Synoptek®

ITaaS Server

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 ITaaS Server (the "Service").
The service definitions found herein reflect Synoptek standards at the time the Service Order(s) was issued. Synoptek reserves the right to change any particular standard herein to reflect Synoptek's best practices or industry standards at its sole discretion with or without notice.

2 SERVICE OFFERINGS

This service provides the Customer with management of a physical or virtual server in either a customer premise, or a cloud environment. The service ensures high levels of Server reliability, uptime and performance through constant monitoring, troubleshooting, timely maintenance, and proactive administration tasks. The service includes 24X7 IT admin and technical support. This service also provides for proactive monitoring, OS patch management, anti-virus and optional backup management. By request, Synoptek will deliver monthly reports documenting critical alerts, scans, and event resolutions. Should a problem be discovered through our 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 service requests, resolution to incidents, and problem management to customer technical contacts and authorized technical team members relative to subscribed tools and services.	Yes
ASSET TRACKING	Synoptek configuration management tools are used to track basic server information such as: Servers, CPU, installed RAM, HDD size, installed OS and SP level, etc. This information is useful for IT managers to make decisions relative to hardware procurement and replacement. Synoptek will track asset information depending on the Synoptek Managed Services being provided, but may include: • General Service Summary • Servers by location • Server Details • Server Patch Status • Virus Software Version Status • Spyware Software Version Status If the Customer creates new Virtual Machines or installs new Hardware for Synoptek to manage, they must notify Synoptek in order to have the correct tools installed on their servers. Synoptek has the right to audit a customer's environment and adjust billing to current volumes.	Yes

PRIVATE NETWORK SETUP (FOR CLOUD HOSTING SERVERS ONLY)	Synoptek will handle setup of all cloud private networks including NAT of public IP to private IP where needed within the local cloud LAN. Connection to remote Customer networks or MPLS based connections are outside of the scope of this Service~~.~~	Yes
DNS AND IP ADDRESSING/MANAGEMENT	Synoptek will assist Customer with making any required internal (local) DNS record changes, as well as IP addressing needed for Synoptek to provide Service monitoring and management support.	Yes
SERVER REBOOTS	Synoptek will perform unlimited reboots per month. If Synoptek determines there is a fundamental server issue that is outside Synoptek's scope of remediation, Synoptek may limit the number of reboots performed until a mutually agreed to resolution can occur.	Yes
SERVER REBUILDS	In the case of system failure, and at customer request, Synoptek will rebuild the Managed Servers using current version of OS. In the event Synoptek is required to rebuild a Server after the initial build, this will remove any existing data and may remove the backup data. Customer may request only a single rebuild after the initial setup of a physical or virtual machine. Additional rebuilds would incur additional costs. If Synoptek is not responsible for Server backup, Customer is responsible for restoring any and all data to the Server, unless otherwise stated in the contract Statement of Work (SoW) for Professional Services. Customer will be responsible for any third party software installations and required configurations unless otherwise stated in the contract and/or SoW for Professional Services. All requests for new Server Builds after Service installation, require a change order. For Server Rebuilds on Customer Server Hardware, Synoptek requires remote access and administrative credentials for Server, including hypervisor access. Customer must provide OS licensing and all required media. There are two (2) options for rebuilding Servers on Customer Server Hardware: 1. Customer boots to OS media. Synoptek walks the Customer through the initial installation. Customer confirms/configures IP information. Customer provides Synoptek IP address and credentials to OS. Synoptek will complete the Server build. 2. Customer provides Synoptek the remote access card IP information. Remote access must include licensing to access the Server console. Customer provides OS media. Synoptek will complete the Server build.	Yes
MONITOR, ALERTING AND REMEDIATION	Synoptek provides proactive monitoring of Synoptek Supported Server Systems and Software. Synoptek will provide Customers with notification of alarms and/or events according to pre-defined usage thresholds assigned to each Component being monitored. Available	Yes

