Synoptek { ITaaS User

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 User (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 FOR DEDICATED USERS

Synoptek's ITaaS User Service combines a robust, reliable IT infrastructure, proactive management capabilities and automated processes, all working seamlessly in the background, to keep your end-users on PCs and Macs productive, protected and satisfied. Backed with a 24x7x365 Help Desk.

The service includes Asset Management, Anti-Virus, Patch Management, as well as a 24x7x365 Help Desk to offer support to end users. Synoptek will transition customers to preferred vendors and technology platforms. A complete list of the included components is included in the Core Components table below.

Upon signing of a Service Order, Synoptek and customer may choose to have Synoptek take over immediate control of customer's IT operations, including management of customer's technology. During this transition phase, and before Synoptek can transition services to preferred technology platforms, Synoptek's service levels will be best effort.

This service is priced per user and unless otherwise specified, includes up to 3 devices per user. Additional devices beyond 3, may be charged an additional fee. A user is defined by the following: any end-user consuming any of Synoptek's services.

2.1 CORE COMPONENTS

FEATURE AND DESCRIPTION:	ADDITIONAL INFO:	INCLUDED
24X7 STAFFED ADMIN/IT HELP DESK W/ CASE TRACKING & REPORTING	Synoptek provides 24x7 support to Customer technical contacts and authorized technical team members relative to subscribed tools and services.	Yes
24X7 STAFFED END USER HELP DESK W/ CASE TRACKING & REPORTING	Synoptek's help desk team is available 24x7x365 to support end users across all technology and service platforms as both a first point of contact, and resolution help desk.	Yes

VENDOR ESCALATION MANAGEMENT	Synoptek will escalate incidents to customer's vendor and maintain ownership of the incident until resolution. This requires working with customer to establish a vendor escalation list. It may also require Synoptek to be listed as the contact of record for certain vendors	Yes
REMOTE CONTROL	Synoptek will provide a way to "Remote In" to an end user's machine to assist in troubleshooting.	Yes
ASSET TRACKING	System hardware and OS versions are tracked throughout customer's environment, with reporting available.	Yes
INCIDENT MANAGEMENT	The Synoptek Support Team will track, manage and resolve any incidents arising from or related to Endpoint Security and Management Tool or Service.	Yes
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 prevent suspicious and malicious activity 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. After a threat is prevented, it is considered detected, then subsequently analyzed for further response (if necessary). Any response needed will be recommended or advised to the Customer	Yes

PATCH MANAGEMENT (WINDOWS USER ONLY)	Microsoft Critical Security patches are tested and automatically distributed to customer's user community with no disruption to customer's service. Synoptek does not release any patch until it has passed quality assurance testing. Critical patches are fully tested and released within the scheduled time. *Note: Full Windows OS upgrades as well as Windows 10 feature updates are excluded from patch management.*	Yes
SOFTWARE DISTRIBUTION	Synoptek can distribute software to Endpoints. This software includes Synoptek's management tools as well as well as 3rd party applications required by our customers. Requests can be made to package (as required) and distribute on demand. Packaging of the software is done on a Professional Services basis, but deployment is included in the monthly service. *Note: For macOS customers there are additional steps to Mac software distribution, including on-premise authorization.*	Yes
NEW EMPLOYEE PROVISIONING / REIMAGING	Synoptek will assist with procurement of new employee computer equipment through Synoptek' procurement group. Synoptek will arrange delivery of new desktops/laptops, less any shipping costs. (Cost of equipment is an additional charge). Synoptek will develop a standard employee desktop aligned to customer's personas (up to three) that will include standard applications. All Provisioning activities are handled remotely. If onsite presence is needed, Synoptek may include an additional charge. If more than 25% of machines are refreshed or provisioned every year and the time to process these machines takes over 2 hours per machine, Synoptek may include an additional charge.	Yes

EMAIL AND ACTIVE DIRECTORY PROVISIONING	On-premise Exchange Server and Active Directory Server Administration are intended to ensure the continued health of these services and perform routine administration services. The following provides a detailed list of what is included and excluded:
	• Add/Delete Users and Service Accounts
	• Create/Edit of Active Directory Group Policies
	• Password resets
	• Modify basic data on Active Directory Users, and (re)assign to Security Groups
	• Manage Exchange Server (or equivalent) mailbox quotas as requested by management
	• Add/Edit/Delete:
	  • User and resource Exchange mailboxes
	  • Exchange distribution groups
	  • Mailbox aliases
	• Direct support of end-users for all related. An example of end-user support is connecting one's Outlook or mobile device to Exchange.
		Yes

