Managed Risk

Product Description

Document ID	MR-PD
Document Version	1.3
Last Updated	2025.05

Document Change History

Version	Date	Summary of Changes
1.4	2025.10	Updates to provide structure (versioning, change history) and copyright information. Changes to technology overview to reference, rather than duplicate, content covered in the Arctic Wolf Core Technologies product description.
1.3	2025.05	Minor changes to wording to account for general terms and conditions updates.
1.2	2025.02	Updates to account for the acquisition of the Auora Endpoint Security (fka Blackberry Cylance) products
1.1	2024.11	Addressing terminology inconsistencies with other product description documents
1.0	2024.08	Initial release

Product Description[1]

Arctic Wolf Managed Risk (MR)

Arctic Wolf® MR solution (the "Solution" or "Product") enables you to discover, prioritize, and harden your environment against digital risks by contextualizing your attack surface across networks, endpoints, and cloud environments. The Arctic Wolf Concierge Delivery Model ensures that our purpose-built technology, combined with our extraordinarily talented teams, helps you deliver security outcomes for your organization.

Included with the Solution, you have access to the Unified Portal (formerly known as the Customer Portal), a real-time, web-based self-service application that enables you to configure and tailor the Solution and provides you with insights to the data, risks, vulnerabilities, and tasks related to your security program. Security touchpoints with your Concierge Security® Team (CST) and your Customer Success Manager (CSM) may be included with MR as described herein depending on your subscription. These security touchpoints are designed to provide not only a detailed understanding of current security events and threats, but proactive security hardening guidance to improve the security maturity of your security program overall.

Table of Contents

[1] This Product Description was formerly referred to as the MR Solutions Terms.

Arctic Wolf Technology Overview

In addition to the core technologies offered to all Arctic Wolf solutions that are listed in the Arctic Wolf Core Technologies product description, the below Arctic Wolf Technology Overview sets forth, in general, the Arctic Wolf Technology and the various features and tools that may be included as part of the Solution. The availability and use of any such Arctic Wolf Technology, features, and tools by you is contingent on the specifics of your subscription and reflected in the ordering document (i.e., your Order Form) pertaining to such subscription.

Scanners

Arctic Wolf MR Scanners ("Scanners") and Virtual Scanners ("vScanners") are data collection devices to capture network device identification and vulnerability data associated with your network devices. Scanners and vScanners will be included with your subscription as set forth on your Order Form. Scanners/vScanners are managed, maintained, and updated by Arctic Wolf and include Arctic Wolf's latest vulnerability feeds. For a list of the different Scanners/vScanners, refer to the table below.

Scanner	Description
External Vulnerability Assessment (EVA) Scanner	The EVA scanner is hosted on Arctic Wolf cloud infrastructure. It scans customer-provided, public facing assets such as IP addresses, domains, and cloud accounts (if purchased and configured) by performing port detection (for IPs), DNS scan (for domains), followed by vulnerability scanning on all assets (Account Take Over, Web Application, Vulnerability, and CSPM). The schedule for these scans can be defined within the Unified Portal.
Internal Vulnerability Assessment (IVA) Scanner	The IVA scanner is a physical or virtual appliance deployed in your environment that is managed by Arctic Wolf. The appliance scans your defined targets with host profile and vulnerability scans. The vulnerability scans can be scheduled at times that meet your needs and preferences and may be run monthly, weekly, daily, or continuously. This frequency is configurable on a network-by-network or host-by-host basis. The host profile report enables you to catalogue the assets you have in your environment. The IVA Scanner collects various datapoints using a variety of ever evolving technologies and reports risks found in your environment by running non-credentialed and credentialed

	detections to the extent you elect to configure such detections. Multiple scanners can be deployed to scan distinct parts of your network depending on your environment, size, and preferences.
Account Takeover (ATO) Risk Detection	ATO scanning focuses on known organizational data breach records. The information contains account usernames and passwords. ATO scanning does not focus on the following data sources: • Marketing lists and/or databases — list of employees, which may include their role, title, or department within the organization. • Spam lists — lists of email addresses, corporate, or personal. ATO scanning may include usernames and user passwords for any of your offboarded resources.