	parameters, thresholds and alerts vary based on the Servers being monitored. Synoptek will monitor Managed Server Disk, CPU and Memory to default thresholds at Synoptek pre-defined intervals. Should a threshold be exceeded, Synoptek will act to remediate. This could include contacting Customer if assistance is needed in order to determine how to resolve. Resolution could include the purchase of additional virtual resources if necessary. 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 than 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. If needed, Synoptek provides Advanced Monitoring of Server, including Operating System, on Customer Server Hardware located at customer premise locations. Synoptek provides automatic notification of alarms on monitored components according to pre-defined usage threshold. Customer must provide Synoptek any required IP addresses and credentials for system access needed to perform monitoring. For Synoptek Public Cloud customers, Synoptek can monitor up to 5 Windows Services (for example IIS) and Customer can specify the action to take on a down alert (i.e. Alert Customer or, Auto-restart). Additional services can be monitored at an additional cost. For Synoptek Public Cloud customers, Synoptek will monitor up to 10 custom ports on the Managed Server for a positive ping result to ensure custom services are actively running. If Server fails to respond with in the predefined thresholds, Synoptek will automatically send an alert notification to Customer provided email addresses. If the Customer creates new Virtual Machines or installs new Hardware for Synoptek to manage, they must notify Synoptek in order to have the correct monitoring probes setup and configured to deliver the advanced monitoring features. If the Customer makes modifications to their Servers, including deleting a VM, it is important that they alert Synoptek so that monitoring setup can be reviewed to make changes as needed. Especially for deleted VM's as this would require removal of monitoring configurations to avoid potential false positives.	
WINDOWS OS PATCH MANAGEMENT	Synoptek will apply any "Critical" or "Security" updates with a priority level of "Important" and higher for Windows operating system patches and OS Hot Fixes.	Yes

Synoptek provides patching support for stable and supported Microsoft Windows versions within 90 days of General Availability ("GA") release.

Synoptek will engage "best efforts" support for versions that have exceeded the "End of extended support" date, but makes no guarantees of success with best efforts activities.

Synoptek will provide Customer with a choice of patching process during on-boarding:

1. Synoptek's managed patching process for production Windows systems through a designated patching window.
2. Tailored patching schedule contingent upon agreement between Synoptek operations team and Customer.
3. Opt-out to not have Synoptek apply patches on specified subset of servers. By choosing this, customer agrees to take on additional risk associated with security vulnerabilities and functional problems associated with critical bugs.

Only critical and security patches are applied, non-core and/or patches that are not critical security updates are not applied. Customer may choose to skip a monthly window if they provide at least 3 days' notice to Synoptek via email. Synoptek does not apply service packs during this process, but can apply those if requested, through a separate manual process and may incur additional charges.

In the event of an issue with a Managed Server, immediately following and as a suspected result of patching, Synoptek will respond as follows:

1. If the Server does not come back online after the Server reboot, then the EOC will notify the Customer and contact a Synoptek Server Engineer to troubleshoot the issue.
2. The EOC will be notified in the event of a service failure after the reboot. The EOC will contact a Server engineer to troubleshoot any core service failures and will escalate to the Customer in the event of an application service issue. In the event of a core OS service outage the Customer will be notified of the issue and notified again after resolution.
3. Synoptek can rollback patches if required. The Customer will be notified in the event that Synoptek must rollback a patch due to a core OS issue.
4. The Customer may submit a ticket to rollback a patch if required to resolve an application issue.

	There are times when a Software Vendor releases a critical patch to address a vulnerability that represents an immediate threat to our Customer's Servers and/or data. Synoptek will notify the Customer of our intention to perform Emergency Patching of all Automatic approved Servers as far as in advance as possible. The Customer will have the option to respond to the notification to stop the Emergency Patching of these Servers otherwise the patching will proceed as scheduled. Customers that manually approve patching will receive notification of the Emergency Patching release along with details of the vulnerability. The notification will also recommend the creation of a ticket to have affected Servers patched immediately.	
LINUX OS PATCH MANAGEMENT	Synoptek will apply "Linux Critical" and "Security Errata" operating system patches and OS Hot Fixes. Synoptek provides patching support for stable and supported Red Hat Enterprise Linux, SuSE Linux Enterprise Server, Ubuntu LTS, CentOS versions within 90 days of General Availability ("GA") release. Synoptek provides best effort support for versions exceeding End of Service Life (EOSL) or equivalent end of patch support by the vendors. Synoptek provides best effort for Linux operating systems not described above. Synoptek will provide Customer with a choice of patching process during on-boarding: 1. Synoptek's managed patching process for production Linux systems through a designated patching window. 2. Tailored patching schedule contingent upon agreement between Synoptek operations team and Customer. 3. Opt-out to not have Synoptek apply patches on specified subset of servers. By choosing this, customer agrees to take on additional risk associated with security vulnerabilities and functional problems associated with critical bugs. Only critical and security patches are applied, non-core and/or patches that are not critical security updates are not applied. Customer may choose to skip a quarterly window if they provide at least 3 days' notice to Synoptek via email. Synoptek does not apply service packs during this process, but can apply those if requested, through a separate manual process and may incur additional charges.	

