Synoptek

Synoptek Owned Public Cloud

Service Definition

TABLE OF CONTENTS

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 owned Public Cloud (the "Service").

The 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's best practices or industry standards at its sole discretion with or without notice.

2 SERVICE OFFERINGS

Synoptek owned Public Cloud Hosting Services are designed to maximize the value of running workloads on a public cloud platform. This is a multi-tenant Infrastructure-as-a-Service (IaaS) Service Offering with logically isolated resources on shared physical infrastructure, configured as a single virtual datacenter with networking resources. This enables customers to assess cloud computing capabilities without having to build and maintain their own datacenter.

Synoptek owned Public Cloud Hosting Services (herein called the "Service Offering" (s)) allows for the hosting of virtual machines (here in called VMs) and applications on two different core platforms allowing IT organizations to extend their cloud infrastructure and software deployments beyond their datacenters.

- Hybrid Powered
  - Virtualization: based on VMware® vSphere® is used for management and automation.
  - **Region:** East Coast, US
  - **Region:** West Coast, US

All Service Offerings offer selections for compute, storage, networking and public IP address resources that can be expanded as your needs grow. Additionally, added features such as Data Protection, Managed Services and a growing list of ancillary data and application services are offered with Synoptek Public Clouds. All services include built-in infrastructure redundancy, high availability, firewalling, load balancing, NAT, DHCP, IPsec VPN, and higher disk I/O at no additional charge.

Having Service Offerings available in multiple regions enables you to manage region specific resources. You can run workloads closer to your business specific customers or comply with various regulations and other legal requirements. You can also choose to leverage multiple regions to enable redundancy of your data or workloads. Redundant configuration can play a role in your business continuity and disaster recovery strategy, which can include failing over to a second data center, protecting data by deploying to a second data center, or recovering operations in a second data center in the event of a disaster.

All services are available a-la-carte to create nearly any compute and storage combination. This includes: **1 vCPU, 1GB RAM, 1GB Blended Storage, 1 Public IP, 1 Virtual Firewall, 1 Site to Site Tunnel, 10Mbs Internet bandwidth and free MS Windows Server Standard OS license(s)**

Customer can add additional resources where needed. One public IP is included with each VM.

Excess bandwidth above committed usage is charge on a consumption model at a 50% premium. By default, bandwidth is capped at twice the committed usage.

3 SUPPORT

Synoptek will provide support for problems that the Customer reports to assist with adoption of and related to the Service Offerings 24x7x365. See Appendix A for more support matrix

Customer may assign up to 3 named contacts to contact the help desk on behalf of the Customer. The Help Desk is a central point of contact for handling the following Customer issues:

- Incident ownership, initial troubleshooting and escalation of incidents within the defined Service Level Agreement (SLA);
- Respond to "how to" questions such as how to provision or remove cloud instances and migrate data.
- Respond to access issues and requests;
- The service desk can be contacted at:
  - Toll-Free number TBD; region based.
  - Email at support@synoptek.com
  - https://www.autotask.net/clientportal/

The Client Advisor (CA) will serve as the single point of accountability in delivering the Service, providing the following support:

- Establish and manage relationship with identified Customer contacts.
- Work with the operations team proactively to identify opportunities and continually improve.
- Customer experience with respect to the services outline here.
- Define key measures and periodically review them with Customer.
- Pro-actively explain any high severity incidents, root causes, and resolution efforts.
- Coordinate with other business units as agreed, to ensure a unified Synoptek solution.
- Develop and review cloud consumption with Customer including forecast and growth projections.
- Public Cloud Best Practices
- Support Ticket Review
- Overall Cost Review

3.1 SERVICE PROVISIONING

Synoptek will provide the following provisioning services:

- Implementation of platform components (physical servers, physical storage, and physical network devices) needed to support contracted resource pools when applicable.
- Providing initial network resources including default public IP addresses when applicable.
- Providing initial resource pools (memory, processing, primary storage, and networking) when applicable.

Customer will be responsible for the following provisioning services:

- Creating user accounts and changing default system preferences as needed.
- Creating and configuring applicable VDCs, vApps, VMs, and networks using deployment templates and wizards.
- Creating and configuring the IPSEC tunnel on the customer premises firewall.
- Installing and configuring custom or third-party applications and operating systems on deployed VMs.

3.2 DATA RECOVERY

Synoptek will provide the following services with respect to data recovery of the Service Offering Platform ONLY:

- Data protection, such as routine backups, for the Service Offering infrastructure, including top-layer management and user-management interfaces owned and operated by us.
- Data and infrastructure restoration for the Service Offering infrastructure, including top-layer management and user-management interfaces owned and operated by us.

