24x7 SOC Service

Singularity Core, Control and Complete benefit from Cyber Vigilance's SOC service.

This service includes:

Monitoring & Alert Analysis

Cyber Vigilance monitors all activities and alerts 24 hours a day, 365 days a year. The service includes analysis of alerts and response to detected threats, enabling us to ensure that threats are identified and mitigated within the agreed SLA response times. The Cyber Vigilance SOC team proactively handles events and will contact your designated point of contact in the event of a detected threat.

Malware Analysis & Threat Remediation

Cyber Vigilance's team of experts will investigate and assist in mitigating and remediating a breach in your environment. Cyber Vigilance mitigates and resolves any threats using SentinelOne's "Kill, Quarantine, Remediate and Rollback" capabilities. Every threat is reviewed, acted upon, and documented to keep you in the loop with proactive notifications.

Should a suspicious threat lead to a Critical Risk severity incident, a Cyber Vigilance analyst will contact you over the phone to make sure you are aware of the incident and to agree on a remediation plan.

Threat Hunting * Singularity Complete Only.

Cyber Vigilance's SOC analysts use data collected by the platform to perform proactive incident-driven threat hunting. Data analysed during threat hunting can be used to create new threat intelligence and identify new indicators of compromise. Our analysts utilise SentinelOne's Storyline technology to uncover the root cause of a threat.

Protect
Prevent attacks a wide variety of attacks using static and behavioural AI.

Monitor
Our analysts continuously monitor your environment, ready to respond to threats.

Remediate
We will mitigate any threats and send you proactive notifications to keep you in the loop.

Deep Dive
Trigger deep dive analysis to identify the root cause of an alert.

Cyber Vigilance
We've got your back...

Service Description
Managed Threat Detection

Support

Cyber Vigilance will be the point of contact for all support issues relating to the service. Our team is responsible for level 1 and 2 support.

Level 1 Support
- Collection of relevant information.
- Problem identification and analysis.
- Initial diagnosis.
- Troubleshooting.
- Problem Resolution, where possible.

Level 2 Support
- Perform greater troubleshooting and diagnosis.
- Potentially replicate the issue in a test lab environment.
- Provide Workaround solutions to End User issues.

Where required, Cyber Vigilance can escalate a support ticket to SentinelOne support. Cyber Vigilance will be the point of contact for any such cases.

Onboarding Process

To get your organisation on board as quickly as possible, the Cyber Vigilance team will work alongside you to provide support and guidance throughout the onboarding process.

Cyber Vigilance will arrange a welcome call to guide you through the initial steps:
- Outline the requirements for successful deployment.
- Answer any technical questions and queries you may have.
- Provide the security agent software for your endpoints.
- Continued support and assistance from the Cyber Vigilance team during the agent rollout phase.

The entire solution, including the endpoint agent, is fully managed remotely using our Singularity cloud management console.

Once the deployment of the agents has been completed, Cyber Vigilance will provide ongoing monthly reporting, giving you complete visibility of how you are protected. The report includes key statistics on alerts and threats.

Cyber Vigilance
We've got your back...

Service Description
Managed Threat Detection

Customer Responsibilities

The Customer is responsible for providing Cyber Vigilance with key points of contact for our team in the event of a cyber incident. At least one of the elected Customer representatives must be always available and have the appropriate approval to take decisive action in the event of a breach.

The Customer will be responsible for deploying the SentinelOne agent to their corporate assets.