Integrated MSP LLC Service Catalog

Service	Includes	Third Party	Description
TIER 1 DESKTOP	RMM	Connectwise Command	Remote Monitoring Management is used to manage the clients' IT systems, such as servers, desktops, laptops, and software, through locally installed agents.
	Antivirus	Webroot or Watchguard EDPR	Provider will provide and manage the Anti-Virus software to ensure virus software is installed and definitions are reasonably up to date. Customer recognizes that this service does not guarantee against infection
	Patch management	Connectwise Command	Provider will manage Microsoft patches for current Microsoft supported Windows Operating systems. and Microsoft supported Microsoft Office applications. Patches will include security updates, critical updates, definition updates, update roll ups, and service packs. This excludes Microsoft Windows Feature Releases
	Asset Monitoring	Connectwise Command	
	Warranty Status	Connectwise Command	Warranty tracking and reporting for vendors such as Dell and HP can be provided.
TIER 2 DESKTOP	RMM	Connectwise Command	Remote Monitoring Management is used to manage the clients' IT systems, such as servers, desktops, laptops, and software, through locally installed agents.
	Antivirus	Webroot or Watchguard EDPR or MS Defender	Provider will provide and manage the Anti-Virus software to ensure virus software is installed and definitions are reasonably up to date. Customer recognizes that this service does not guarantee against infection
	Asset Monitoring	Connectwise Command	Hardware and software inventories are maintained within the monitoring systems. Asset reports are available. Additionally, warranty tracking and reporting for vendors such as Dell and HP can be provided.
	Warranty Status	Connectwise Command	Warranty tracking and reporting for vendors such as Dell and HP can be provided.
	Patch management	Connectwise Command	Provider will manage Microsoft patches for current Microsoft supported Windows Operating systems. and Microsoft supported Microsoft Office applications. Patches will include security updates, critical updates, definition updates, update roll ups, and service packs. This excludes Microsoft Windows Feature Releases
	Unlimited Help Desk		Helpdesk is available during normal business hours from 7am to 5pm, Monday through Friday, except during Holidays. Holidays are New Year's Day, Memorial Day, Independence Day, Labor Day, Thanksgiving Day, and Christmas Day. After-Hours Support is available on weekdays 5pm-7am, Holidays and Saturday and Sunday 24 hours a day. After-hours support is intended for critical systems outages. After-hours support has a one-hour call back response time and may incur additional charges as defined by the Order. Help Desk is available to provide phone and remote control support on issues related to the operation and use of supported products.
TIER 1 SERVER	RMM	Connectwise Command	Remote Monitoring Management is used to manage the clients' IT systems, such as servers, desktops, laptops, and software, through locally installed agents.
	Antivirus	Webroot or Watchguard EDPR	Provider will provide and manage the Anti-Virus software to ensure virus software is installed and definitions are reasonably up to date. Customer recognizes that this service does not guarantee against infection
	Patch management	Connectwise Command	Provider will manage Microsoft patches for current Microsoft supported Windows Operating systems. and Microsoft supported Microsoft Office applications. Patches will include security updates, critical updates, definition updates, update roll ups, and service packs. This excludes Microsoft Windows Feature Releases
	Asset Monitoring	Connectwise Command	Hardware and software inventories are maintained within the monitoring systems. Asset reports are available. Additionally, warranty tracking and reporting for vendors such as Dell and HP can be provided.
	Warranty Status	Connectwise Command	Warranty tracking and reporting for vendors such as Dell and HP can be provided.
TIER 2 SERVER	RMM	Connectwise Command	Remote Monitoring Management is used to manage the clients' IT systems, such as servers, desktops, laptops, and software, through locally installed agents.
	Antivirus	Webroot or Watchguard EDPR	Provider will provide and manage the Anti-Virus software to ensure virus software is installed and definitions are reasonably up to date. Customer recognizes that this service does not guarantee against infection
	Patch management	Connectwise Command	Provider will manage Microsoft patches for current Microsoft supported Windows Operating systems. and Microsoft supported Microsoft Office applications. Patches will include security updates, critical updates, definition updates, update roll ups, and service packs. This excludes Microsoft Windows Feature Releases
	Asset Monitoring	Connectwise Command	Hardware and software inventories are maintained within the monitoring systems. Asset reports are available. Additionally, warranty tracking and reporting for vendors such as Dell and HP can be provided.