Customer will be responsible for the following services with respect to data recovery within the Service Offering:

- Data protection, such as routine backups, for the data and content accessed or stored on Customer VMs or storage devices, configuration settings, etc.
- Data, content, VM, and configuration restorations for assets accessed or stored.

See Data Protection Service 4.2 **(Optional Service – Additional charges apply)**

3.3 MONITORING

Synoptek will provide the following services with respect to monitoring:

- Monitoring the infrastructure, infrastructure networks, top-layer management and user-management interfaces, and computing, storage, and network hardware for availability, capacity, and performance. Synoptek will also provide the customer with a VDC- and VM-level view of compute and storage resource utilization and availability (upon request).
- See Appendix C Monitoring 0.0

Customer is responsible for the following services with respect to monitoring:

- Monitoring the assets deployed or managed within the account, including but not limited to VMs, operating systems, applications, specific network configurations, operating system or application vulnerabilities, etc.
- See Managed Services 4.4 **(Optional Service – Additional charges apply)**

3.4 INCIDENT AND PROBLEM MANAGEMENT

Synoptek will provide incident and problem management services (e.g., detection, severity classification, recording, escalation, and return to service) pertaining to:

- Infrastructure over which Synoptek has direct administrative and/or physical access and control, such as Synoptek owned Public Cloud Hosting servers, storage, and network devices.
- Service software over which Synoptek has direct administrative access and control and other applications that Synoptek uses in delivery of the Service Offerings.
- Synoptek provided operating system templates, to the extent that
    - Published templates cannot be accessed from the Service Catalog
    - Published templates cannot be instantiated without modification
    - Published templates cause errors at first run time
    - There are substantial hangs or excessive delays in the retrieval of a template from the Service Catalog
    - The configuration of a published template affects the VM’s interaction with the hypervisor
    - Time synchronization issues (NTP) exist
- Specific required hypervisor provided tools, including but not limited to
    - VMware Tools installation and configuration
    - Performance tuning as it relates to VMware tools and drivers

Customer is responsible for incident and problem management (e.g., detection, severity classification, recording, escalation, and return to service) pertaining to:

- User-deployed and user-configured assets such as VMs, custom developed or third-party applications, custom or user-deployed operating systems, network configuration settings, and user accounts.
- Operating system administration including the operating system itself or any features or components contained within it.
- Performance of user-deployed VMs, custom or third-party applications, customer databases, operating systems imported or customized by customer, or other assets deployed and administered by customer that are unrelated to the Service Offering platform.

3.5 CHANGE MANAGEMENT

Synoptek will provide the following change management elements:

- Processes and procedures to maintain the health and availability of the network, or the Service Offering platform.
- Processes and procedures to release new code versions, hot fixes, and service packs related to the network services, or the Service Offering platform.

Customer is responsible for:

- Management of changes to their VMs, operating systems, custom or third-party applications, databases, and administration of general network changes within the Customers control.

3.6 SECURITY

Responsibility for the end-to-end security of the Service Offering is shared between Synoptek and the Customer. Synoptek will provide security for the aspects of the Service Offerings over which Synoptek has sole physical, logical, and administrative level control. The Customer is responsible for the aspects of the Service Offerings over which the customer has administrative level access or control. The primary areas of responsibility as between Synoptek and the customer are set forth below.

Synoptek will use commercially reasonable efforts to provide:

- **Physical Security:** The Service Offering is housed in state of the art data center facilities. The following controls are in place at the physical layer in the data centers:
  - Equipment Location: The Service Offering operates in the United States. A site selection team determines each data center site. The site selection process includes a rigorous assessment, ensuring that each site has appropriate measures and countermeasures in place such as man traps, locking cages, staffed personnel and cameras.
  - Data Centers: Synoptek use well-established data center providers to host workloads. Each data center is certified. The providers are reviewed by independent third party auditors to meet the physical security requirements for, SOC 1 Type 2/SSAE 16 and SOC 2 Type 2. SOC2 reports outlining these specifications are available, upon request, subject to execution of an appropriate confidentiality and nondisclosure agreement.
- **Information Security:** Synoptek will protect the information systems used to deliver the Service Offerings for which Synoptek have sole administrative level control.
- **Network Security:** Synoptek will protect the networks containing our information systems up to the point where the Customer haves some control, permission, or access to modify the networks.
- **Security Monitoring:** Synoptek will monitor for security events involving the underlying infrastructure servers, storage, networks, and information systems used in the delivery of the Service Offerings over which Synoptek has sole administrative level control. This responsibility stops at any point where the customers has   some control, permission, or access to modify an aspect of the Service Offerings.
- **Antivirus / Malware:** Synoptek will leverage Anti-Virus and Anti-Malware protection at the hypervisor level. Synoptek manages daily virus definition updates and ensures all host based clients and local agents are managed from our centralized management platform and are working as expected.

