THRIVE SM

SERVICE DESCRIPTION

Secure Internet Gateway

Executive Summary

Thrive Secure Internet Gateway Service Definition

Thrive Secure Internet Gateway provides the first line of defense against threats on the Internet. Utilising the Cisco Umbrella platform, the service delivers visibility into Internet activity across corporate network locations and blocks threats before they ever reach end points. As a cloud-delivered, open platform, Umbrella integrates easily with existing security infrastructure and delivers live threat intelligence about current and emerging threats. By analysing and learning from Internet activity patterns, Umbrella automatically uncovers attacker infrastructure staged for attacks, and proactively blocks requests to malicious destinations before a connection is even established — without adding any latency for users. With Umbrella, phishing and malware infections can be stopped earlier, infected devices identified faster, and data exfiltration prevented.

Services Scope

The service shall include:

- Cisco Umbrella roaming agents for all subscribed users
- Configuration of roaming agent DNS to direct end users to Cisco Umbrella for name resolution
- Blocking of malicious content
- Standard content category filtering policy
- Custom content category filtering enabled upon request
- Custom “Content Blocked” page upon request

Thrive Scope of Work and Deliverables

- Thrive shall create a Client tenant within the Thrive Secure Internet Gateway platform.
- Thrive shall deploy the Cisco Umbrella roaming agent to end user devices. Clients that are not subscribed to Thrive End User Support will be responsible to deploy the agent using their own Remote Monitoring and Management (RMM) platform.
- Thrive shall apply a standard content filtering policy for protection against the following:
    - Malware
    - Command and Control Callbacks
    - Phishing Attacks
    - Cryptomining
- Thrive shall upon Client request enable additional content category filtering. Examples of these are Social Networking, Adult Themes, Gambling, etc.

- Thrive shall upon Client request customise the “Content Blocked” web page that users will be directed to when attempting to access malicious or blocked sites.

Client Responsibilities

- Client shall provide Thrive with a list of all subscribed users.
- Client shall notify Thrive of any new users or users that should be removed from the service.
- Client shall be responsible for notifying Thrive of any additional content categories beyond the standard filtering categories listed above
- Client shall provide Thrive with a primary point of contact for the Secure Internet Gateway service.

Service Exclusions

Any service not explicitly included in the Security Awareness Training Definition above is considered optional and may be provided under separate agreement for an additional fee.