	Customer must provide Synoptek with local administrative rights on Managed Servers and ensure that all physical Managed Servers and devices are covered under warranty. In the event of an issue with a Managed Server, immediately following and as a suspected result of patching, Synoptek will respond as follows: 1. If the Server does not come back online after the Server reboot, then the EOC will notify the Customer and contact a Synoptek Server Engineer to troubleshoot the issue. 2. The EOC will be notified in the event of a service failure after the reboot. The EOC will contact a Server engineer to troubleshoot any core service failures and will escalate to the Customer in the event of an application service issue. In the event of a core OS service outage the Customer will be notified of the issue and notified again after resolution. 3. Synoptek can rollback patches if required. The Customer will be notified in the event that Synoptek must rollback a patch due to a core OS issue. 4. The Customer may submit a ticket to rollback a patch if required to resolve an application issue. There are times when a Software Vendor releases a critical patch to address a vulnerability that represents an immediate threat to our Customer's Servers and/or data. Synoptek will notify the Customer of our intention to perform Emergency Patching of all Automatic approved Servers as far as in advance as possible. The Customer will have the option to respond to the notification to stop the Emergency Patching of these Servers otherwise the patching will proceed as scheduled. Customers that manually approve patching will receive notification of the Emergency Patching release along with details of the vulnerability. The notification will also recommend the creation of a ticket to have affected Servers patched immediately.	
STORAGE AREA NETWORK (SAN) MANAGEMENT	Synoptek will monitor SAN health and facilitate the operability of Client SANs and utilize the client's vendor support contracts as required. Basic SAN management includes provisioning and expansion of LUNs. This service includes the maintenance of replacing failed drives, opening vendor cases to resolve issues, migrating applications or virtual devices hosted on the storage, updating the firmware, software, or OS code. Storage monitoring is provided to perform a proactive view into performance and capacity. This monitoring is done to provide predictive availability and will be managed by the following standard levels:	Yes

	• Hardware (controllers, service processors, disks, etc.…) and various levels of performance. • Overall array capacity. • RAID groups or storage pools and their capacity. • LUN and its capacity and performance.	
ENDPOINT PROTECTION	Synoptek will provision managed devices with Anti-Virus and Anti-Malware. Synoptek manages daily virus signature updates and managed to our centralized management platform for control and visibility. Should a virus be detected, Customers will be notified. Synoptek will provide assistance in containment and eradication of malware using the appropriate tools and methods necessary. In some circumstances removal of malware may not be possible and Disaster Recovery may be the recommended path to restore availability ASAP. Malware remediation services will incur additional cost for ITaaS standard subscribers.	Yes
ENDPOINT DETECTION AND RESPONSE (EDR)	Synoptek will provision managed servers with the ability to continuously detect suspicious activity and automatically respond to active threats through a combination of advance threat prevention capabilities: • Simulates the presence of sandbox and analysis tools that are considered “hostile” for malware. • Intercepts attempts to inject malicious code into memory for protection against file-less threats • Terminates weaponized files such as VBA scripts, Excel Macros, and Powershell scripts. • Simulates artifacts of infected devices to deceive the malware to think it’s already infected the system.	Yes
CHANGE MANAGEMENT	Synoptek will provide change management as it relates to the following: • Processes and procedures to maintain the health and availability of the Monitoring Appliance, or the Service Offering platform. • Processes and procedures to release new code versions, hot fixes, and service packs related to the Monitoring Appliance, or the Service Offering platform. Customer will provide change management as it relates to changes to custom or third-party applications, databases, and administration of general network changes within customer control.	Yes

