

Integrated MSP Service Catalog 04/15/2026

Our Services are limited to the following Services

<u>Service</u>	<u>Third Party *</u>	<u>Description</u>
Essentials 25 Plan	See Individual Services details	Minimal set of tools and hourly support services ideal for Co-Managed Environments including: Tier 1 Desktop (PCs and Macs) Managed EDR Premium Plus Email Security SaaS alerting Hardware Procurement Dedicated Account Manager Semi Annual Business Reviews
Standard 25 Plan	See Individual Services details	A comprehensive plan for businesses looking for remote support, robust security protection and strategic advisory services including: Unlimited HelpDesk MS365 and Google Workspace Admin Employee Onboarding and Offboarding Managed Workstations (PCs and Macs) Managed EDR Email Security/Spam filtering Hardware Procurement Dedicated Account Manager Quarterly Business Reviews IT Advisor Service
Compliance 25 Plan	See Individual Services details	Everything you get in our Standard_25 plan PLUS enhanced security services for those industries with advanced compliance requirements including: Unlimited HelpDesk MS365 and Google Workspace Admin Employee Onboarding and Offboarding Managed Workstations (PCs and Macs) Managed EDR Email Security/Spam filtering Managed SaaS alerting Hardware Procurement Dedicated Account Manager Quarterly Business Reviews IT Advisor Service Advanced Phishing Protection Security Awareness Training Security Incident and Event Monitoring (SIEM) Email Encryption Data Loss Prevention (DLP)

Tier 1 Server Monitoring & Monthly Maintenance	NinjaOne or Connectwise	<p>Monthly Maintenance- A Systems Administrator will perform a maintenance checklist to ensure servers are running optimally and identify any necessary remediation.</p> <p>RMM - Remote Monitoring Management agent is used to manage the clients' IT systems, such as servers, desktops, laptops, and software, through locally installed agent.</p> <p>Patch management-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.</p> <p>Asset Monitoring -Hardware and software inventories are maintained within the RMM systems. Asset reports are available. Additionally, warranty tracking and reporting for vendors such as Dell and HP can be provided</p> <p>Warranty Status-Warranty tracking and reporting for vendors such as Dell and HP can be provided when the RMM system is capable of doings so.</p>
Tier 1 Server Monitoring & Quarterly Maintenance	NinjaOne or Connectwise	<p>Quarterly Maintenance- A Systems Administrator will perform a maintenance checklist to ensure servers are running optimally and identify any necessary remediation.</p> <p>RMM - Remote Monitoring Management agent is used to manage the clients' IT systems, such as servers, desktops, laptops, and software, through locally installed agent.</p> <p>Patch management-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.</p> <p>Asset Monitoring -Hardware and software inventories are maintained within the RMM systems. Asset reports are available. Additionally, warranty tracking and reporting for vendors such as Dell and HP can be provided</p> <p>Warranty Status-Warranty tracking and reporting for vendors such as Dell and HP can be provided when the RMM system is capable of doings so.</p>
Tier 1 Server Monitoring, Monthly	NinjaOne or Connectwise	<p>Monthly Monitoring- RMM - Remote Monitoring Management agent is used to manage the clients' IT systems, such as servers, desktops, laptops, and software, through locally installed agent.</p> <p>Patch management-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.</p> <p>Asset Monitoring -Hardware and software inventories are maintained within the RMM systems. Asset reports are available. Additionally, warranty tracking and reporting for vendors such as Dell and HP can be provided</p> <p>Warranty Status-Warranty tracking and reporting for vendors such as Dell and HP can be provided when the RMM system is capable of doings so.</p>
Tier 1 Managed Services	NinjaOne or Connectwise	<p>Support for a users additional device:</p> <p>RMM - 24x7 Remote Monitoring and Management agent is used to manage the clients' IT systems, such as servers, desktops, laptops, and software, through locally installed agent.</p> <p>Patch management-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</p> <p>Asset Monitoring -Hardware and software inventories are maintained within the RMM systems. Asset reports are available. Additionally, warranty tracking and reporting for vendors such as Dell and HP can be provided</p> <p>Warranty Status-Warranty tracking and reporting for vendors such as Dell and HP can be provided when the RMM system is capable of doings so.</p>

