THRIVE℠

SERVICE DESCRIPTION

Endpoint Security and Response

Executive Summary

Thrive Endpoint Security and Response Service Definition

Thrive Endpoint Security and Response service provides Next Generation malware detection & protection for servers and workstations. With the advent of sophisticated malware such as fileless attacks and zero-day executables, a feature rich signature-less endpoint solution is needed in many organisations. Our solution offers all of the necessary features to combat advanced endpoint attacks while meeting multiple compliance guidelines that typically require traditional antivirus protection.

Services Scope

The service shall include:

- Workstation and server endpoint software security agent
- Cloud-based aggregation and processing of security events
- One (1) Client administrator login for reporting and visibility
- Management of whitelist exclusions for common applications
- Device Isolation in the event of attack or theft
- USB Blocking Functionality (requires implementation plan)
- Alerting to Thrive Security Operations Center (SOC) for all Malicious and Suspicious level events

Thrive Scope of Work and Deliverables

- Thrive shall provide all license subscriptions for the endpoint security agents.
- Thrive shall perform initial configuration of Client console and develop ongoing support strategy including Client communication and general steps on response handling for threats generated by the Thrive endpoint security platform.
- Thrive shall perform investigation and analysis of all Malicious and Suspicious level alerts and determine response actions, if required. Thrive shall provide notification to the Client of events that require action with remediation instructions. If the affected endpoint is under management by Thrive under separate Managed Server or End User Support managed services, Thrive shall remediate the endpoint provided it can be accessed remotely by Thrive.

Client Responsibilities

- Client shall be responsible for deployment of the software security on subscribed servers and workstations. If Client subscribes to Thrive Managed Server and/or Thrive End User managed services, Thrive shall perform security agent installation utilising existing Remote Monitoring and Management (RMM) tools in the agent deployment.
- Client shall ensure all required server, workstation and firewall ports are open to all the endpoint security agent to communicate to the Thrive security platform.
- Client must notify Thrive of any new servers or workstations requiring an endpoint security agent subscription and deployment and of workstations and servers that are removed or decommissioned.
- If Client requires integration with a 3rd party Security Information and Event Management platform, Thrive shall assist with consultation related to the Thrive endpoint security platform configuration.

Service Limitations

- If the endpoint security agent is reported in the management console as “Degraded”, Thrive will not investigate end user workstations or servers for compatibility or insufficient resource issues that prevent the security agent from operating (unless subscribed to Thrive End User support)
- The security agent does not provide scheduled or on-demand scans.

Service Exclusions

Any service not explicitly defined in the Endpoint Security and Response Service Description above is considered out of scope and may be provided under separate agreement for an additional fee.