BACKUP MANAGEMENT	Included in ITaaS Server, Synoptek will provide management of a customer's existing backup system to ensure the server is operating and performing the backups per the scheduled back-up times. If a customer doesn't have an existing backup system, customer may choose to purchase one from Synoptek. By default, Synoptek will schedule daily backups with a 14-day retention unless other requirements are specified. NOTE: Because files may be open at the time of the scheduled backup operation, and machines may be inaccessible, some backups may not succeed. Synoptek, will provide up to 3 restores per month from the customer backup servers. Beyond 3 restores, restoration is considered a billable activity. In addition, if the time to perform a restore is over 4 hours, Synoptek may make this a billable activity, with customer approval. This service does not include physical tape rotations or the relocation to an off-site facility. Additional services may be provided under other service line items identified in the service agreement.	Yes
MONITOR AND MANAGE - 3RD PARTY SOFTWARE AND APPLICATIONS (INCLUDES INSTALL AND PATCHING)	Application patches includes services such as SQL, IIS, Exchange and .Net. Customers may request non-critical patching of applications at any time (additional charges may apply). The testing and approval of application patches remains the responsibility of the Customer. Synoptek recommends that the Customer have a testing environment for critical application services. Synoptek will work with the Customer to apply patches to test Servers to validate application issues that might occur as a result of patching. This allow Synoptek to work with the Customer to keep their Servers up to date with as little affect to their Servers as possible. Customers must maintain 3rd party Application support.	Optional Service – Additional Charges Apply

2.2 PREMIUM COMPONENTS

FEATURE AND DESCRIPTION:	ADDITIONAL INFO:	INCLUDED
VULNERABILITY MANAGEMENT	Synoptek will deploy a scanning agent to subscribed devices that shall, upon scheduled initiation, perform a full vulnerability scan on subscribed device to identify weaknesses inherent in the software or operating system on subscribed device. Client shall receive a quarterly report of vulnerabilities found. Synoptek will work with client to ensure that found vulnerabilities are categorized by risk ranking and that vulnerabilities are remediated within the patch management and change management schedule as appropriate.	Premium

2.3 MAX COMPONENTS

FEATURE AND DESCRIPTION:	ADDITIONAL INFO:	INCLUDED
SIEM AS A SERVICE	Synoptek's Security Information and Event Management services, or SIEM-as-a-Service, is designed to provide organizations all the benefits needed from a security information and event management system without any of the headache or capital investment. The offering is a comprehensive SIEM-as-a Service solution, fully hosted in a secure and compliant cloud to manage and monitor your critical systems regardless of where they may be. A daily review of cyber security events is also provided by Security Analysts and a report is delivered to Customers. See Formal SIEMaaS Service Definition for addition detail.	MAX
ADVANCED ENDPOINT DETECTION AND RESPONSE (EDR)	Synoptek will provision managed devices with additional advance threat prevention capabilities to augment the base standard EDR capabilities: • Cloak sensitive files from malware, even in the event of an infection. • Intercept attempts of ransomware to encrypt files and place them in a secure cache hidden from malware, allowing recovery of files after ransomware has been mitigated.	MAX
MALWARE REMOVAL AND SERVER RECOVERY	In the event that malware is identified, Synoptek will remove the malware's presence from the afflicted device. In the event that the malware cannot be removed, or a ransomware incident, Synoptek will either restore files or re-image the device to the best available known-good-state from backups/snapshots. Recovery from malware or ransomware that cannot be performed by these means is out of scope. All other post-breach services such as root-cause analysis, forensics, support for insurance and law enforcement and extraordinarily time consuming, and therefore only available at an extra labor cost. Recovery from backup can span several days. In the event that ransom is requested from perpetrators, Client may initiate payment at Client's sole cost.	MAX

3 SUPPORT

The service and support operate 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 on-boarding (set up), server off-boarding (decommission), and enterprise server configuration changes unless otherwise noted in this service definition); 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 (Suppport@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.

- Synoptek support for operating systems includes the most recent two major versions of Windows Server OS, Windows Desktop OS, Mac OS, and most common Linux OSes. Support of some Linux OSes may require that the customer maintain an active subscription. Not all operating systems fully support Synoptek's standard Anti-Virus and Anti-Evasion platforms.

- 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).

Customer acknowledges and agrees that Synoptek may directly or remotely communicate with the agents we install on Customer's Devices for purposes related to the security and management, including, (i) verifying Credentials; (ii) issuing reports and alerts such as automated support requests and alert messages; (iii) providing support and maintenance services; (iv) applying policy and configuration changes; and (v) extracting usage information, service performance information and event logs.