The output from the EVA, IVA, and ATO scanning processes will be a comprehensive security risk posture based on an industry standard and recognized Cybersecurity Framework and Arctic Wolf's proprietary algorithm.

Arctic Wolf Agent

The Arctic Wolf Agent ("Agent") is software installed on endpoints and allows Arctic Wolf to run local system scans to augment your telemetry information collected via the Scanners/vScanners and is used to (a) identify security vulnerability analytics, trends in your network and endpoints, (b) scan for system misconfigurations through the security controls benchmarking function, and (c) perform host-based vulnerability assessment scans. The Agent is managed, maintained, and updated four times daily with the latest vulnerability feeds provided by Arctic Wolf. The Agent is capable of self-updating, collecting software and asset inventory data, and sends operational metrics and telemetry to the Security Services Team (comprised of the Security Operations Team (SOC) and the CST), if included with your subscription, for analysis and investigation. The Agent can co-exist with your existing Endpoint Security vendor, but for the best possible service, visibility, and coverage, we recommend that the Agent be deployed to all devices in your environment alongside Sysmon, if your subscription mix warrants.

During the onboarding phase, the Deployment Security Team will assist with the deployment of the Agent at scale within your organization using an appropriate method of deployment such as Microsoft Intune, Microsoft System Center Configuration Manager (SCCM), Jamf, or group policy.

Arctic Wolf Unified Portal

The Arctic Wolf Unified Portal is the self-service application for Arctic Wolf Products, including MR. The Unified Portal is the single point of access to your CST, if included with your subscription.

You can perform the following tasks related to MR within the Unified Portal:

- Get a consolidated view of EVA, IVA, and Agent scan schedules across all risk sources.
- Manage and create IVA and Agent scan schedules.
- Configure IVA Scanner to manage scanner settings, deny list entries, and authenticated scan credentials.

Arctic Wolf MR Workbench

Accessed through the Unified Portal, the Solution includes access to the MR Workbench that provides visibility into the real-time risk landscape on your networks, endpoints, and cloud environments (if purchased and configured). The MR Workbench is a cloud-based portal that is tailored to your organization's priorities to help you make sense of potential vulnerabilities, while also managing and prioritizing patching with the goal of reducing your cyber risk exposure by enabling operational optimization through insights into the prioritization of your information security and technology activities.

For a list of sub-features within MR, refer to the table below.

Feature	Description
Overview of dashboard metrics and health status	Provides visibility into your cybersecurity posture, overall cyber risk score over time, industry comparisons, and asset health.
Management Plan	Lite Gantt chart view where you can create plans, and review progress and deadlines of risk mitigation efforts for risks added into these plans.
Risks	View a catalog of risks with the ability to filter and sift through the list of discovered cyber risks. You can view the following: • Risks and unassigned risks sections • Risk information pane • Risk states

	• Risk statuses • Risk state and status lifecycles • Risks based on an assigned due date • Rescan assets with risks • Active risks • Inactive risks • Mitigated risks • Risks that failed validation • Arctic Wolf Agent vulnerability debug scans You can perform the following tasks: • Assign a user and a due date to a risk • Accept a vulnerability • Edit the state of inactive risks • Edit risks • Unassign a user and a due date from a risk • Download a remediation report • Download risks table data
Assets	View a catalog of assets. You can perform the following tasks: • Assign asset context • Filter assets • View an asset profile • Rescan assets • Review assets • Create an asset tag • Edit assets • Reset sensor details • Remove an asset • Download asset catalog data.
Agent	View risks, assets, and Center for Internet Security (CIS) benchmark data discovered during Agent scans.

External Vulnerabilities Assessment	View a list of configured target groups with risk data discovered during External Vulnerability Assessment (EVA) scans.
Attack Surface Coverage	Provides details about coverage by different scanning technology with target, network capacity, device count, missed, and scheduled targets information.
Scanner configurations	Review operational status of sensors, network, and subnetworks, and a list of hosts enabled for credentialed scanning.
Resources	Provides quick reference links to release notes, and documentation.
Downloads	Provides you with the ability to download a Scanner Virtual Machine image for your virtualization infrastructure.

