

Addendum to Master Services Agreement

- i. This service addendum is made pursuant to the Master Services Agreement (The “Agreement”) between (1) the customer (who is identified in the accompanying electronic rider, the terms of which are explicitly incorporated herein) and the customer’s affiliates (collectively the “Customer”) and (2) Dynamic Quest, LLC (“Dynamic Quest”).
- ii. Term of Service: This Addendum will remain in effect until the termination date of the Agreement.

Description of the Service

91% of cyber-attacks starting in the inbox, email is the most targeted point of entry for attackers. Dynamic Quest’s Email Security service delivers comprehensive inbound & internal protection against phishing, malware, spoofing, and business email compromise.

Dynamic Quest offers two service tiers—Basic and Advanced—so you can choose the level of protection that best fits your security needs and compliance requirements.

Basic Email Security

Basic Email Security service provides strong, AI-powered protection against phishing, malware, and impersonation attacks. Basic is ideal for organizations seeking modern threat detection with minimal complexity and low management overhead.

- 1) AI-Driven Phishing Detection: Uses computer vision, behavioral analysis, and sender authentication to identify brand spoofing, lookalike domains, QR-code phishing, and other advanced phishing techniques.
- 2) Inbound & Internal Threat Protection: Blocks spam, malicious links, malware attachments, and zero-day threats using multi-layered analysis.
- 3) Real-Time Inbox Coaching: Smart, contextual banners inside emails help users recognize risky messages and make safer decisions.
- 4) Zero-Day Malware & Attachment Analysis: Identifies previously unseen threats using AI-based file and payload inspection.
- 5) URL Time-of-Click Protection: Prevents users from accessing malicious websites even if links become dangerous after delivery.

Advanced Email Security

Advanced Email Security service goes beyond threat detection to include automated remediation, data protection, and compliance capabilities. Advanced is ideal for organizations with higher security requirements or regulatory obligations.

- 1) Multi-Layered Threat Defense: Combines gateway filtering, API-based inbox defense, AI threat detection, sandboxing, and URL rewriting to block spam, malware, ransomware, phishing, and zero-day attacks.
- 2) Post-Delivery Detection & Automated Remediation: Identifies threats that bypass initial filters and automatically removes malicious emails from all affected inboxes.
- 3) Account Takeover Protection: Detects suspicious login behavior and stops compromised accounts from sending fraudulent messages.
- 4) Advanced Threat Protection (ATP): Sandboxing and deep payload analysis to detect sophisticated, evasive malware.
- 5) Email Encryption: Provides secure, policy-based email encryption to protect sensitive information in transit and support regulatory compliance requirements.
- 6) Data Protection & Compliance: Includes long-term email archiving, e-discovery, and retention policies for compliance-driven industries.

The Email Security Service description explains the service to be provided by Dynamic Quest. This service description may be adjusted at any time by Dynamic Quest for accuracy. Please contact your sales representative or go to our on-line service description site for the latest service description.

https://info.dynamicquest.com/service_description

Service Set-up

The Service set-up includes:

- 1) Setting up the Email Security technology on the Customer's systems; and,
- 2) Required DNS adjustments.

The Service set-up does not include:

- 1) Transferring Allow or Do Not Allow lists from the Customer's previous email security technology; and,
- 2) Site Surveys; and,
- 3) Migration efforts from another service to this service; and,
- 4) Removing, organizing or arranging files on an endpoint; and,
- 5) Removal or disposing of equipment not owned by Dynamic Quest.

Pricing

Services will be invoiced one (1) month in advance of services provided.

The following billing elements are used to invoice for this service:

- Email Security Deployment - A non-recurring charge for the set-up of Email Security.
- Basic Email Security - Licensed Per User / Mailbox - A monthly recurring charge for software licensing for each email account; or,

- Advanced Email Security - Licensed Per User / Mailbox - A monthly recurring charge for software licensing for each email account.

Service Limitations

In addition to other limitations and conditions set forth in this Service Description, the following service and support limitations are expressed:

Dynamic Quest expects the use of a fully implemented Microsoft local Active Directory or Azure AD structure, which facilitates and streamlines management, oversight, security, and project implementations. If a reactive support solution requires substantial time to implement due to the absence of a fully implemented Microsoft local or Azure Active Directory structure, Dynamic Quest, at its sole discretion, may bill the extra time as hourly out of scope in accordance with Addendum E *(use this link to go to the Service Description site with the Addendums: https://info.dynamicquest.com/service_description)*.

