

These AI Pentesting Services Terms (the “**AI Pentesting Terms**”) supplement and form part of the Wiz Subscription Agreement or other agreement entered into for Wiz Services (the “**Agreement**”) by and between Wiz and Customer (each as defined in the Agreement) and apply to Customer’s use of the Wiz platform features utilizing AI and automation to conduct active penetration testing and threat actor simulations on Target Assets (the “**AI Pentesting Services**”). For the avoidance of doubt, the AI Pentesting Services are part of the Wiz Services (or other similar term) described in the Agreement. Capitalized terms not defined in these Terms have the meanings given to them in the Agreement. In the event of any conflict between these AI Pentesting Terms and the Agreement, except as set forth herein, these AI Pentesting Terms will control with respect to the AI Pentesting Services unless Customer and Wiz have separately entered into AI Pentesting Terms which expressly states the Parties’ intent to amend the terms set forth herein, in which case Customer’s access to and use of the AI Pentesting Services will be governed by such amended terms. Notwithstanding anything to the contrary, if the AI Pentesting Services are identified as Preview Features within the Platform, the preview terms in the Agreement shall also apply to such AI Pentesting Services and shall govern in the event of any conflict with these AI Pentesting Terms for as long as they remain Preview Features.

1. REPRESENTATIONS AND WARRANTIES.

1.1. Explicit Authorization. By designating specific applications, endpoints, APIs, networks, or other digital infrastructure (the “**Target Assets**”) for scanning via the Platform and providing any required credentials or secrets to Wiz, Customer explicitly directs and authorizes Wiz to perform active security testing using agentic AI solely for the purpose of identifying security vulnerabilities, misconfigurations or other attack paths. Customer acknowledges that active penetration testing is inherently risky. The AI Pentesting Services are designed to simulate real-world attacks, which may cause unintended consequences, including but not limited to: system crashes, performance degradation, service unavailability, application behavioral changes, or data corruption on the Target Assets.

1.2. Backups. Customer is solely responsible for ensuring that full, reliable backups of all data, applications, and configurations residing on or connected to the Target Assets are actively maintained and readily recoverable prior to initiating any AI Pentesting Services scan.

1.3. Credentials. Customer is responsible for providing any credentials or keys required for Wiz to access the Target Assets to the extent necessary, for the performance of the AI Pentesting Services. Customer acknowledges that the AI Pentesting may not function as intended without such credentials or keys.

1.4. Automated Service and Reports. The AI Pentesting Services and the resulting report (the “**AI Pentest Report**”) are automated and AI-generated, without human oversight or manual validation by Wiz personnel, and are provided “AS IS.” Customer acknowledges that the AI Pentest Report may contain false positives, false negatives, or incomplete findings, may not identify all vulnerabilities, and is not, by intended to satisfy Customer’s compliance, regulatory, or certification requirements.

1.5. Ownership and Consent. Customer represents and warrants that it owns, operates, or has obtained all necessary rights, consents, and authorizations from applicable third-party owners to designate each Target Asset for the AI Pentesting Services. Wiz conducts the AI Pentesting Services solely based on Customer’s instructions and designations.

2. INDEMNIFICATION AND LIMITATION OF LIABILITY.

2.1. To the maximum extent permitted by law, Wiz will have no liability, and Customer will defend, indemnify, and hold harmless Wiz from and against any claims, losses, damages, liabilities, or expenses (including reasonable attorneys' fees) arising out of or relating to: (a) Customer's designation of any Target Asset without proper authorization; or (b) any third-party claims alleging unauthorized access, penetration, disruption, or violations of applicable law (including the Computer Fraud and Abuse Act, 18 U.S.C. § 1030, or similar statutory or common law claims) resulting from Wiz accessing or testing such designated Target Assets. Customer's indemnification obligations described herein shall not be subject to any limitation of liability set forth in the Agreement, and shall survive terms with the AI Pentesting Services, except with respect to Wiz's gross negligence, willful misconduct, or breach of its confidentiality obligations under the Agreement, which shall be as agreed by Wiz and Customer under the Agreement.

3. MISCELLANEOUS.

3.1. These AI Pentesting Terms shall become effective upon Customer's use or receipt of the AI Pentesting Services (the "**AI Pentesting Terms Effective Date**") and will survive termination of the Agreement. Wiz may update these AI Pentesting Terms, and such updates will be made available at www.wiz.io/legal/legal-hub (or any successor page(s)). Any updates required to comply with applicable law or address a material security risk, or to Preview Features, shall become effective immediately. All other updates to these AI Pentesting Terms shall become effective for Customer upon the earlier of: (i) the renewal of Customer's then-current Subscription Term; or (ii) upon the effective date of a new Order. Wiz will notify Customer of any material updates to the AI Pentesting Terms if Customer has subscribed to receive such updates via the "**Legal Contact**" within the Platform settings.

The representative signing or accepting these AI Pentesting Terms represents that it has the authority to bind its organization to these AI Pentesting Terms.