	Warranty Status	Connectwise Command	Warranty tracking and reporting for vendors such as Dell and HP can be provided.
	Unlimited Help Desk		Helpdesk is available during normal business hours from 7am to 5pm, Monday through Friday, except during Holidays. Holidays are New Year's Day, Memorial Day, Independence Day, Labor Day, Thanksgiving Day, and Christmas Day. After-Hours Support is available on weekdays 5pm-7am, Holidays and Saturday and Sunday 24 hours a day. After-hours support is intended for critical systems outages. After-hours support has a one-hour call back response time and may incur additional charges as defined by the Order. Help Desk is available to provide phone and remote control support on issues related to the operation and use of supported products.
Antivirus	Antivirus	Webroot or Watchguard EDPR or MS Defender	Provider will provide and manage the Anti-Virus software to ensure virus software is installed and definitions are reasonably up to date. Customer recognizes that this service does not guarantee against infection

Advanced Security for Endpoints	EDR	Watchguard EPDR or SentinelOne or Huntress	Endpoint Detection and Response (EDR), also referred to as endpoint detection and threat response, is an endpoint security solution that continuously monitors end-user devices to detect and respond to cyber threats like ransomware and malware
Essentials Complete Email Security	Spam filtering	Barracuda Email Gateway Defense	The Barracuda Email Security Gateway leverages Barracuda Central to identify email from known spammers and determine whether domains embedded in email lead to known spam or malware domains. Its industry-leading techniques protect against attempts to embed text inside images with the intent of hiding content from traditional spam filters.
	Email Archiving	Barracuda Email Archiving	Retain email communication. Capture an accurate and unmodified copy of each new message at the time it's sent or received and keep it for as long as needed. Reduce storage requirements. Cloud Archiving Service provides unlimited storage per user, reducing the need to store emails on your Exchange Server and in Office 365 mailboxes. Ensure compliance. Meet demanding compliance requirements and address e-discovery requests with tamper-proof archiving and granular retention policies.
	365 Mailbox, OneDrive, SharePoint backups	Barracuda Backup	Easy to use. Find and recover the exact data you want quickly and easily with a newly redesigned user interface that is accessible from anywhere with an internet connection. Flexible, comprehensive Office 365 support. Back up all your Teams, Exchange, SharePoint, and OneDrive data, and choose full or granular restore depending on your specific needs. Cloud native. Your Office 365 data is already in the cloud — saving secure, encrypted backups in the same network means better performance and instant scalability.
	email encryption	Barracuda Email Encryption	If you are sending a sensitive email, you can manually mark it for encryption. However, you can also create a policy to automatically encrypt emails based on their sender, content and other criteria. Encryption policies ensure that your organization complies with regulations designed to protect customer data, such as HIPAA.
Impersonation Protection	Phishing protection	Barracuda Sentinel	Barracuda can automatically detect and prevent spear-phishing attacks that evade traditional email security systems. Barracuda's AI engine learns each organization's unique communication patterns and leverages these patterns to identify anomalies and quarantine spear-phishing attacks in real time. Barracuda automatically quarantines business email compromise attacks by detecting anomalies in the email header, as well as the content of the email. The AI does not require any manual rules or user setup and can detect any type of BEC attack automatically from day one. Barracuda can detect any type of employee impersonation, including impersonation of executives, as well as mid- and low-level employees. It can detect spoofed emails, typo squatted domains, and impersonation emails sent from free or personal email clients. By discovering anomalous communication patterns within the body of the email, the link, or the email header, Barracuda can stop zero-day phishing attacks that evade other email security systems. It can detect any type of zero-day phishing attacks, including links leading to a fake sign-in page, as well as links to malicious websites. Barracuda has been trained to recognize and automatically quarantine phishing emails that impersonate web services, such as Microsoft Outlook, DocuSign, and Dropbox. The Barracuda AI can prevent web impersonations, even when they use deceptive characters or zero-day links. Barracuda automatically stops attacks that impersonate employees by spoofing their email address. The AI engine recognizes the anomalies in spoofing emails and quarantines them. Barracuda AI can automatically predict which employees are likely to be targeted by spear-phishing attacks, based on their role and their day-to-day access to sensitive information. Customers can report false positives and missed attacks to Barracuda, which are used to retrain the AI classifiers. This enables the AI to continuously improve its precision and adapt its detection capabilities. The raw data from the AI detections can be exported to a CSV file.