Arctic Wolf MR Analytics

You can use MR Analytics to view and organize MR and Agent information in your environment. You can view historical data, up to 365 days, to analyze the vulnerability management program. MR Analytics enables you to generate custom dashboards and schedule email delivery to stay updated on changes in your environment. You can use MR Analytics to view raw data tables, refine results to specific subsets of data using filters, aggregate results to answer questions, and combine multiple data views into interactive dashboards.

Cloud Security Posture Management (CSPM)

You may additionally license CSPM for Amazon Web Services (AWS), Microsoft Azure, and any such other cloud and SaaS environments. If included in your subscription, Arctic Wolf will monitor, evaluate, and track your agreed upon cloud configurations and compare such configurations to best practices to identify possible configuration errors in your environment. Any such errors will be displayed within your MR Workbench and a report will be provided to you outlining any additional details.

Security Expertise: Overview of Security Teams

The Arctic Wolf Security Teams engage with you to support your subscriptions and to ensure Arctic Wolf has a complete understanding of your unique IT environment right from the start. Support from the Security Teams is provided remotely.

For a full description of the Arctic Wolf Security Teams and the scope of activities performed by each Security Team across all Arctic Wolf Products, please see the Scope of Service document. The specific scope of activities handled by the pertinent Security Teams related to MR can be found in the MR Solution Overview section below.

MR Solution Overview

This MR Solution Overview sets forth, in general, the Solution delivery process that is offered. The specific details pertaining to any of the phases below is dependent upon the specifics of your subscription as reflected in your Order Form.

If your subscription includes a Concierge Security Tier (CST Tier), your CSTs involvement and participation in the Solution will include activities as set forth in the "MR Activities" section below as enhanced by the specifics of the CST Tier selected by you in your subscription. If your subscription does not include a CST Tier, CST is not included as part of the MR Activities described below and any assistance with the Solution will include the support set forth in the "Technical Support" section below.

MR Activities

Discover

Risk Monitoring

Monitors for vulnerabilities, system misconfigurations, and account takeover exposure across your endpoints, networks, and cloud environments, to the extent licensed and configured.

Risk Prioritization

Security observations are enriched with digital risk information to add greater context, quantify your exposure, and prioritize actions.

Asset Discovery

The solution continuously maps, profiles, and classifies assets on your network to help you understand your attack surface.

Assess

Configuration Benchmarking

Reveal configuration errors and drift over time that are invisible to most vulnerability assessment and management tools.

Risk Scoring

Presents a quantified view of digital risks that exist in your environment weighted based on severity and benchmarked against peers to track the progress of your remediation efforts.

Actionable Reporting

Automated and exportable risk score trends, action lists, executive summary, and risk assessment reports that summarize risk exposure in consumable, shareable formats to help you prioritize actions that harden your environment.

Harden

Guided Remediation

If available with your subscription, the CST provides you with guided personalized risk remediation and validation to assess whether the vulnerability has been successfully remediated, while also enabling you to determine if the vulnerability is still present in your environment.

On-Demand Reporting

Through the Unified Portal you may be able to create and configure dashboard-based reports to showcase the data visualizations important to you. Upon request, the CST may assist with the creation of these reports or generate ad-hoc reports with rich charts and dashboards for meeting compliance needs or provide on-demand executive reporting to support you in gaining the visibility of vulnerabilities and assist with closing gaps.

Strategic Recommendations

If included with your subscription, the CST's goal is to become your trusted security advisor, working with you to make recommendations that harden your security posture over time. Arctic Wolf Labs may be leveraged by your CST during your subscription to provide you with the latest emerging threat intelligence on vulnerabilities with reliable and actionable information.

Solution Delivery Phases

Process

There are four phases that the Solution covers to ensure it can be leveraged to effectively discover, prioritize, act, and report on your cybersecurity risks.

