

TABLE OF CONTENTS

1	INTRODUCTION	2
2	SERVICE OFFERINGS	2
2.1	CORE COMPONENTS	2
2.2	SUPPORTED DEVICES.....	4
3	SUPPORT	7
3.1	REQUIREMENTS FOR THIS SERVICE	7
3.2	SYNOPTEK RESPONSIBILITIES	8
3.3	CUSTOMER RESPONSIBILITIES.....	9
4	OPTIONAL SERVICES	10
4.1	ITAAS SITE – ADDITIONAL DEVICES (OPTIONAL)	10
4.2	NETWORK ANOMALY DETECTION (OPTIONAL).....	10
4.3	SIEM AS A SERVICE (OPTIONAL)	10
4.4	DESIGNATED CONSULTING ENGINEER (OPTIONAL)	10

1 INTRODUCTION

This Service Definition is subject to all terms and conditions of the Service Order to which it was attached. This Service Definition describes and contains additional terms that apply to Synoptek’s ITaaS Site (the “Service”).

This service definitions found herein reflect Companies standards at the time the Service Order(s) was issued. Company reserves the right to change any particular standard herein to reflect the current company best practices or industry standards at its sole discretion with or without notice.

2 SERVICE OFFERINGS

This service provides the Customer with management of Network devices to ensure a Site location has high availability, performance and security. The site location can be either a customer premise or Cloud environment. This is accomplished through constant monitoring, troubleshooting, timely maintenance, and proactive administration tasks. Synoptek can provide monthly reports documenting critical alerts and event resolutions. Should a problem be discovered through Synoptek’s remote monitoring, Synoptek will make every attempt to rectify the condition in conformance with the Service Level Agreement.

2.1 CORE COMPONENTS

FEATURE AND DESCRIPTION:	ADDITIONAL INFO:	INCLUDED
24X7 STAFFED ADMIN/IT HELPDESK W/CASE TRACKING & REPORTING	Synoptek provides 24x7 support to Customer technical contacts and authorized technical team members relative to subscribed tools and services.	YES
PROACTIVE MANAGEMENT SYNOPTEK INFRASTRUCTURE AND SYNOPTEK EDGE	<p>In order to supply the management capabilities in this service definition, the customer may require a dedicated physical or virtual monitoring device called the Synoptek Edge. This device aggregates all monitoring data and forwards to Synoptek’s centralized monitoring system. Customer is responsible for providing an environment for Synoptek to run the device.</p> <p>In addition to this device, Synoptek will maintain and manage all the equipment within the Synoptek Infrastructure and Network to provide the monitoring, maintenance and management of the customer’s network devices as described in this service definition, including:</p>	YES

	<ul style="list-style-type: none"> • Synoptek Data Centers, Networks, Servers, Switches, Storage Equipment and related components, including the required power, heating/cooling systems, security controls and fire detection/suppression equipment • Synoptek Building Management Systems (BMS) used to monitor Synoptek facilities • Synoptek Monitoring Infrastructure used to monitor and alert on Service components • Capacity Planning on Synoptek Infrastructure • Technology refresh/upgrades on Synoptek Infrastructure components. 	
ASSET TRACKING	<p>Synoptek configuration management tools are used to track basic Network equipment information. This information is useful for IT managers to make decisions relative to hardware procurement and replacement.</p> <p>If the Customer installs or decommissions any Network equipment (either physical or virtual), they must notify Synoptek in order to have the correct tools installed on their equipment. Synoptek has the right to audit a customer's environment and adjust billing to current volumes.</p>	YES
MONITOR, ALERTING AND REMEDIATION	<p>Synoptek provides proactive monitoring of Synoptek supported network equipment and services. Synoptek will provide customers with notification of alarms and/or events according to pre-defined usage thresholds assigned to each Component being monitored. Available parameters, thresholds and alerts vary based on the equipment being monitored.</p> <p>Should a threshold be exceeded, Synoptek will act to remediate. This could include contacting customer if assistance is needed to determine how to resolve. These thresholds are defaults only and may need to be adjusted based on the requirements of your specific environment to avoid too many false positives or to account for higher resource usage. The Customer can also designate a lower threshold value to receive direct email notification if they desire to have notifications and resolve at a lower value on their own.</p>	YES
CHANGE MANAGEMENT	<p>Synoptek will provide change management as it relates to the following:</p> <ul style="list-style-type: none"> • Processes and procedures to maintain the health and availability of the Monitoring Appliance, or the Service Offering. 	