Customers can be alerted to blocked files through the use of a low impact system tray application that runs within their virtual machine. If files are improperly blocked, Customers can request the files through our normal support process or retrieve with their local agent if present. All other operations of the protection are transparent to the Customer.

- **Patching and Vulnerability Management:** Synoptek will maintain the systems Synoptek use to deliver the Service Offerings, including the application of patches Synoptek deem critical for the target systems. Synoptek will perform routine vulnerability scans on a quarterly basis to surface critical risk areas for the systems Synoptek use to deliver the Service Offerings. Critical vulnerabilities will be addressed in a timely manner.

Customer is responsible for the following:

- **Information Security:** Customer is responsible for ensuring adequate protection of the information systems, data, content, or applications that customer deploys and/or access on the Service Offerings. This includes but is not limited to any level of patching, security fixes, data encryption, access controls, roles, and permissions granted to the Customers internal, external, or third party users, etc. Customer must also meet their own regulator controls.
- **Network Security:** Customer is responsible for the security of the networks over which the Customer has administrative level control. This includes but is not limited to maintaining effective firewall rules, exposing only communication ports that are necessary to conduct business, locking down promiscuous access, etc.
- **Security Monitoring:** Customer is responsible for the detection, classification, and remediation of all security events that are isolated within the Customers virtual instance(s), associated with VMs, operating systems, applications, data or content surfaced through vulnerability scanning tools, or required for a compliance or certification program in which the Customer is required to participate and which are not serviced under another Synoptek provided security program.

3.7 VIRTUAL SERVER DEPLOYMENT TEMPLATES

Synoptek will provide the Service Catalog (the “Catalog”) of supported virtual server deployment templates that the Customer may deploy into the Customers Service Offering environment. The deployment and use of such templates will be subject to the Third Party Terms within the Master Service Agreement and may be subject to additional Subscription Software fees. Synoptek will provide these templates, test them for quality, check for viruses, and install security patches before making them available in the Catalog. Synoptek will also maintain and update these templates from time to time. The customer is responsible for deploying and configuring the virtual server deployment templates that they choose to use, activating related licenses, and maintaining compliance with all applicable license terms.

In order to comply with our legal obligations to our third party licensors, the customer will not be permitted to export, download, or remove certain templates or any installed forms of certain templates for installation or use outside of the Service Offerings, as set forth in the Third Party Terms within the Master Service Agreement. The customer may implement or import their own virtual server deployment templates so long as the customer has the legal right to deploy and use the software contained in such templates.

Templates provided by Synoptek that are infrequently used, out of date, or no longer supported may be removed at any time.

3.8 STORAGE

The Service Offering includes persistent block storage as a part of the subscription. There is one storage option available; Blended Storage. The storage options allow for growth of virtual machine disks without downtime. At the time of purchase, the customer can specify additional storage which can be included with the Service Offering instance(s). After the time of purchase, the customer can purchase additional storage by submitting a ticket through the service desk.

3.9 NETWORKING AND FIREWALL SERVICES

The Service Offerings include the following network services as a part of the Service Offering:

- Network Address Translation (NAT): Separate controls for source and destination IP addresses, as well as port translation.
- Dynamic Host Configuration Protocol (DHCP): Configuration of IP pools, gateways, DNS servers, and search domains.
- Static Routing: Static routes for destination subnets or hosts.

See Appendix C for Fortigate Dedicated Virtual Firewall appliances (**Optional Service – Additional charges may apply**)

SSL VPN: SSL VPN enables remote users to connect securely to private networks behind the firewall. **(Optional Service – Additional charges may apply)**

ENHANCED LOAD BALANCING: SSL offloading and Application level load balancer. **(Optional Service – Additional charges apply)**

3.10 SELF-DIRECTED MIGRATION

PROFESSIONAL MIGRATION SERVICES: are not included but are available for the conversion of existing physical or virtual services. These capabilities support onboarding to Synoptek and export from Synoptek. **(Optional Service – Additional charges apply)**

3.11 MICROSOFT SPLA LICENSING AND SETUP (MANDATORY – ADDITONAL CHARGES APPLY)

Synoptek must provide Microsoft specific licensing's under the Microsoft SPLA rules and guidelines. All licensing must run within the walls of Synoptek datacenters. Synoptek can assist with the installation of Synoptek provided SPLA licensing though it's Move, Add, Change and Delete, Service Request process and/or Professional Services. If you have eligible license mobility software with Microsoft, Synoptek can accept those licenses so long as you maintain eligibility for license mobility.

