Managed Endpoint Defense

Product Description

Document ID	MED-PD
Document Version	1.4
Last Updated	2025.10

Document Change History

Version	Date	Summary of Changes
1.4	2025.10	Minor changes to incorporate MSP language and roles and responsibilities. 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.
1.0	2025.02	Initial release

Product Description

Arctic Wolf Aurora Managed Endpoint Defense (MED)

The Arctic Wolf Aurora Managed Endpoint Defense (MED) Solution provides a 24x7x365 managed endpoint detection and response offering in which Arctic Wolf SOC analysts monitor and manage Customer threats using Aurora Endpoint Defense (including email and web interactions) and closed-loop communications with direct phone access to Arctic Wolf SOC analysts. Arctic Wolf SOC analysts help Customer navigate incidents and provide regular updates on overall threat prevention status, analyzing and responding to data log feeds from Aurora Protect and Aurora Endpoint Defense, and provide regular reporting access through the Portal.

Table of Contents

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 MED Solution. The availability and use of any such Arctic Wolf Technology, features, and tools by you is dependent upon the specifics of your subscription and reflected in an ordering document (i.e., Order Form).

Aurora Protect

Arctic Wolf Aurora Protect is a next-generation AI-driven endpoint protection solution designed to prevent malware and ransomware attacks before they execute. Originally known as Cylance PROTECT, Aurora Protect delivers autonomous threat prevention without relying on traditional signatures or frequent updates. By leveraging a machine learning engine trained on billions of file features, it stops known and unknown threats with high efficacy and low system impact.

Aurora Protect provides organizations with:

- **Preventive Security at the Endpoint**: Stops malicious executables, scripts, and exploits before they run.
- **Autonomous Protection**: Works online or offline, with minimal need for cloud lookups or user interaction.
- **Low Operational Overhead**: Reduces alert noise and eliminates the need for frequent signature updates or definition management.
- **Consistent Protection Across Operating Systems**: Supports major desktop and server OSes including Windows, macOS, and Linux distributions.
- **Seamless Integration with Arctic Wolf's Security Operations** (where applicable): Enabling threat correlation, enriched response actions, and better context when used alongside other Arctic Wolf offerings.

Aurora Endpoint Defense

Aurora Endpoint Defense builds on the capabilities outlined in *Aurora Protect*, combining AI-powered prevention with endpoint detection and response. In addition to machine learning-based malware prevention and layered controls, AED leverages the Aurora Focus Agent to provide behavioral threat detection, telemetry collection, and response actions—enabling organizations to detect, investigate, and respond to threats from a single interface.

Aurora Focus Agent

The Aurora Focus Agent enhances endpoint protection with autonomous detection, investigation, and response—executed directly on the device. It continuously monitors system activity, applies behavioral detection logic locally, and enforces automated responses without relying on cloud connectivity. Operating alongside the Aurora Protect Agent as part of Aurora Endpoint Defense, it delivers rich telemetry and actionable insights in real time, even in offline or low-connectivity environments.

Note: *Some capabilities may not be available in all versions of the Aurora Focus Agent or on all supported operating systems. Refer to the product documentation for a complete understanding of these dependencies.*

Behavioral Threat Detection

Identifies malicious activity based on suspicious behaviors, tactics, and execution flows—without relying on traditional IOCs or signatures.

Continuous Endpoint Telemetry

Captures detailed telemetry on the endpoint to support investigations, threat hunting, and retrospective analysis by monitoring the following event types:

- Application
- Device
- File
- Memory
- Network
- Process
- Registry
- Scripting
- SharedObjects
- System
- Threat
- User

Note: *Available sensors may vary based on Agent version, platform, and platform version. Check product documentation for your configuration.*

Local Detection and Policy Response

Executes detection logic locally and enforces automated responses such as process termination, file deletion, or user logoff based on defined policies.

Hunting and Investigation Support

Enables security teams to explore endpoint activity, trace attack paths, and validate threats using high-fidelity data enriched with context.

Integrated Response Capabilities

Allows rapid remediation actions—including isolating hosts or applying custom remediation scripts—without requiring third-party tooling.

Data Retention

Arctic Wolf's Endpoint defense standard log retention is thirty (30) days

Arctic Wolf Portals

Managed Endpoint Defense Workbench

The Arctic Wolf Managed Endpoint Defense Workbench is a self-service tool, that can be accessed stand-alone or via the Arctic Wolf Unified Portal, that provides a single point of access to your licensed Aurora Endpoint Security Solutions and a channel to collaborate with your Security Team.

As part of Aurora Managed Endpoint Defense, the Workbench allows you to perform the following tasks:

- View Security Alerts (aka Escalations)
- View configuration health score and details on the configurations
- Access dashboards and reports
- Update contacts
- Manage permissions, and organizational profile information.
- Manage Aurora Endpoint Defense security policy as described in the Aurora Endpoint Defense Product Description Document.