Responsibility for workstation, server and network equipment software version upgrades are described in Addendum B *(use this link to go to the Service Description site with the Addendums: https://info.dynamicquest.com/service_description)*.

Any audit support provided by Dynamic Quest will be in accordance with Addendum F *(use this link to go to the Service Description site with the Addendums: https://info.dynamicquest.com/service_description)*.

Customer Hardware and Systems must be current in hardware and software standards to support the customer's existing operating environment. This requires: Warrantable, serviceable and able to support and perform Customer's current business operating environment.

Customer understands that no monitoring service, software product, or training program can fully protect them from digital theft. DYNAMIC QUEST HAS NO OTHER EXPRESS OR IMPLIED GUARANTEES, WARRANTIES, OR CONDITIONS beyond those provided by the Agreement.

Customer Responsibilities

- 1) Customer grants permission for Dynamic Quest to have secure remote access into Customer's network for management, reporting, alerting, and support functionality.
- 2) Customer will promptly notify Dynamic Quest of any events/incidents that could impact the services defined within this Addendum and/or any supplemental service needs, and for Dynamic Quest to respond in a timely manner via phone, email, and/or remote access.

- 3) Customer agrees that it will inform Dynamic Quest of any modification, installation, or service performed on the Network by individuals not employed by Dynamic Quest to assist Dynamic Quest in providing an efficient and effective Network support response.
- 4) Customer grants permission for Dynamic Quest to become the CSP (Customer Service Provider) for Microsoft Office 365 licenses, Microsoft 365 licenses, and any instances of Azure Hosting. Dynamic Quest will provide for the management and troubleshooting of any issues as well as Tier One helpdesk. Being the Microsoft assigned CSP allows Dynamic Quest to provide the quickest and most proactive levels of support for our Customers.
- 5) All Dynamic Quest owned equipment:
 - a) The Customer is responsible for providing space for the equipment that meets the following criteria:
 - b) Kept inside a climate-controlled, dry area that is protected from the weather. The climate-controlled area must maintain a temperature between 50 degrees Fahrenheit and 80 degrees Fahrenheit; and,
 - c) The climate-controlled area must be kept at a humidity between 50% - 80% and provides air flow; and,
 - d) The area cannot be under construction or have excessive dust.
 - e) Customer is responsible to provide power for the equipment. The power must be in compliance with local electrical regulations. The Customer is responsible for knowing the electrical regulations pertaining to their location; and,
 - f) Customer will provide power conditioning and battery backup for the Appliances; and,
 - g) Customer will provide two (2) gigabit network drops and two (2) internal static IP addresses for each piece of Dynamic Quest provided equipment; and,
 - h) Equipment must be kept in a location that is secure so that only authorized personnel can access the equipment.
 - i) Equipment must be installed in a telecom rack and the rack must be properly installed.
- 6) The Customer is responsible for 3rd party fees for products, software, services, and subscriptions not expressly provided by Dynamic Quest.
- 7) The Customer is responsible for providing adequate and reliable Internet connectivity including appropriate bandwidth.
 - a) All network connections from the Internet Provider (ISP) to the endpoint are minimum 1GB handoffs.
 - b) The Customer is responsible for the wiring within the building.
 - i) The wiring type will impact the internet speed for any equipment connected to the wiring.
 - ii) If the Customer selects high speed internet, it is recommended the Customer confirm the internet speed supported by the wiring type.
 - iii) Installing new wiring may be required in order to obtain higher internet speed.
- 8) Cost of consumables, replacement parts, hardware, software, network upgrades, and associated services owned by the Customer.
- 9) Manufacturer warranty parts and labor/services of equipment owned by the Customer.
- 10) Legal use rights to monitor digital credentials.

- 11) For failed server restoration: Customer must have a vendor supported network-based backup solution that produces Full Bare-Metal Recovery Backups (“Proper Backups”).
 - a) In the absence of Proper Backups, Dynamic Quest, will attempt to restore on a best effort basis and at its sole discretion, may bill the recovery time for failed servers as hourly out of scope in accordance with Addendum E (*use this link to go to the Service Description site with the Addendums: https://info.dynamicquest.com/service_description*).
- 12) Customer infrastructure equipment (including switches, Wi-Fi, firewalls, and other similar equipment) must be considered business class equipment and not residential-use equipment AND be a Dynamic Quest support brand and model in Addendum A (*use this link to go to the Service Description site with the Addendums: https://info.dynamicquest.com/service_description*).