<p>Tier 2 Server Monitoring & Monthly Maintenance</p>	<p>NinjaOne or Connectwise</p>	<p>Monthly Maintenance- A Systems Administrator will perform a maintenance checklist to ensure servers are running optimally and identify any necessary remediation. Unlimited Help Desk-Helpdesk is available 7am to 5pm (24hr optional) , except during Holidays. Holidays are New Year’s Day, Memorial Day, Independence Day, Labor Day, Thanksgiving Day, and Christmas 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 RMM - Remote Monitoring Management agent is used to manage the clients' IT systems, such as servers, desktops, laptops, and software, through locally installed agent. Patch management-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 -Hardware and software inventories are maintained within the RMM systems. Asset reports are available. Additionally, warranty tracking and reporting for vendors such as Dell and HP can be provided Warranty Status-Warranty tracking and reporting for vendors such as Dell and HP can be provided when the RMM system is capable of doings so.</p>
<p>Tier 2 Server Monitoring & Quarterly Maintenance</p>	<p>NinjaOne or Connectwise</p>	<p>Quarterly Maintenance- A Systems Administrator will perform a maintenance checklist to ensure servers are running optimally and identify any necessary remediation. Unlimited Help Desk-Helpdesk is available 7am to 5pm (24hr optional) , 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 RMM - Remote Monitoring Management agent is used to manage the clients' IT systems, such as servers, desktops, laptops, and software, through locally installed agent. Patch management-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 -Hardware and software inventories are maintained within the RMM systems. Asset reports are available. Additionally, warranty tracking and reporting for vendors such as Dell and HP can be provided Warranty Status-Warranty tracking and reporting for vendors such as Dell and HP can be provided when the RMM system is capable of doings so.</p>

Tier 2 Managed Services	NinjaOne or Connectwise	<p>Unlimited Help Desk-Helpdesk is available 7am to 5pm (24hr optional) Monday through Friday, except during Holidays. Holidays are New Year's Day, Memorial Day, Independence Day, Labor Day, Thanksgiving Day, and Christmas Day. Help Desk is available to provide phone and remote control support on issues related to the operation and use of supported products</p> <p>RMM - Remote Monitoring Management agent is used to manage the clients' IT systems, such as servers, desktops, laptops, and software, through locally installed agent.</p> <p>Patch management-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.</p> <p>Asset Monitoring -Hardware and software inventories are maintained within the RMM systems. Asset reports are available. Additionally, warranty tracking and reporting for vendors such as Dell and HP can be provided</p> <p>Warranty Status-Warranty tracking and reporting for vendors such as Dell and HP can be provided when the RMM system is capable of doings so.</p>
Data Loss Prevention - Scanning and Encryption	Actifile	Provider will manage a Data Loss Prevention solution which will scan users computers, servers, OneDrive, SharePoint and Google Workspace for sensitive files. This is includes scanning and encryption.
Data Loss Prevention -Scanning Only	Actifile	Provider will manage a Data Loss Prevention solution which will scan users computers, servers, OneDrive, SharePoint and Google Workspace for sensitive files. This is scanning only and does not include encryption.
SaaS Backups	Barracuda	Provider will manage the solution to backup customer's 365 tenant including Mailboxes, OneDrive, SharePoint
Adv Email Security - SPAM Filter Only	Barracuda	Provider will manage the Barracuda Email Security Gateway cloud based service. 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
Essentials Complete Email Security	Barracuda	<p>Email Gateway Defense - Provider will manage the Essentials Complete Mail Security cloud based service. 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.</p> <p>Email Archiving - Provider will manage the Essentials Complete Mail Security cloud based service. 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.</p> <p>MS365 Backups - Provider will manage 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.</p> <p>Barracuda Email Encryption - Provider will configure the system so that 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.</p>
Impersonation Protection	Barracuda	Provider will manage the Barracuda service which can automatically detect and prevent spear-phishing attacks that evade traditional email security systems