	Excluded: • Custom management of the Exchange Global Address List • Migration of users or email from other Network Operating Systems (e.g. Novell, Windows, IOS) • Consolidation of systems because of company acquisitions Additional Exchange Management and Active Directory Management is available as an additional charge.	
EMAIL SECURITY	Synoptek will manage a filter profile of subscribed users' email inbox from email-borne viruses as well as SPAM. A user-manageable antispam portal enables users to managed white-lists and block-lists as well as retrieve filtered email. Synoptek will support a customer's email security solution during a transition period, but for long-term support, Synoptek requires usage of Synoptek's vendor solution.	Yes
SELF SERVICE PASSWORD RESET	Synoptek will enable subscribed end users with the ability to reset their user passwords for a supported Directory Service (such as ActiveDirectory) via a customizable online portal. During onboarding, IT admins will be able to select the following supported factors for end users to authenticate themselves: • OTP Authenticators such as OneLogin Protect, Google Authenticator, Microsoft Authenticator • Soft and Hard Tokens such as YubiKey Supported factors are tailorable per user but require additional one time setup fee. Consult with your security department for guidance which factors are allowed under your security policy. SMS, Email, Voice are not supported factors.	Yes
ADVANCED MAC ADMINISTRATION	Synoptek can provide device management for macOS environments. These services include Synoptek setting policies for macOS, as well as providing macOS reporting to the Customer. Further details provided in Section 5.1. (Minimum quantity of 50 users).	Optional Service – Additional Charges Apply
CUSTOMER TICKETING SYSTEM	Synoptek can provide a ticketing system and processes for customers and Synoptek to share and collaborate on tickets.	Optional Service – Additional Charges Apply

DESIGNATED CONSULTING ENGINEER	For customer Application management, Synoptek offers Designated Consulting Engineers. These resources will work remotely and are scheduled in advance for a set number of hours per month.	Optional Service – Additional Charges Apply
ONSITE ENGINEER	If you would like to have someone on site at your location, Synoptek offers that through our Onsite Engineer. These resources are scheduled in advance for a set number of hours per month.	Optional Service – Additional Charges Apply

2.2 MAX COMPONENTS

FEATURE AND DESCRIPTION:	ADDITIONAL INFO:	INCLUDED
SECURITY TESTING AND TRAINING	Synoptek will enroll the Customer's workforce into an online, on-demand, interactive training program to educate on security best practices. Synoptek will also provide a comprehensive anti-phishing program to minimize the organization's vulnerability to phishing. This program entails: • Baseline Testing: Synoptek will deploy an initial phish campaign to establish a baseline of phish-prone users. • Ongoing Phishing Tests: Users will receive ongoing phishing security tests, scaling in difficulty, to keep users sharp and up-to-date on latest threats. • Enterprise-strength Reporting: Synoptek will provide reporting showing statistics and data on phishing failures and training status.	MAX
ADVANCED ENDPOINT DETECTION AND RESPONSE	Synoptek will provision managed devices with additional advance threat prevention 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
WEB CONTENT FILTERING	Web Content Filtering allows the enablement and enforcement of web browsing policies in support of internet usage policies. The system is Active Directory integrated and allows for policy management via AD group membership.	MAX

MALWARE REMOVAL AND DATA 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

2.3 SHARED COMPONENTS

FEATURE AND DESCRIPTION:	ADDITIONAL INFO:	INCLUDED
ITAAS USER FOR SHARED WORKSTATIONS	Synoptek's ItaaS User for Shared Workstations is a user services only version of ItaaS User Standard. While there is no device support offered in this variation, this service can be complemented with Synoptek's ItaaS User offerings as detailed in this document. This variation of ItaaS User is priced per user with zero device coverage unless otherwise specified. This service offers reactive support for users who employ work through shared workstations (devices) and includes support for end users (email security, password assistance, and 3rd party vendor governance for simple apps/services such as timesheets/timecards). This service includes the following aspects of ItaaS User Standard: • 24x7 Staffed End User Help Desk w/ Case Tracking & Reporting • Vendor Escalation Management • Email and Active Directory Provisioning • Email Security And adds the following aspect: • Password Reset Synoptek will reset end user passwords on a reactive basis. Only passwords for end user credential will be serviced; workstation admin (local and global) credentials will not be serviced and should be serviced through our ItaaS – User Standard/Max services.	Yes

3 SERVICE DEPLOYMENT

Synoptek's Service Deployment team is responsible for the onboarding and offboarding of ItaaS services.