Phase	Details
Deployment phase	The Deployment Security Team (DST) will work with you to deploy the Arctic Wolf platform, integrate critical data points, and build an understanding of your network. **Installation and Integration** DST starts with the essential task of identifying assets in your environment and defining your attack surface across network, perimeter, host, and accounts. Arctic Wolf configures and validates the environment, and makes reports available for the internal, external, and agent-based scanners, as well as CSPM (if purchased).
Configuration phase	Throughout the deployment phase, DST will continue to gain a clear understanding of and visibility into your attack surface by establishing asset context and a vulnerability baseline. **Concierge Kick-Off** If applicable to your subscription, Concierge kick-off is when your CST will begin the proactive MR security process. The CST contextualizes your attack surface with definition and identification of your internal IT practices and requirements, including asset criticalities, policies, procedures, patching cycles, and your service level objectives (SLOs), enabling you to prepare your environment to end cyber risk. Once this information has been collected, the CST assesses and provides you with your documented risk priorities within your environment. **Identity and Coverage Resolution** CST delivers your overall vulnerability management program context, providing insight on your current device and network

	coverage, as well as identity issues within your environment. CST will provide recommendations to fix any identified coverage issues and ensure coverage of your desired attack surface is covered by the Solution. **Define and Configure Asset Context** The Arctic Wolf platform provides an initial critical asset list. This list is reviewed with you to identify any gaps. We then recommend asset criticalities, workflow, and organization tagging to make your environment more contextualized. **Threat Landscape and Prioritization Review** The Solution provides you with tailored risk prioritization according to asset and risk context on your overall attack surface so you can begin patch management.
Active Cycle phase	**Active Cycle phase** The Active Cycle phase centers on vulnerabilities and is a steady state and continuous cycle. The goal of the Active Cycle is to ensure proper coverage of your environment, provide surface information that will aid the prioritization of risks, provide consultation to you as you harden your environment (if included with your subscription), and ensure your risk mitigation efforts are successful. The goal is accomplished through the following four sub-phases that are continuously cycled through: **Discover** Identify differences between the initial or previous asset baseline to understand your attack surface. **Assess** Obtain risk metrics and prioritized list of risks and their descriptions through the MR Workbench and/or Unified Portal to gain a clear understanding of prioritization of risks and to support assignment to an appropriate mitigation team.

	Harden With CST's support, if included, resolve prioritized risks and manage and mitigate overall cyber risk, ensuring you benchmark against configuration best practices and continually harden your security posture. **Validation** Review progress made towards overall cyber risk mitigation by rescanning such risks to ensure efforts were successful.
Decommissioning phase	Decommissioning is the process of removing MR from your organization's environment and your organization's data from the Arctic Wolf environment.

Technical Support Options

You can contact Arctic Wolf for assistance at 888-272-8429 x2 or the toll-free number found at https://arcticwolf.com/toll-free/ for your location. You may also access the Arctic Wolf Support Center via email at support@arcticwolf.com. If Arctic Wolf's hosting provider(s) issue an outage notice that could materially impact delivery of the Solutions, Arctic Wolf will use commercially reasonable efforts to promptly notify you about the outage and communicate the planned recovery time provided by the hosting provider.

Roles and Responsibilities

To ensure that full value of the Solution is received, each party's roles and responsibilities are defined in the table below.

Activity	Arctic Wolf	Customer
Deployment		
Install Scanners/vScanners		X
Scanner/vScanner configuration recommendations	X	
Configure Scanners/vScanners		X
Provide credentials for internal vulnerability scanning		X

Provide IP and domain targets for external vulnerability scanning		X
Provide domain targets for Account Takeover (ATO) scanning		X
Create a defined outbound security rule from your scanner IP address to all necessary Scanner IP addresses		X
Discover and deduplicate assets	X	
Assign asset criticality and tag assets	X	
Verify assigned asset criticality and tags		X
Configuration of owned network or host devices		X
Ongoing		
Enumerate vulnerabilities	X	
Patch systems showing vulnerabilities		X
Platform prioritized risks	X	
Remediation and mitigation of the risks		X
Verification of remediation activities	X	
Monitoring and alerting	X	
If ATO targets are configured, alert on high and critical severity breaches	X	
Metrics and reporting	X	
Update and maintain scanners	X	
Troubleshoot scanning MR technologies for issues and coverage	X	