Premium Plus Email Security	Barracuda	<p>Provider will manage the Barracuda Services:</p> <p>Email Security - Spam and Malware Protection, Attachment Protection, Link Protection, Email Continuity, Email Encryption, Data Loss Prevention.</p> <p>Sentinel - Phishing and Impersonation Protection, Account Takeover Protection, Domain Fraud Protection</p> <p>FIR - Threat Hunting and Response, Automated Workflows, Automated Remediation</p> <p>Data Inspector - Data Insight and Protection</p> <p>Cloud Backups - MS365 backups of Mailbox, OneDrive, SharePoint</p> <p>Cloud Archiving - Journaling of email in and out of the MS365 Tenant</p>
MDR Cloud	BlackPoint or Sherweb or Huntress	<p>Provider will provision the service to provide Managed Detection and Response (MDR) for MS365 and Google Workspace, a security solution to actively defends MS365 cloud workflows and provide contextual alerting for unauthorized logins by gathering contextual analysis about the unauthorized use of MS 365 and Google Workspace logins. Identity Threat Detection and Response (ITDR)</p>
MDR Endpoint	Blackpoint Cyber, SentinelOne, Hutress, or Watchguard	<p>Provider will provide Endpoint Detection and Response (EDR), an endpoint security solution that continuously monitor by end-user devices to detect and respond to cyber threats like ransomware and malware.</p>
Advanced Security for Endpoints	Blackpoint Cyber, SentinelOne, Huntress, or Watchguard	<p>Provider will provide Endpoint Detection and Response (EDR), an endpoint security solution that continuously monitors end-user devices to detect and respond to cyber threats like ransomware and malware.</p>
Advanced Security for MS365	Sherweb or Blackpoint or Huntress	<p>Provider will provision the service to provide Managed Detection and Response (MDR) for MS365, a security solution to actively defends MS365 cloud workflows and provide contextual alerting for unauthorized logins by gathering contextual analysis about the unauthorized use of MS 365 logins. Identity Threat Detection and Response (ITDR)</p>
SIEM Monitoring	Blumira	<p>Provider will manage Blumira's open SIEM cybersecurity platform that provides ransomware protection, advanced detection and response. The SIEM provides for real-time security event analysis to help with investigations , early threat protection and incident response.</p>
SIEM Monitoring	Connectwise	<p>The provider will manage the Connectwise SIEM. The SIEM provides for real-time security event analysis to help with investigations , early threat protection and incident response.</p>
MFA for Remote Access	Cisco or Duo	<p>Provider will configure the service designed to protect remote access via Remote Desktop or VPN to corporate networks and business-critical systems.</p>
Compliance Program CyberWatch	Galactic Advisors	<p>Vulnerability scanning and penetration testing</p> <p>Framework alignment across NIST, CIS, SOC2, HIPAA, and others</p> <p>Audit-ready reports for insurers and regulators</p> <p>Executive dashboards that communicate progress and readiness</p> <p>Third-party attestation that reinforces trust and credibility</p>
Server Backup Files	Cove	<p>Provider will manage the service which is a Software-only data protection featuring local and cloud backup for physical and virtual environments. Includes a file level backups sync'd offsite - servers only. Does not include DR capabilities.</p>
Backup Service DATTO	Datto	<p>Provider will manage the service designed to backup and protect the customers data stored on an on-premises server. 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.</p>
Backup Service Virtual	Veeam	<p>Provider will manage the Virtual Server backups using a comprehensive enterprise backup solution that protects all workloads, cloud, virtual & physical. Backup jobs can use Azure blob 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.</p>
Keepit for Google Workspace	Keepit	<p>Provider will provide a solution to backup the user's Google Workspace data.</p>

Security Awareness Training Services	KnowBe4	Provider will manage the KnowBe4's AI-powered, new-school security awareness training and simulated phishing that allows organizations to drive awareness and change user behavior. This enables you to build on stronger security culture by effectively managing the ongoing problem of social engineering.
LastPass	LastPass	Provider will provide the password manager software which will 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.
Virtual Server Hosting	Microsoft	The Provider will manage the virtual server environment within the Microsoft Azure.
Website Hosting	Microsoft or Flywheel	Provider will manage the hosting environment of basic websites or WordPress websites. Provider is not responsible for ADA compliance of the customer's website.
Nessus Scan Annual billed monthly	Nessus	An annual Nessus Scans will be performed to identify internal risks to the environment and reviewed with the customer.
Wireless As A Service	Ubiquiti	Provider will deploy and manage a Wireless as a Service that combines both infrastructure such as access points as well as managed services including monitoring, configuration, hardware replacement, and support.
Firewall As A Service	Watchguard	Provider will deploy a firewall appliance that 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.
AutoElevate	CyberFox	Provider will manage the solution using a product, Cyberfox AutoElevate, which is a Privileged Access Management (PAM). Reduce local admin rights and secure clients with AutoElevate Privileged Access Solutions.
Project work		Quoted projects

* Third Party - Refer to:

[Schedule of Third-Party Services Attachment – notice of third-party services and waiver of claims.](#)