We have two primary interfaces for Aurora Endpoint Security:

1. Managed Endpoint Defense Workbench, will have all the features above for single tenant customers
2. Multi-Tenant Managed Endpoint Defense Workbench, will have all the features above for multi-tenant customers (e.g. MSP Partners, Conglomerates). Multi-Tenant customers will have a consolidated view for its own tenant and all affiliated sub-tenants including Security Alerts (aka Escalations) health score, and dashboards.

Incident Escalation Paths and Workflow

Escalation paths and policies include details to tell the Security Team who should be contacted within your organization, in the event of a Security Incident or Emergency.

You are encouraged to have at least two escalation paths defined and your Deployment Security Team (DST) will help you navigate the right escalation processes for your organization during onboarding. There are no limits to the number of escalation paths that you can define.

Escalation policies may support different escalation paths based on incident type or severity – for example, all Critical incidents can be routed to one contact, while all Medium and Low incidents can be routed to another.

Managed Endpoint Defense Workbench provides a workflow for you to collaborate on an ongoing incident investigation. The workflow will provide the following:

- Incidents summary and details
- Customer validation for normal and unnormal system behavior
- Chat panel Arctic Wolf SOC team
- Recommended Actions, actions recommended by Arctic Wolf SOC team to remediate the incident, or post incident recommended actions to improve your security posture, and reduce the risk of repeating the same incident, such as enforcing str9nger password policy, or have better access control on systems.

Security Expertise: Overview of Security Teams

The Arctic Wolf Security Teams engage with you remotely to support your use of the Solutions and ensure Arctic Wolf has a complete understanding of your unique IT environment. For a full description of the Arctic Wolf Security Teams and the scope of activities performed by each team across all Arctic Wolf Products, please see the Scope of Service document (here). The specific scope of activities handled by the Security Teams related to MED can be found in the MED Solution Overview section below.

MED Solution Overview

If your subscription includes a CST Tier, your CSTs involvement and participation in the Solution will be enhanced in accordance with the specifics of the CST Tier selected by you for your subscription. The following may be included with your MED subscription:

- Solution Management – Arctic Wolf may manage policy settings within the Solution to facilitate better detection and response readiness.

- Endpoint[1] Detection and Response – Alerts generated by security events from the Solution will be detected, triaged, researched, and responded to in accordance with the approved actions.
- Threat Hunting, Reporting, and Advisory Services – See descriptions below.

Working with Arctic Wolf Security Services

During your subscription term, you may regularly engage with your Security Team. The level of interaction with your Security Team will be based on your subscription and, if applicable, Tier. These teams are available to answer questions about MED, guide you on your Security Journey, and work with you to enhance your security posture.

The SOC is available 24x7x365. To contact them, call 1-888-272-8429 ext. 2 or email security@arcticwolf.com. If you are calling from outside of North America, toll-free numbers can be found here: https://arcticwolf.com/toll-free/. For all customers, the members of Security Team outside the SOC, also known as Concierge Security Team, ThreatZero, or Endpoint Specialists depending on which Arctic Wolf Solutions you have, is available Monday through Friday from 8:00 a.m. - 5:00 p.m. in the time zone within which they are located.

Note: *Arctic Wolf's third-party hosting providers 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 Solution, 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.*

Solution Delivery Response Times

All actions referred to below will be made by Arctic Wolf Security Services.

All Security Incidents are assigned a severity level[2] as follows:

Severity Level	Description	Example
Urgent	An active threat requiring immediate action. Incidents of this severity pose a high risk of data loss, service disruption, or significant financial/legal consequences.	• Ransomware attack encrypting large portions of critical infrastructure • Zero-day Exploit

[1] "Endpoints" means wireless devices, desktops, computer systems and any other endpoints with which the Solution operates.
[2] Arctic Wolf reserves the right to adjust the severity of a given Security Incident at our discretion.

Severity Level	Description	Example
		• Massive Data Exfiltration
High	A considerable threat that could lead to significant compromise or disruption if left unaddressed. Incidents of this severity require immediate attention.	• Malware/Botnet Detected • HTTP Download of Malicious Payload
Medium	Security Incidents with this severity level generally involve a security vulnerability or suspicious activity that may require attention.	• Individual host or Widespread targeting but no sign of compromise
Low	Security Incidents with this severity level involve security posture issues with low impact or benign activities that don't pose a significant threat.	• Individual host or non-critical user

The response time service levels for the specified inquiries, Security Incidents, and Emergencies are as follows:

Action	Service Level
Acknowledgement of any schedule request submitted by you to security@arcticwolf.com	One (1) hour from receipt of request.
Acknowledgement of receipt of any Security Incident (inbound) submitted by you to security@arcticwolf.com	One (1) hour from receipt of request; Security Services will follow up with you with an estimate of response time determined by scope, size, and urgency.
Notification and escalation of any Security Incidents (outbound notice)	Two (2) hours of Arctic Wolf's discovery.
Escalation of any Emergency (outbound notice)	Thirty (30) minutes of Arctic Wolf's discovery.