3.1 EXPECTATIONS DURING ONBOARDING

3.1.1 Synoptek Requirements:

- For dedicated workstations:
  - Domain Environments
    - A staging point for package deployment – a server on this domain upon which Synoptek engineers can install RMM tools used for pushing out RMM packages.
    - Domain Administrator Credentials for a remote push of the Remote Monitoring and Management (RMM) Windows client.
  - Non-Domain Environments
    - Machines not on a domain will require a common local admin credential (same username and password) for all workstations in order to attempt a remote push of the Remote Monitoring and Management (RMM) Windows Client.
    - If a remote push is not possible or where not successful, end users of non-domain workstations will be required to install the RMM Windows client provide by the Synoptek Service Deployment team OR customer can provide access to an onsite resource that can help install RMM locally.
      - NOTE: There is no remote install capability of the RMM Client for Mac systems due to Mac security. Installs will require local/user-based efforts mentioned above.
- For shared workstations:
  - Synoptek will provide email security services as part of the ItaaS – User Standard/Max deployment which in most cases will be deployed in additional to ItaaS – User Shared. Email security is configured for the entire company at the same time, so no additional actions are required for this service.
  - Customer will provide contact information for each user utilizing this service which will be added to Synoptek's ticketing system.

3.1.2 Other Requirements:

- For dedicated workstations:
  - Previous management/security tools removed where possible (i.e. RMM tools, Anti-virus, anti-malware, etc.).
    - If a 3rd-party entity (i.e. outgoing MSP or separate corporate division) is in control of previous management/security tool management, that party is responsible for removing the tools from end user devices unless they provide Synoptek with the appropriate access or removal tools/passwords.
    - If the customer or vendor is unable to remove previous tools, then scripting and testing of removal tasks will need to be coordinated between Synoptek Deployment Engineers and the customer's project contact.
    - If central management consoles are used for previous management/security tools, Synoptek will need credentials and access to those management consoles.
  - Access to all software licensing portals and SaaS services (or a designated resource that handles these requests for the users)

- Customer should make all users aware that Synoptek tools are not optional, and not negotiable on a per-user basis, and that they must make their machines available to minimal interruption.
- End User workstations should have operating systems that are supported by the OS vendor (i.e. Windows 7+, MacOS 10.11+, etc.…).
    - *Microsoft only supports Windows 10 operating systems within the last 3 feature updates.*
    - *There is an additional system requirement for the Advanced Mac Administration Add-On Service.*
        - *To eligible for the encryption component of the service, the systems require a recovery partition and macOS version 10.13.1 or higher.*
        - *Synoptek can assist with these pre-requisites as a separate project for an additional cost.*
- Workstations should have at least 1GB of free/unused memory available for Synoptek tools; this usually means an end user device should have at least a total of 4GB of memory but could require more if a user is a power user consuming larger amounts of memory.
- Customer will provide within 7 days of kickoff a testing group of users spread across the enterprise for User Acceptance Testing (UAT) that will serve to identify problems with Synoptek tools before they are pushed the rest of the enterprise.
- Customer will provide within 7 days of kickoff domain access to all in-scope active-directory domains and priority access to existing IT knowledgeable staff to ensure a quick and seamless transition.

- For shared workstations:
    - Access to all customer-owned/provided software licensing portals and SaaS services that are in scope for end user support will be required.

3.1.3 Synoptek Deliverables:

- Applicable to dedicated workstations only:
    - Deployment of the RMM client (where supported)
    - UAT testing of the ItaaS Management tools on a cross-department selection of user systems
    - Mitigation of any issues found during UAT
    - Deployment of ItaaS management tools to the remaining systems – upon customer UAT testing sign off.
    - Initialization of Windows workstation patching
    - Updating of Synoptek Customer support information

4 SERVICE SUPPORT

The Synoptek help desk operates 24x7x365 and will act as the single point-of-contact for all IT-related issues, including those that are outside of the scope as defined. 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. Synoptek's Global Shared Help Desk will be staffed by our industry standard level 2 specialists. Incidents may be reported by phone via toll-free 800 number, through free format email or by forms submitted via email. Also included is the online portal and remote-control tool. A customer satisfaction measurement will be included for all closed cases regardless of who ultimately handled the case.

If Synoptek cannot solve the issue remotely, Synoptek may choose at its sole discretion to send someone onsite to a customer's location. Synoptek can dispatch someone to a customer site at an hourly rate. If the Customer wants someone onsite on a regular basis, Synoptek offers an Onsite Engineer Service.