3.2 SYNOPTEK RESPONSIBILITIES

- For Servers managed within Synoptek Cloud, 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 servers as described in this service definition, including:
  - 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
- Synoptek will install and configure the server monitoring appliance to report on the standard "monitored metrics"
- In conjunction with the Customer, Synoptek will establish an Escalation Plan for each class of alert.
- Synoptek will configure alert thresholds for all monitored metrics using standard Synoptek-specified thresholds.
- Synoptek will verify that all monitored metrics are being collected from the server by Synoptek's monitoring system.
- Synoptek will verify remote access to the Server by Synoptek.
- Synoptek will verify with the Customer and the manufacturer of the supported System that the Synoptek Service Desk has been added as an authorized service contact to the customer's support agreement for the supported device. (Note: this applies if Synoptek is responsible for escalating hardware events to manufacturer of the supported System for resolution).
- Synoptek will configure reports for all "monitored metrics" as listed above upon customer request
- Synoptek will install the Patch Management client software on the physical or virtual servers covered by the Patch Management service, if not already present
- Synoptek will configure the centralized patch management system to include the covered servers.

3.3 CUSTOMER RESPONSIBLITIES

- For premise based, physical servers, the supported servers must remain covered by an active manufacturer on-site support agreement, be under warranty, and have Synoptek listed as an authorized service contact with the manufacturer.

- The Customer must give Synoptek administrative-level login usernames and passwords for the managed servers and must not disable or remove these accounts, or otherwise hinder Synoptek's access to managed System.

- This Service does not include on-site response by Synoptek staff for problem resolution. All troubleshooting and problem resolution are done by Synoptek staff working remotely in conjunction with Customer staff and/or vendor staff where on-site tasks are required.

- For physical servers running a virtualization hypervisor (e.g. VMware ESX or ESX/I or Hyper-V), this service only includes monitoring and remediation of the host hypervisor and does not include monitoring and remediation for individual guest virtual machines. Unless this Service Order includes monitoring services for the individual guest VMs, it is the Customer's responsibility to monitor and manage any guest virtual machines running on this server.

  Customer-installed software: The Customer is responsible for the installation, configuration and ongoing management of any application or system software on the managed System.
- The Customer is responsible for backup of any and all data and programs stored on the System unless optional remote backup services have been purchased for the System.
- The Customer is responsible to work with Synoptek to establish pre-approved maintenance windows for application of OS patches according to the patch frequency.
- Following the application of OS patches in a maintenance window, the Customer is responsible to verify the proper operation of all hosted applications.
- The Customer is responsible for the ongoing management of user accounts for the System and for all database, application and other software.
- The Customer must not perform any action on the System which would interfere with Synoptek's ability to monitor or manage the Server including, but not limited to the following actions:
  - Disabling or changing any user or service login accounts used by Synoptek for monitoring or managing the System
  - Removing or changing any monitoring agent software settings
  - Adding deleting or changing any IP addresses associated with the System
  - Changing the Host Name of the System
- The Customer is responsible to notify the Service Desk (Support@Synoptek.com) when shutting down or rebooting the System, or when performing any other activity which would result in an "outage" as seen from the monitoring system.
- 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.

4 OPTIONAL SERVICES

4.1 DATA PROTECTION - BACK UP

See: Backup Service Definition.

4.2 DATA PROTECTION – REPLICATION (OPTIONAL)

Computers on the Data Protection (Replication) service are replicated daily, gaining the ability to restore either individual files or entire systems from a secondary location. Individual files can be restored in minutes, while an entire system is dependent on a Disaster Recovery Plan and scope of service.

4.3 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.

5 APPENDIX

5.1 Comparison Chart: ITaaS Server Bundles

ITaaS Server	Standard	Premium	MAX
Server Support			
24x7 Server Monitoring	X	X	X
24x7 Alerting & Remediation	X	X	X
Server Reboots and Rebuilds	X	X	X
Server Management			
Change Management	X	X	X
Patch Management	X	X	X
Asset Tracking	X	X	X
DNS and IP Management	X	X	X
SAN Management	X	X	X

Backup Management	X	X	X
Server Security			
Anti-Virus	X	X	X
Endpoint Detection and Response	X	X	X
Vulnerability Management		X	X
Advanced Endpoint Detection and Response			X
Malware Removal and Server Recovery			X
SIEM as a Service			X