Enhanced Security for Endpoints	DNS Protection	Webroot	Automated filtering uses Webroot BrightCloud® Internet Threat Intelligence to automatically block requests to undesirable, dangerous or malicious internet domains, even encrypted DNS over HTTPS (DoH) requests. This filtering alone stops most internet threats before they can infect networks or endpoints. It helps organizations achieve the management control over their DNS connection recommended by the joint NSA and CISA Guidance on Strengthening Cyber Defense Through Protective DNS.
	Profile and Protect	ConnectWise Fortify Protection	Monitoring and analytics-Monitor key log files to identify and correlate events that could be malicious, while providing additional security and adherence to regulatory guidelines. Customized security profiles- Reduce the data noise so you can focus on what really matters in identifying technical gaps in your customer's networked environment. ConnectWise Fortify Protection helps you to take action on what's needed to prevent costly attacks on your customers' vital assets. Risk scoring and alert thresholds-Risk scoring helps you identify protection gaps and how they might impact a device's vulnerability to threats you're trying to protect against. ConnectWise Fortify Protection lets you customize alert thresholds on a per-device basis, and generate tickets based on elevated risk scores.
	Security Awareness Training	Webroot or Barracuda Phishline or Knowbe4	Ongoing training program that significantly reduces the risk of security breaches through phishing simulations based on real-world attacks and training that covers relevant security and compliance topics.
	Hardened Baseline Configuration for servers		A baseline configuration is a group of settings placed on a system before it is approved for production. Using baselines is a technique that evolved from administration checklists to ensure systems were set up correctly for their intended purpose.
	Hardened Baseline Configuration for desktops and laptops		A baseline configuration is a group of settings placed on a system before it is approved for production. Using baselines is a technique that evolved from administration checklists to ensure systems were set up correctly for their intended purpose.
	DarkWeb research	Connectwise	Provide a list of email addresses provided to identify customers that have been part of a known data breach.
Remote Access Audit	Project to review who has Remote access via RDP and VPN capabilities	LionGard	Project to review who has Remote access via RDP and VPN capabilities
Privileged Account Audit	Project to review who has privileged accounts in O365, Active Directory, Local computers	LionGard	Project to review who has privileged accounts in O365, Active Directory, Local computers
User Account Management	Project to review password policy,admin groups, inactive accounts, inactive computers.	LionGard	Project to review password policy,admin groups, inactive accounts, inactive computers.
MFA for Privileged Accounts	MFA product	Cisco DUO or Watchguard AuthPoint	Ensure that only authorized personnel have access to your powerful privileged account passwords. You need to ensure that only the right people can utilize the powerful privileged account passwords that control access to your systems with sensitive data.
MFA for Remote Access	MFA product	Cisco DUO or Watchguard AuthPoint	Multi-factor authentication is a method to protect remote access via Remote Desktop or VPN to corporate networks and business-critical systems.
MFA for Office 365	Built into O365	Microsoft	By setting up MFA, you add an extra layer of security to your Microsoft 365 account sign-in. For example, you first enter your password and, when prompted, you also type a dynamically generated verification code provided by an authenticator app or sent to your phone.

Server Backup BDR	BDR Appliance sync'd offsite -servers only	Datto SIRIS	SIRIS is the secure data protection solution built to protect their data. Security comes first with two-factor authentication and the immutable Datto Cloud to deliver the all-in-one solution for backup and recovery in a ransomware world.
Server Backup files	File level backups sync'd offsite - servers only	Barracuda MSP Intronis Online Backup	Software-only data protection featuring local and cloud backup for physical and virtual environments.
Backup workstations	File level backup of workstations	Carbonite or Microsoft OneDrive	Carbonite will backup all the data on your computer as long as it's connected to the internet. OneDrive is a secure access, sharing & file storage solution which enables users to store MyDocuments, My Desktop files, photos, videos, documents, & more
Backup Virtual	VM level backup of virtual machines sync'd to Azure blog storage	Veeam and Microsoft Azure	Veeam Backup & Replication is a comprehensive enterprise backup solution that protects all workloads, cloud, virtual & physical. Veeam backup jobs can use Azure blog storage as a backup repository which affectively places a copy of the backups into Microsoft Azure where they can be restored as an Azure server for DR purposes.
