Company Overview

AT A GLANCE

FOUNDED:

2012

EMEA HEADQUARTERS:

Newcastle upon Tyne, UK

GLOBAL CUSTOMERS:

10,000+

SOLUTIONS:

- **Endpoint Security**
- **Managed Detection and Response**
- **Managed Risk**
- **Managed Security Awareness®**
- **Incident Response**

AWARDS

CNBC DISRUPTOR 50

Great Place To Work. Certified JUL 2024-JUL 2025 UK

500 Technology Fast 500 2024 NORTH AMERICA 30 YEARS OF INNOVATION Deloitte. WINNER

Gartner Peer Insights Customers' Choice 2024

THE CHANNEL CO. CRN PRODUCTS OF THE YEAR 2024

The Importance of Security Operations Solutions

Arctic Wolf ends our customers' cyber risk by making security work. Our unique approach to security operations combines purpose-built technology, security expertise, and risk transfer solutions to achieve the security outcomes our customers are striving for at an unprecedented scale.

Organisations Face Fundamental Security Challenges

TOO MUCH NOISE

Alert fatigue, tool fatigue, and compliance and regulation fatigue — the journey never ends

SECURITY SKILLS SHORTAGE

Recruiting and retaining cybersecurity talent is hard, sometimes impossible

COST OF RESPONSE TIME

The longer it takes to respond to an incident, the more expensive it is to remediate

Arctic Wolf Security Operations

Arctic Wolf® is a global leader in security operations, delivering the first cloud-native security operations platform to end cyber risk. Built on open XDR architecture, the Arctic Wolf Aurora™ Platform operates at a massive scale and combines the power of artificial intelligence with world-class security experts to provide 24x7 monitoring, detection, response, and risk management. We make security work.

THE LEADER IN SECURITY OPERATIONS

The Arctic Wolf Aurora Platform

SOLUTIONS

Endpoint Security

AI-driven prevention, detection, and response to stop endpoint threats before they disrupt your business.

Managed Detection and Response

Quickly detect, respond, and recover from advanced threats.

Managed Risk

Discover, assess, and harden your environment against digital risks.

Managed Security Awareness

Engage and prepare employees to recognise and neutralise social engineering attacks.

Incident Response

Recover quickly from cyber attacks and breaches, from threat containment to business restoration.

DATASHEET

Arctic Wolf® Managed Risk

Reduce Risk, Increase Resilience

Organizations everywhere struggle with the complexity of identifying and managing security risks within their environment. Often, even fundamental information like what assets exist, which systems have vulnerabilities, and which systems are misconfigured is difficult to obtain. Even when this information is available it usually overwhelms the security team because their existing tools generate too many alerts and lack context. As security teams struggle with what to do next and how to prioritize, these risks pile up and leave organizations vulnerable to threats and damaging data breaches.

> ***"By 2026, organizations prioritizing their security investments based on a continuous exposure management programme will be three times less likely to suffer from a breach."***
>
> — *Jeremy D'Hoinne, Implement a Continuous Threat Exposure Management (CTEM) Program - Published 21 July 2022 - ID: G00763954*

Built on the industry's only cloud-native platform to deliver security operations as a concierge service, Arctic Wolf Managed Risk enables you to define and contextualize your attack surface coverage across your networks, endpoints, and cloud environments; provides you with the risk priorities in your environment; and advises you on your remediation actions to ensure that you benchmark against configuration best practices and continually harden your security posture.

Discover

The ability to discover and gain visibility into your current attack surface.

- Attack surface coverage
- Dynamic asset discovery
- Account takeover risk detection

Prioritize

Determine your cyber risk in the context of your business.

- Classification and contextualization
- Risk scoring
- Concierge-led prioritization

Harden

Expertise to guide your strategy and help you harden your environment.

- Configuration benchmarking
- On-demand reporting
- Guided remediation

Concierge Security® Team

The Concierge Security Team (CST) is your single point of contact for your Arctic Wolf Managed Risk solution. Your CST intimately learns your environment and then develops a Security Journey based on your security objectives, hardening your security posture and helping to tune your environment.

24x7 Monitoring

Around-the-clock monitoring for vulnerabilities, system misconfigurations, and account takeover exposure across your endpoints, networks, and cloud environments. Deliver timely critical outcomes with the deep scan tools.

Unified Visibility

Gain greater insight into your security posture and broader visibility into your attack surface by pairing the detection and response of MDR with the risk-based vulnerability management provided through Managed Risk for proactive improvements as well as faster remediation.

Strategic Recommendations

Your named security operations expert becomes your trusted security advisor, working with you to make recommendations that harden your security posture over time.

Personalized Engagement

Regular meetings with your named security operations expert let you review your overall security posture and find areas of improvement that are optimized for your environment.