4 OPTIONAL SERVICES

4.1 SEED LOADING SERVICE (ADDITIONAL CHARGES APPLY)

Seed Loading Service is an optional data copy service for the purpose of transferring large numbers of VMs or templates from your local environments to your Synoptek environment.
As part of this service, Synoptek will:

- Ship a physical storage device, permitting the customer to load VMs or templates onto the device and ship it back to Synoptek using the customers preferred carrier. The content that the customer load onto the device will be encrypted thereby ensuring security of your content during transfer.
- Transfer the data from the device into your instance.

Customer will be responsible for:

- Following the instructional documentation accompanying the storage device.
- Returning the storage device to us within 45 calendar days from date of shipment. If the storage device is not returned within the 45-day period, you will pay us a replacement fee for the storage device plus any shipping and handling charges, as assessed by us.

Backing up any data, applications, or VMs transmitted via the service; Synoptek will not be responsible for any data loss that may occur as a result your use of this service. This optional service may be subject to additional fees.

4.2 DATA PROTECTION SERVICE (ADDITIONAL CHARGES APPLY)

Data Protection Service is an optional service that provides secure, backup and recovery capabilities that enable the customer to protect important VM data and content hosted in their Service Offering environment beyond any inherent default data protection.
Data Protection Service may be ordered and is subject to additional fees based on the amount of VMs being backed up and retention required. For more information, see ***Service Description for Data Protection Service***

4.3 DISASTER RECOVERY (ADDITIONAL CHARGES APPLY)

Disaster Recovery is an optional service that provides secure recovery capabilities and resources into a different datacenter for full site recovery. For more information, see ***Service Description for Disaster Recovery***

4.4 MANAGED SERVICE (ADDITIONAL CHARGES APPLY)

Managed Synoptek IaaS - Synoptek will provide enhanced management of customer managed virtual servers including 24x7 monitoring, OS patch management, backup management, Anti-Virus, and OS troubleshooting within the Service Offering. Synoptek will also provide enhanced management of customer's virtual router, virtual switch and virtual firewall systems within the Service Offering Synoptek. Additionally Synoptek will provide monthly reports documenting critical alerts, scans, and event resolutions. Should a problem be discovered through our remote monitoring, Synoptek shall make every attempt to rectify the condition in conformance with the Service Level Agreement

APPENDIX A – SUPPORTED SERVICES

Synoptek 24x7x365 Service desk will work with your team to provide consulted and informed support around the following self-serve functions at a minimum as it relates to the Service Offering platform once transitioned to support. Additional Managed, Application and Professional Services are available optionally as stated in the Service Description.

Category	Supported
Virtual Data Centers	✓ Creating and Viewing a Virtual Data Center ✓ Managing Resource Allocation for a Virtual Data Center ✓ Managing Virtual Machines in a Virtual Data Center ✓ Locking and Unlocking a Virtual Data Center ✓ Setting a Limit on Number of Virtual Machines in a Virtual Data Center ✓ Changing Virtual Data Center Name or Description ✓ Deleting a Virtual Data Center
Gateways and Networks	✓ Creating and Viewing Gateways and Networks ✓ Modifying and Deleting Gateways and Networks
Basic Management	✓ Understanding Catalogs ✓ Adding a Virtual Machine from a Template ✓ Powering On a Virtual Machine ✓ Suspending a Virtual Machine ✓ Resetting a Virtual Machine ✓ Deleting a Virtual Machine ✓ Viewing and Editing Virtual Machine Details
Virtual Machine Monitoring	✓ Viewing a Virtual Machine's CPU and Memory Usage ✓ Viewing Virtual Machine CPU and Memory Usage History
Storage Management	✓ Adjusting Storage for a Virtual Data Center ✓ Adjusting Storage for a Virtual Machine
Snapshot Management	✓ Creating, Reverting and Deleting a Snapshot for a Virtual Machine
User Management	✓ Understanding User Privileges by Role ✓ Adding Users ✓ Assigning Users to a Virtual Data Center ✓ Understanding and Viewing Activity Logs ✓ Editing User Details ✓ Resetting Passwords ✓ Deleting Users

APPENDIX B – FEATURES

Hosts:

- Designed to have no single point of failure
- Fault Tolerant capable of suffering host fails
- Fully automated VM and Storage movement and redundant N+1 compute and storage capacity. Architected for resiliency and high availability. (Does not include disaster recovery capability)

Network:

- Multiple, redundant connections to Synoptek core network

Storage:

- Designed to have no single point of failure
- 10GB FCoE fabric
- Blended Storage consisting of SSD and Standard Disk

APPENDIX C – FIREWALL FEATURES and OPTIONS

Features	Included NSX Edge FW	Optional Virtual FortiGate FW
Port/Protocol Filtering – IP/TCP/UDP/ICMP	X	X
Tunnel Based IPSEC VPN	X	X
Rate Limiting / Bandwidth Shaping	X	X
Can be deployed in HA	X	X
Comes in different sizes for increased throughput	X	X
DHCP	X	X
NAT (DNAT/SNAT/PAT)	X	X
Customer self-management through web UI	X	
Policy Based IPSEC VPN		X

Load Balancing *		X
SSL VPN (including no per user charge) **		X
Network Access Control (NAC) – additional charges		X
Endpoint Control – additional charges		X
Included SSL VPN Agent		X
IPv6 Stateful Firewalling Support		X
Multicast Firewalling Support		X
Dynamic Policy Learning		X
Dynamic Routing (OSPF/BGP/RIP/RIPv2/MULTICAST)		X
Policy Routing		X
Dynamic Security Profiles integrated with AD groups		X
Session Helpers for SIP, FTP, TFTP, DNS, H.323, MGCP, etc.		X
Advanced Security Features:		
IDS/IPS		X
Anti-Malware		X
DOS (Denial of Service) Protection		X
Web Content Filtering – whitelists, block lists, content, user		X
Application Control		X

IP Reputation		**X**
DNS Filtering		**X**
DLP		**X**
WAF capability		**X**
Sandboxing option at an additional cost		**X**
SSL Payload Inspection		**X**

APPENDIX D – MONITORING

Synoptek monitors our data center environments using SNMP, syslog and other API based technologies. Comprehensive monitoring templates ensure that all aspects of the environment are monitored for performance, availability, and capacity. The following metrics are monitored:

Category	Datapoint
UCS hardware status monitoring	✓ Chassis ✓ Power Supplies ✓ IO Modules ✓ Blades Servers ✓ Fabric Interconnect ✓ Operational status ✓ Fault condition ✓ Physical Switch I/O operational and administrative status ✓ UCS chassis Management controller statistics ✓ CPU Statistics
UCS environmental status monitoring	✓ Power status ✓ UCS cooling fan type and condition ✓ Temperature statistics on all components ✓ Voltage status for each component
Storage Monitoring	✓ Disk, Memory Modules, Chassis Temperature ✓ Inventory – Storage Processors, Front end (FC, Gb) Ports, Back End (FC,SAS) Ports, Disk Drives ✓ Configuration Details – LUN details, Raid Groups, Host-Port Mappings ✓ Availability – SP Status, SP Port Status, FC/Gb/SAS Ports Status, Disk Drive Status, LUN Status and Raid Group Status ✓ Performance – Array, Device Drive, LUN, Storage Pool and Storage Volume Statistics
Virtual environment monitoring	✓ Server availability

Legal Notice: *The information transmitted in this document is intended only for the addressee and may contain confidential and/or privileged material. Any interception, review, retransmission, dissemination, or other use of, or taking of any action upon this information by persons or entities other than the intended recipient is prohibited by law and may subject them to criminal or civil liability.*

	✓ Server performance (**CPU**: Clock Speed, CPU utilization **Memory**: Free, Total and Used Memory **Disk**: Free, Used, Total and Virtual Allocation) ✓ Network Interface – Total Bytes/sec ✓ Network Interface – packets Outbound errors ✓ VMware Hypervisor Host Storage: Storage Type, Availability Storage size, used size and free size

APPENDIX E – REPORTS

Reports	Description	Upon Request
VM Inventory Reports	Device details Report	X
	Disk space Report	X
	Virtual Hardware Report	X
	Software Report	X
	Virtualization Performance Report	X
Network Reports	Interface errors and discards	X
	Interface utilization and traffic	X
Firewall	Bandwidth Report	X
	Basic Security Report	X
	Detailed Application Usage Report	X
	Threat Report	X
	User Report	X
	Web Usage Report	X
Security Reports	Hypervisor based Anti-Malware status report	X
	Hypervisor based Anti-Virus status report	X
	Log Inspection Report (HIPAA Only- Agent)	X
	Log Inspection Detailed Report (HIPAA Only - Agent)	X