- Exclusions: Unsupported Incidents. These services are not intended as consulting, design or implementation services. The following items and functions are not supported under the ItaaS User Service:
    - Administration of Customer's Servers or Network equipment (including server on-boarding (set up), server off-boarding (decommission), and enterprise server configuration changes unless otherwise noted in this service definition)
    - Administration of Customer's Shared Workstations (Shared workstations only)
    - On-site desktop support
    - Data backup and file restoration
    - Printer RMA issues
    - Smartphone, PDA and tablet applications, and devices and applications not provided by Synoptek unless 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

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.

4.1 REQUIREMENTS FOR THIS SERVICE

The following specifications are required for Synoptek ItaaS User Service:

- Customer must have Active Directory in operation. If Customer does not already have Active Directory in operation, and upon Customer request, Synoptek will provide consulting services related to the design and deployment of Active Directory for additional fees.
- Customer will provide Synoptek with Account Operator administration rights to Customer's Active Directory server.
- Customer will provide Synoptek with information pertaining to hardware warranties and hardware maintenance providers. (Dedicated workstations only)
- Customer will assist Synoptek with creation of the documentation necessary for Synoptek to provide customer care services. Documentation includes, but is not limited to the following:
    - Support Escalation matrices
    - Frequently Asked Questions and Troubleshooting Techniques for Best Effort support topics
    - Authorized User information

- List of Applications

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.

4.2 SYNOPTEK RESPONSIBILITIES

4.2.1 Help Desk

- Synoptek will remediate end user desktop issues within a predefined scope of work including:
  - Dedicated workstations: Workstation Hardware Support, Operating System Support, Printing / Network Connectivity Support, Microsoft Office Application Support, and Email Support provided customer is subscribed to Synoptek Exchange or ItaaS services
  - Shared workstations: Password Resets, Timecard Application Support, Email Support
- Synoptek will provide best effort and work with the Customer to generate guidelines to log and route incidents not provided by Synoptek to identified vendors for support, and notification to Customer

4.2.2 Endpoint Management for Dedicated Workstations

- Windows/ macOS Support:
  - In general, the following are the currently, supported platforms:
    - We support all Windows and macOS versions through the end of their mainstream support date
- Peripheral Hardware/Setup and resolution.
- Basic Network Connectivity to end user devices
- Application Support
  - How to questions MS Office and OS
  - Core Application: Microsoft Office, Citrix client, Adobe Reader
- Security:
  - Initiate scans: virus, spyware, adware, malware
  - Email services: anti-virus scanning, URL and attachment defense, Spam and Phishing Detection
  - Synoptek will support customer's existing technologies and platforms during a transition phase but requires migration to Synoptek's systems for Sustained Operations.
- Custom/Proprietary Applications (with proper documentation)
- Provisioning and General Administration:
  - User level adds, removes and changes in AD provided AD servers are under Synoptek Management.
  - AD password resets
- Printer:

- Connectivity Support
- Mapping, Drivers and connectivity

4.2.3 End User Management for Shared Workstations

- End Use Application Support
  - Vendor Management for Timecard Applications
- Security:
  - Email services: anti-virus scanning, URL and attachment defense, Spam and Phishing Detection
  - Synoptek will support customer's existing technologies and platforms during a transition phase but requires migration to Synoptek's systems for Sustained Operations.
- Provisioning and General Administration:
  - User level adds, removes and changes in AD provided AD servers are under Synoptek Management.
  - AD password resets

4.3 CUSTOMER RESPONSIBILITIES

- Providing profile support information prior to onboarding
- Submitting changes to knowledge base support information via Synoptek's change control process
- Providing timely escalation instructions for support issues that Synoptek is unable to resolve due to lack of information or issues deemed out of scope
- Ensuring that any person authorized to access or use the Service fully complies with the Agreement;
- Cooperating with Synoptek regarding its performance of the Service, including, but not limited to, granting reasonable access to Customer's personnel, premises and equipment
- Installing any updates and patches to its OS software that may be reasonably requested by Synoptek (Dedicated workstations only)

4.3.1 Monthly Workstation Maintenance Window (Dedicated Windows workstations only)

- Synoptek will require a monthly maintenance window. During the maintenance window, routine updates are distributed to customer's workstation to resolve known issues and to protect customer from vulnerabilities. Synoptek delivers critical security updates to customer's workstation whenever threats arise, usually without waiting for the maintenance window. It is permissible to continue working during the maintenance windows; however, response time may be occasionally sluggish, and customer's users may be prompted to reboot when updates complete.
  - Patches are only deployed to systems that are specifically relevant to the particular application / operating system (Synoptek doesn't deploy every security patch to every system.)
  - *Windows 10 devices must be kept within the latest three feature update releases. Feature updates are excluded from patching. These will require a separate PS engagement project at an additional fee.*
    - *Note: Feature updates are full version updates released by Microsoft on a 6 month cadence.*