	<ul style="list-style-type: none"> Processes and to release new code versions, hot fixes, and service packs related to the Monitoring Appliance, or the Service Offering. 	
PATCH REQUESTS	Customer may request security patching to be applied once per year, per device. These requests must be submitted as a new service request to the Synoptek Service Desk. Customer must specify targeted patch window in the request.	YES

2.2 SUPPORTED DEVICES

MANAGED FIREWALL	<p>Synoptek will service managed physical and virtual firewalls, inclusive of VPN support.</p> <p>The service may connect up to 5 VLANS (additional fees may apply for additional).</p> <p>This service supports up to 5 site-to-site VPN connections. Additional site-to-site VPN connection “bundles” can be purchased.</p> <p>Synoptek will back up managed device(s) configuration(s).</p>	YES
MANAGED ROUTER	<p>Synoptek will service managed physical or virtual routers.</p> <p>Synoptek will configure router monitoring using standard Synoptek-specified thresholds.</p> <p>Synoptek will configure alerts for all specified thresholds.</p> <p>Synoptek will backup the router configuration.</p>	YES
MANAGED SWITCH	<p>Synoptek will service managed physical or virtual switches.</p> <p>Synoptek will configure switch monitoring using standard Synoptek-specified thresholds.</p> <p>Synoptek will configure alerts for all specified thresholds.</p>	YES

	Synoptek will back up the switch configuration.	
MANAGED WIRELESS ACCESS POINT	<p>Synoptek will service all managed physical or virtual Wireless Access Points or LAN Controllers.</p> <p>Multiple WAPS would require purchase of ITaaS Site - Add-on services.</p> <p>Synoptek will configure Wireless Access Point monitoring using standard Synoptek-specified thresholds.</p> <p>Synoptek will configure alerts for all specified thresholds.</p>	YES
MANAGED CIRCUIT	<p>This service provides the Customer with a remote monitoring services for a Wide Area Network (WAN) or Telco circuit (e.g. T1, DS3, PRI, MPLS node, etc.).</p> <p>Customer must provide a Letter of Authorization (LOA) to allow Synoptek to act on their behalf.</p> <p>For Carrier provided network circuits, because of multiple factors outside the direct control of Synoptek, and due to the large variety of issues which can occur outside of Synoptek's control, the time to restore service for a Priority-1 incidents is "as soon as possible, best effort" and does not carry a specific Service Level Guarantee.</p>	YES
MANAGED LOAD BALANCER	<p>Synoptek will remotely monitor and remediate (troubleshooting and problem resolution) services for a supported Load Balancer (e.g. F5 LTM or other, including Virtual Load Balancer).</p> <p>This Service requires the ITaaS Server service with at least one Monitoring Appliance (physical or virtual) deployed on the Customer's network. This appliance provides remote monitoring and remote access capabilities for the Customer's network.</p> <p>The supported Network Device must be covered by an active manufacturer on-site support agreement with Synoptek listed as an authorized service contact with the manufacturer.</p> <p>The device being covered under this Service must be officially supportable by the device manufacturer for the life of this Service Order.</p>	YES