Backup Cloud	Azure backup of Servers running in Azure	Microsoft Azure	The Azure Backup service provides simple, secure, and cost-effective solutions to back up your data (virtual servers) and recover it from the Microsoft Azure cloud.
SIEM	Security Incident and Event Monitoring	Connectwise Eventtraker or Connectwise Perch	Perch is a co-managed threat detection and response platform backed by an in-house Security Operations Center (SOC). We built Perch to be flexible, scaling to any size business and tailored to fit your specific needs.
Firewall as a Service	Firewall hardware, Total Protection Suite licensing, hardware replacement, monitoring, support	Watchguard Firebox	A firewall protects private networks from unauthorized users on the Internet. Traffic that enters or leaves the protected networks is examined by the firewall. The firewall denies network traffic that does not match the security criteria or policies. Firewall as a Service includes the appliance, all applicable licenses, and complete management of the firewall.
Wireless as a Service	Wireless hardware, Hardware replacement, monitoring, support	Ubiquiti or Watchguard	Wireless as a Service combines both infrastructure like access points as well as managed services including monitoring, configuration, and support.
Monthly Projects/Support Hours	Labor to provide HelpDesk or Onsite support as needed		These services will be billed on an hour for hour basis and invoiced at the end of each month.
Project work	Quoted or hourly project work		Project work will be estimated or quoted and invoiced when the project is completed
Break Fix	Onsite or offsite hourly support		Break Fix support is provided on an hourly basis and will be invoiced at the completion of the support incident.
Email DNS Security	Project to configure SPF, DMARC, DKIM recores to further secure email		Project to configure SPF, DMARC, DKIM recores to further secure email
Service Installation			
Vulnerability Scans	Scan network for know vulnerabilities	Nessus	Nessus is the de-facto industry standard vulnerability assessment solution for security practitioners. The latest intelligence, rapid updates, an easy-to-use interface.
Password Manager	Password Manager	LastPass	Improve password hygiene and security, without compromising ease of use for employees or admins. With LastPass to manage your logins, it's easy to have a strong, unique password for every online account and improve your online security.
Application and Hardware Lifecycle Management	5 year budget		We ask that you attend quarterly business reviews where we review a 5 year budget that we maintain for you
Application Isolation and containment technology (Zero Trust- Applications)	EDR product	Watchguard EDPR	What Is Zero-Trust? Forrester Research Inc. first popularized the term "zero-trust" around 2009. Its premise focuses on a more comprehensive approach to IT security, where organizations apply stronger restrictions and redefine access control. This security model assumes nothing is to be trusted despite the relationship with a company network. https://www.watchguard.com/wgrd-resource-center/feature-brief/zero-trust-application
Laptop Encryption	Service to encyrpt laptops	Microsoft Bitlocker	
Mobile Device Management	MDM solution	Microsoft Intune (Device manger)	Microsoft Intune is a cloud-based service that focuses on mobile device management (MDM) and mobile application management (MAM). You control how your organization's devices are used, including mobile phones, tablets, and laptops. You can also configure specific policies to control applications. For example, you can prevent emails from being sent to people outside your organization. Intune also allows people in your organization to use their personal devices for school or work. On personal devices, Intune helps make sure your organization's data stays protected and can isolate organization data from personal data.
Email External Source Notification	Project to configure MS365 to put notification at top of email	Microsoft 365	
Disaster Recovery Testing - minimal	File recovery		Restore some critical files to verify they can be restored
Disaster Recovery Testing - FULL	Server(s) recovery		Fully recover the servers in another environment or on other physical or virtual servers
Website hosting	Hosting of customer's website	Microsoft Azure or Flywheel	Hosting of basic websites or WordPress websites.
Server Hosting	Hosting of customer virtual server	Microsoft Azure	Facilitation of Azure hosted files servers
Privileged Account Manager	Manage user admin credentials	Cyberfox Autoelevate	Designed to protect end users. AutoElevate is Privileged Access Management (PAM) for MSPs. Reduce local admin rights and secure clients with AutoElevate Privileged Access Solutions.