    - A monthly reboot request action is sent as part of the monthly maintenance, after the patches have been deployed.
- Guidelines to Ensure Proper Maintenance
    - During the monthly maintenance window, any or all Synoptek-Managed Workstations may be delivered application and operating system updates and patches. Below are some guidelines that will ensure that systems receive the latest updates and patches as they are delivered, on Thursday nights:
        - Customer's system must be powered ON. *Please also disable "standby" or hibernation*
        - Customer's system must be connected to a network
        - Users should be logged off from their machines
        - If customer's system is not connected to the network or the Internet in time for the Thursday night update, any distributed updates will be delivered the next time the system connects to the Internet or to the network.
    - Note: Synoptek strongly encourages occasional distribution of this notification as a reminder to customer's users of this maintenance window and of the services that are performed on their behalf. This proactive maintenance process is in place to protect customer's end-user systems as close to real-time as possible.

4.4 REPORTING

Synoptek may provide the following reporting based upon customer request.

- Open Tickets
- Monthly Service Metrics
    - First Contact
    - First Response
    - Resolution Met
    - Created and Completed quantity of tickets over 30 days
    - Tickets by Month
    - Open Tickets by Resource (User)
    - Ticket Survey Score
    - OS Patching status
    - Anti-Virus status

5 OPTIONAL SERVICES

5.1 ADVANCED MAC ADMINISTRATION

Synoptek can provide advanced ItaaS capabilities for macOS. This service is priced per device and is available for dedicated workstations only. This service contains the following:

FEATURE AND DESCRIPTION:	ADDITIONAL INFO:	INCLUDED
ENDPOINT CONFIGURATION CONTROL	Synoptek will set policies to enforce desired settings in order to manage endpoint configuration. This service allows for a more robust configuration of macOS than allowed with standard ItaaS service. Examples of endpoint configuration control include the following: • Password Compliancy • Application Blacklisting Note: Policies are based on customer specific requirements. Any additional policy settings may require a separate project at an additional fee.	Requires Advanced Mac Add On
PATCH MANAGEMENT	Synoptek will provide macOS security updates for customer devices. Note: full version upgrades are excluded, these will require a separate PS engagement project at an additional fee.	Requires Advanced Mac Add On
ENCRYPTION ENFORCEMENT	Synoptek will set up enforcement policies for encryption status on customer devices. Synoptek will provide status reporting, as well as encryption key management, and FileVault disk encryption. Note: To be eligible for encryption, the systems require a recovery partition and macOS version 10.13.1 or higher. Synoptek can assist with these pre-requisites as a separate project for an additional cost. MacOS systems that are encrypted must be decrypted prior to Synoptek providing FileVault encryption as a service.	Requires Encryption as a Service

5.2 CUSTOMER TICKETING SYSTEM

Synoptek can provide a ticketing system for customers and a process for which customers and Synoptek to share and collaborate on tickets.

5.3 DESIGNATED CONSULTING ENGINEER

For customer Application management, Synoptek offers Designated Consulting Engineers. These resources will work remotely and are scheduled in advance for a set number of hours per month.

5.4 ONSITE ENGINEER

If you would like to have someone on site at your location, Synoptek offers that through our Onsite Engineer. These resources are scheduled in advance for a set number of hours per month.

6 APPENDIX

6.1 Comparison Chart: ITaaS User Bundles

*Requires Advanced Mac Add On

ITaaS User	Shared		Standard		MAX	
	Windows	macOS	Windows	macOS	Windows	macOS
Vendor Escalation	X	X	X	X	X	X
Email and AD Provisioning	X	X	X	X	X	X
Patch Management			X	X*	X	X*
Endpoint Configuration Control			X	X*	X	X*
Desktop Admin			X	X	X	X
Remote Control			X	X	X	X
New Employee Provisioning			X	X	X	X
Software Distribution			X	X	X	X
Asset Tracking			X	X	X	X
24x7x365 Incident Support	X	X	X	X	X	X
Email Protection	X	X	X	X	X	X
Self Service Password Reset			X	X	X	X
Anti-Virus			X	X	X	X
Endpoint Protection, Threat Prevention, Detection and Response (EDR)			X	X	X	X

Encryption Enforcement				X*		X*
Advanced EDR					X	X
Malware Removal					X	X
Security Testing and Training					X	X
DNS Filtering					X	X
Endpoint and Data Recovery					X	X

- Additional T&M charge may apply if Synoptek does not have components already built for Software Distribution.
- Endpoint Configuration Control requires Active Directory.