<p>MANAGED SD-WAN APPLIANCE</p>	<p>Synoptek will provide basic monitoring for the availability of the network service health that would device availability (i.e. CPU & memory utilization, interface status, throughput, device status, latency).</p> <p>VPN, connection status, cloud on-ramp connection status, and application performance are not monitored.</p> <p>Synoptek will provide support for physical and virtual SD-WAN Appliances, inclusive of VPN support for partial- or fully-meshed VPN topologies. Monitoring</p> <p>Synoptek will back up managed device(s) configuration(s) where supported through Command Line, Text-based configuration files.</p> <p>Support for SD-WAN appliances is limited to the existing configuration and does not include provisioning of new locations or making changes to the existing architecture or application profiles. These changes can be facilitated through Synoptek Professional Services or through Designated Consulting Engineer hours.</p> <p>The SD-WAN appliance must be covered by an active manufacturer support agreement with Synoptek listed as an authorized service contact with the manufacturer.</p> <p>The device being covered under this Service must be officially supportable by the device manufacturer for the life of this Service Order.</p>	<p>YES</p>
<p>MANAGED APPLICATION EXPERIENCE</p>	<p>Synoptek will augment managed SD-WAN appliance services with a quality of experience (QoE) monitoring and alerting for requested application services which incorporates user surveying and User Champion interview, qualitative assessment, and correlation with monitoring reports.</p> <p>Synoptek will create optimized profiles based on an analysis of customer's network topology and desired application services prioritization (e.g):</p> <ul style="list-style-type: none"> • Voice and Video • Cloud SaaS, IaaS and PaaS • Main, Edge and Branch Offices (excluding Home) <p>Cloud data and/or cloud file services (e.g. Box, Dropbox, Google Drive, OneDrive)</p>	<p>Discuss with your Client Advisor – Requires Managed SD-WAN Appliance + AE Add-On</p>

3 SUPPORT

The service and support operates 24x7x365. As the owner of the issue, Synoptek will log, track and isolate the problem, and either resolve the issue or escalate it to the appropriate service provider designated by Customer or to Customer's internal support group.

- Exclusions; Unsupported Incidents. These services are not intended as consulting, design or implementation services. The following items and functions are not supported under the Service: the administration of Customer's systems (including server set up and enterprise server configuration changes); on-site desktop support; device setup; data backup and file restoration; printer RMA issues; smartphone, PDA and tablet applications; and devices and applications not provided by Synoptek as part of the Service or specifically identified in a Statement of Work ("SOW") signed by the Parties.
- Communication of Out-of-Scope Issues. Out-of-scope issues identified by Synoptek will be documented and communicated to the Customer. The Customer will be responsible for management of its systems and must work directly with its manufacturer or vendor for assistance with unsupported, third-party applications and devices. The Customer also is responsible for failures caused by viruses, user abuse, environmental conditions and other causes not within Synoptek's control. Out-of-scope can be remedied with Synoptek Professional Services on a time and material basis.

3.1 REQUIREMENTS FOR THIS SERVICE

The following specifications are required for Synoptek's ITaaS Server Service:

- This Service requires the at least one physical or virtual monitoring appliance deployed on the Customer's network. This appliance provides remote monitoring and remote access capabilities for the Customer's systems.

The Customer must provide the following for installation of the physical monitoring appliance on the network the devices or systems to be monitored and/or managed are installed (Does not apply to Cloud customers):

- One rack unit (1U) of space for installation of the appliance. This appliance can be installed in a 2 or 4-post rack, or can be table-top mounted if a rack is not available. Maximum dimensions of the appliance are 10" W x 1.7" H x 7" deep.
- One 110 VAC power outlet (less than 1A total power required) for the appliance (single AC cord).
- Synoptek can also per Customer request provide a virtual guest appliance.
 - 2 vCPU, 8GB vRAM, 100GB of storage
- One 100 Mbps or 1 Gbps Ethernet connection switch port on the same network as the devices or systems being monitored.
- Note: The appliance must be able to initiate an outbound SSL/HTTPS connection to Synoptek Data Center for monitoring and remote access.

- The Customer is responsible to notify the Service Desk (Support@Synoptek.com) if it becomes necessary to disconnect from the network, shut down or restart the appliance.
 - As security is application-dependent, the Customer is responsible for the overall security of the System and the network it is connected to, including applications and data. Synoptek is not responsible for the security or the integrity of software or data installed on the System or any applications which it is running.
 - The Customer is responsible for any function, service or task not explicitly outlined above as a responsibility of Synoptek.
- This Service assumes that the systems being managed have been fully deployed, are stable and are operating at an acceptable level of performance. If not, the Customer should engage Synoptek Professional Services (PS) to correct any issues prior to deploying Managed Services.
 - If Synoptek is responsible for escalating hardware issues to the server manufacturer for resolution, the supported Systems must be covered by an active manufacturer on-site support agreement with Synoptek listed as an authorized service contact with the manufacturer.
 - If Synoptek is responsible for escalating operating system issues to the OS vendor for resolution, the supported software must be covered by an active support agreement with Synoptek listed as an authorized service contact with the vendor.
 - The system being covered under this Service must be officially supportable by the device and OS manufacturer for the life of this Service Order, i.e. must not be EOS (End of Support).

