# Solutions Terms: Managed Risk

Last Updated: November 1, 2021

These Managed Risk – Solution Terms set forth the terms and conditions of the Managed Risk Solution (the "Solution"). The Solution, if purchased by Customer as evidenced by Customer's election on an Order Form, will be provided in accordance with the terms set forth herein and the Solutions Agreement (the "Agreement") made by and between Customer and Arctic Wolf Networks, Inc. ("Arctic Wolf"). Any capitalized terms not otherwise defined herein shall have the meaning set forth in the Agreement.

**The Solution:**

The Solution provides Customers with security vulnerability analytics and trends in Customer's network and endpoints which assist in the prevention of system attacks.

Specific services included as part of the Solution include:

- Arctic Wolf will provide Customer with internal vulnerability assessment (IVA) through an on-premise Managed Risk scanner. Managed Risk scanners, at the election of Customer at the time of order, may be a deployed as a physical piece of equipment or virtual instance.
- During onboarding, Arctic Wolf will work with Customer to determine Customer's Managed Risk scanner configuration. The scanner, based upon the agreed upon configuration, will scan Customer's network to identify security vulnerabilities within Customer's host and/or network infrastructures.
- Information obtained from the IVA scans will be paired with an external vulnerability assessment ("EVA") function. The EVA will be run from Arctic Wolf's cloud-hosted environment, will scan Customer's IP addresses associated with Customer's organization or such other addresses designated by Customer and for which Customer is legally authorized to scan, and will provide Customer with a comprehensive security risk posture based on an industry-standard and recognized Cybersecurity Framework and Arctic Wolf's proprietary algorithm.
- The EVA function will also be used to scan external network environments for dark web exposures to identify any Customer personally identifiable information that is publicly accessible through the Account Takeover (ATO) capability.
- Customer may elect not to deploy the Arctic Wolf Agent (the "Agent"), proprietary end point software, which will be configured by Arctic Wolf during onboarding as agreed. Use of the Agent allows Arctic Wolf to run local system scans to augment the Solutions Data used to identify security vulnerability analytics, trends in Customer's network and endpoints, scan for system misconfigurations through the security controls benchmarking function, and perform host-based vulnerability assessment scan.
- Customer understands and agrees that Arctic Wolf, in the performance of the Solution, may use a GeoIP service (i.e., a method of locating a computer terminal's geographic location by identifying that terminal's internet protocol ("IP") address) to report the location of Customer's IP address.
- Customer may access and use the Arctic Wolf Analytics platform that aggregates Solutions Data from the Agent and IVA. Analytics will allow Customer the ability to build custom dashboards and reports and will be licensed in accordance with the terms and conditions set forth in the Agreement.

**Data Transfer.** Any Equipment provided by Arctic Wolf to Customer is physically or virtually deployed to monitor Customer's system traffic. Such system traffic is augmented with additional sources of log data, as required, to deliver Managed Detection and Response, if licensed by Customer. All such system traffic information is deemed Solutions Data. Essential log sources will be determined by Arctic Wolf during the onboarding process preceding the Subscription Term Start Date (as defined in an Order Form).

[1] Solutions Data also may be referred to in the Agreement as Customer Data.

Any Solutions Data will be transmitted to Arctic Wolf in accordance with the terms of the Agreement via a secure tunnel in compliance with ISO27001 and SOC 2 Type II. The Solution may be provided redundantly to Customer's high availability (HA) specifications in order to minimize potential service interruptions. Hosting providers used by Arctic Wolf to deliver the Solution may experience service interruptions and service outages outside the control of Arctic Wolf. If such a hosting provider issues an outage notice that could materially impact delivery of the Solutions, Arctic Wolf will use commercially reasonable efforts to promptly notify Customer about the outage and communicate the planned recovery time provided by the hosting provider.

Solutions Data may include personal or confidential information. Customer will provide such personal or confidential information in accordance with the terms of the Agreement.

**Data Storage.** Arctic Wolf will store Solutions Data in the hosting provider location selected by Customer and set forth on an Order Form.

**Additional Modules.** Customers may license Cloud Security Posture Management ("CSPM") for Amazon Web Services (AWS), Microsoft Azure, and any such other cloud and SaaS environments that Arctic Wolf may agree to monitor at a frequency agreed upon with Customer. Customer's election to license such CSPM feature will be set forth on an Order Form. If licensed as part of the Solution, Arctic Wolf will monitor, evaluate, and

track Customer's agreed upon cloud configurations and compare such configurations to best practices to identify possible configuration errors in Customer's environment. Any such errors will be displayed within Customer's dashboard and a report will be provided to Customer outlining any additional details.

**Updates & Upgrades.** Any automated maintenance and update cycles to the Solution will be performed remotely by Arctic Wolf. Arctic Wolf will provide any services related to the replacement or upgrades of the Equipment. Any costs related to such Equipment replacement or upgrades will be in accordance with the Agreement.