- Scans your environment for digital risks
- Performs regular risk posture reviews
- Provides actionable remediation guidance
- Works with you to build risk management plans
- Delivers a customized risk management plan to prioritize remediation and measure progress
- Provides comprehensive visibility into your risk posture

Arctic Wolf Managed Risk Capabilities

External Vulnerability Assessment

Scans internet-facing assets to understand your company's digital footprint and quantify your business's risk exposure. Key features include:

- Scanning of external-facing assets
- Cloud Security Posture Management (CSPM)
- Account takeover risk detection
- OWASP Top 10 scanning
- Automated sub-domain detection

Internal Vulnerability Assessment

Continuously scans all your internal IP-connected devices while cataloging your core infrastructure, equipment/peripherals, workstations, Internet of things (IoT) devices, and personal (e.g., tablets, cell phones) devices. Key features include:

- Continuous scanning of internal assets
- Proactive risk monitoring
- Stateless scanning and secure transfers

Host-Based Vulnerability Assessment

This capability extends visibility inside devices through continuous host-based monitoring to identify and categorize assets, as well as reveal system misconfigurations, user behaviors, and vulnerabilities that put your organization at risk. Key features include:

- Endpoint agents for Windows Server/workstation, MacOS, and Linux distributions
- Proactive endpoint risk monitoring
- Audit reporting
- Security controls benchmarking

Quantify Your Cyber Risk Posture

A cloud-based portal provides visibility into continuous cyber risk assessment by incorporating all meaningful cyber risk indicators from your business. It identifies the highest-priority issues and alerts you to emerging risks before they escalate into real problems. It empowers you to take meaningful, efficient action to mitigate risk using these key features:

- Comprehensive risk profiling
- Informative user interface
- Proactive notifications and alerts
- Actionable reporting
- API integrations

Security Risk Scoring

For effective risk management, you need to know if your security posture improves or declines over time. Benchmarking against other organizations in similar industries helps you understand where you stand and how to improve.

Configuration Benchmarking

To help you prioritize your risk mitigation, configuration benchmarking is a risk score based on criteria such as the attack vector accessibility, attack complexity, and the impact of accessed data. These benchmarks provide context so you can address the most critical misconfigurations first.

"Having a team to assess and manage vulnerabilities while monitoring our environment really helps us reduce our threat surface. We've made considerable progress in rebuilding integrity and trust in our IT systems, but risk never goes away — and if we aren't aware of it, we can't work to mitigate it."

— Dr. Jason A. Thomas, Chief Operating Officer and Chief Information Officer, Jackson Parish Hospital

JACKSON PARISH HOSPITAL

Managed Risk

Product Description

Document ID	MR-PD
Document Version	1.3
Last Updated	2025.05

Arctic Wolf Managed Risk Capabilities (continued)

Account Takeover Risk Detection

By continuously scanning the dark and gray web for corporate credentials harvested in data breaches, account takeover detection enables you to quickly take action to secure compromised accounts. Typically, your solution partner provides details such as the source, description of the data breach involved, and the exposed emails.

Cloud Security Posture Management (CSPM) Add-On

A solution that protects against misconfigurations, mismanagement, and other mistakes occurring in cloud infrastructure, CSPM includes prevention, detection, and response capabilities based on criteria such as security frameworks, IT policies, and regulatory compliance.

Asset Inventory

Your attack surface constantly changes as you add more users and hosts. To build and maintain a comprehensive inventory of assets, dynamic asset identification profiles and classifies your IT assets automatically and continuously so that no new asset falls through the cracks.

Asset Tagging

Managed risk allows you to gain additional asset context of your risk prioritization efforts, assisting with asset classification and asset organization efforts. You can use asset tags to pivot and review assets as well as your risks during your risk management and hardening efforts. It makes the automation of managing assets possible, makes reports more meaningful for the business, and improves risk prioritization efforts.

Asset Criticality

Assigning an asset a level of criticality as an attribute for risk prioritization provides a standardized critical labeling system with a clear definition of the asset's importance. The level of asset criticality can be critical, high, medium, low, or unassigned.

Risk Remediation Steps

Managed Risk allows you to export a report with remediation resources against your risk, vulnerabilities, and assets. By including the remediation steps alongside the vulnerabilities, you can efficiently — and consistently — remediate known risks.

About Arctic Wolf

Arctic Wolf® is a global leader in security operations, enabling customers to manage their cyber risk via a premier cloud-native security operations platform. The Arctic Wolf Aurora Platform ingests and analyzes more than eight trillion security events a week to help enable cyber defense at an unprecedented capacity and scale, empowering customers of virtually any size across a wide range of industries to feel confident in their security posture, readiness, and long-term resilience. By delivering automated threat protection, response, and remediation capabilities, Arctic Wolf delivers world-class security operations with the push of a button.

For more information about Arctic Wolf, visit **arcticwolf.com**.

ARCTIC WOLF

SOC2 Type II Certified

AICPA SOC

ISO 27001 CERTIFIED
CYBERGUARD COMPLIANCE

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	