3.2 SYNOPTEK RESPONSIBILITIES

- Synoptek will configure the devices according to Synoptek best practices.
- Synoptek will by inherit process of monitoring devices keep an active inventory of the customers subscribed devices.
- Rule changes should be limited to less than 5 per month per site, additional changes may require Time and Material Change order prior to service.
- Synoptek will configure device monitoring using the following standard monitored metrics (if available), as detailed in Appendix A.
 - Synoptek will configure alert thresholds for all monitored metrics using standard Provider-specified thresholds.
 - Synoptek will verify that alerts are valid and actionable (i.e., filter out false alerts).
 - Synoptek will monitor for alerts from the monitoring agent for the supported Network Device and establish Priority level (P1-P4) for each alert.

- Synoptek will monitor for alerts from the subscribed device(s) (provided in the service order or change orders) monitoring and resolve problems as they occur.
- Synoptek will create an Incident Ticket for each actionable alert.
 - In conjunction with the Customer, Synoptek will establish an Escalation Plan for each class of alert.
 - Synoptek will notify the Customer as Incident Tickets are created according the Escalation Plan.
 - In the event of a device failure requiring vendor support, escalate to the supported Network Device hardware vendor as determined by the pre-defined Escalation Plan.
 - Synoptek will coordinate with the hardware vendor and/or Customer for repair or replacement as required to resolve the incident, provided we have letter of authorization.
 - In the event of a device hardware replacement, Synoptek will attempt to configure the new device to the last known configuration.
- Synoptek will verify Customer acceptance of the final escalation plan.

3.3 CUSTOMER RESPONSIBILITIES

- During the initial setup of the Monitoring Appliance, Customer may need to provide customer's network/IT staff to answer questions, as required. Customer will need to rack the equipment and bring online. Alternatively, professional service team can be engaged for this task at additional charge.
- The Customer must not perform any action or change which would interfere with Synoptek's ability to monitor or access any device or system covered under this Service Order, including, but not limited to, the following actions:
 - Disabling or changing any user or service login accounts Removing or changing any Provider-supplied software setting
 - Adding deleting or changing any IP addresses associated with the device or system without first notifying Synoptek
 - Changing the Host Name of a device or system without first notifying Synoptek.
- The Customer is responsible for any function, service or task not explicitly outlined above as a responsibility of Synoptek.
- This Service does not include on-site response by Synoptek staff for problem resolution. All troubleshooting and problem resolution is done by Synoptek staff working remotely in conjunction with Customer staff and/or carrier staff where on-site tasks are required.
- The Customer is responsible for returning any Synoptek owned equipment upon end of term. Synoptek will provide shipping labels.

- It is the Customer's responsibility to manage and maintain active, on-site support contracts for all supported Network Devices with Synoptek listed as an authorized service contact with the manufacturer.

4 OPTIONAL SERVICES

These are recommended Add-On services to augment the standard devices and additional quantities in the Customer's environment. Each site includes up to four devices, the service "Add-On – Additional Devices" is used to include additional devices per site.

4.1 ITAAS SITE – ADDITIONAL DEVICES (OPTIONAL)

Standard ITaaS site includes up to 4 devices per location. Additional devices can be added on a per-device charge. Synoptek will tune alert threshold as needed to minimize false alerts.

4.2 NETWORK ANOMALY DETECTION (OPTIONAL)

Synoptek has the ability to monitor the traffic within your network and detect anomalies indicative of Security incidents

4.3 SIEM AS A SERVICE (OPTIONAL)

Synoptek's Security Information and Event Management service is designed to provide your organization logging and alerts of Security incidents detected from your equipment.

4.4 DESIGNATED CONSULTING ENGINEER (OPTIONAL)

Synoptek recognizes that you may have custom needs that are not met within this the standard definition of these services. Synoptek offers Designated Consulting Engineers (DCE) to be assigned to your account to work on custom initiatives. These are sold in reserved hours and are for the duration of your term.