Action	Service Level
Emergency escalated via phone to the SOC (inbound notice)	Arctic Wolf will respond within five (5) minutes; you will be required to describe the Emergency. In the unlikely event that your call goes to Voice Mail, the caller must leave a message to receive a reply.

Emergencies generally include any Urgent Severity Security Incident and other Severity Security Incidents at the discretion of the analyst that could cause degradation or an outage to your systems and infrastructure.

Arctic Wolf's standard Security Incident (as defined below) notification process is through a ticket to your administrator(s); however, we may agree to alternate notification processes. Security Incident notifications will include a description of the Security Incident, the level of exposure, and a suggested remediation strategy.

Note:

- *Solution delivery, including specifically, notification of Emergencies or Security Incidents, will commence once deployment is complete*.
- *Remediation services for Security Incidents, the re-imaging of your systems, or change of policy settings is outside the scope of MDR*.

Escalation Paths and Policies

Escalation paths and policies include details to tell the SOC and CST who should be contacted within your organization, in the event of a Security Incident or Emergency.

You are encouraged to have at least two escalation paths defined and your Deployment Security Team (DST) will help you navigate the right escalation processes for your organization during onboarding. There are no limits to the number of escalation paths that you can define, and you can change, add, or remove them via self-service in the Unified Portal or by collaborating with your CST following onboarding.

Escalation policies may support different escalation paths based on incident type – for example, all endpoint incidents can be routed to one contact, while all email incidents can be routed to another.

Escalation policies support multi-tenant environments. A parent customer can customize the polices and limit escalations to its own members or extend it to some or all sub-tenants its affiliated with.

Response Action Policies

Response Action policies tell the SOC and your CST, if applicable, when they can contain or action on an identified threat. As part of MED, Arctic Wolf will use reasonable efforts to perform Response Actions which include, but are not limited to, the following:

Response Actions	Description
Application Logs	The agent logs detection events to the Windows application log.
Delete Files	The agent permanently deletes any file artifacts that are identified as an artifact of interest (AOI).
Delete Registry Keys	The agent permanently deletes the entire registry key of any AOI that are identified as registry artifacts.
Delete Registry Values	The agent permanently deletes the registry value of any AOI that are identified as registry artifacts.
Dump Detection to Disk	The agent creates a detection data file in the Aurora Endpoint Defense application data directory.
Log Off All Users	The agent logs off all interactive and remote users.
Log Off Users	The agent logs off the specified users.
Log Off Interactive Users	The agent logs off all users that are currently physically interacting with the device.
Log Off Remote Users	The agent logs off all users that currently have a remote session established on the system.
Notification Window	The agent displays a notification window with the detection notification message that you specified, using the native OS notification box instead of the Aurora Protect agent.
Suspend Processes	The agent suspends any process artifacts that are identified as an AOI.

Response Actions	Description
Suspend Process Trees	The agent suspends the entire process tree of any process artifacts that are identified as an AOI. The AOI is treated as the root of the tree
Terminate Processes	The agent terminates any process artifacts that are identified as an AOI.
Terminate Process Trees	The agent terminates the entire process tree of any process artifacts that are identified as an AOI. The AOI is treated as the root of the tree.
Whitelist Processes	This option excludes the specified processes from being observed by Aurora Focus.
Remote Access for Custom Actions	Remote connection to Endpoint for custom actions (subject to customer approval)

The default Response Action policy is “always enable Response Actions” to allow the Arctic Wolf SOC to stop threats and threat actors, minimizing the impact of a Security Incident. Your DST (during onboarding) and your CST (after deployment) can help you document the Response Actions policy that is best for your organization.

Based on (i) the information you provide to your CST following deployment, (ii) a mutually agreed upon escalation policy, the SOC may remotely isolate your endpoint device(s) that show evidence of compromise or other suspicious activity. When the Security Services Team identifies certain indicators of attack on an endpoint the Response Action will be initiated in accordance with the agreed upon escalation policy to rapidly quarantine the suspected compromised system or account.

The indicators of attack that may drive Response Actions include those relating to ransomware (and other types of malware), malicious command-and-control (C2) activity, or active data exfiltration attempts.

The endpoints participating in the Response Actions will receive a notification and the Response Actions will be detailed in an incident ticket. The Security Services Team is available to you to answer questions or provide detailed information on any endpoints participating in the Response Action.

In multi-tenant environment, response actions can be customized per tenant or globally across all tenants.

Incident Investigation, Notification, and Guided Remediation

Security Investigations and Security Incidents

The telemetry data (defined as "Solutions Data" in our Privacy Notice) accepted and ingested by Arctic Wolf that is deemed critical and/or is interesting and relevant from a security perspective, may prompt further analysis by the Arctic Wolf Platform and/or a member of the SOC– this is called a Security Investigation. During the Security Investigation, the SOC may collaborate with you to do further investigation, detail Response Actions, remediate the discovered issue(s), and/or provide a detailed report of the Security Investigation – if these events occur, we identify this as a Security Incident.

You may also request that Arctic Wolf conduct a Security Investigation for data and/or situations that Arctic Wolf does not deem critical and/or interesting and relevant. As part of any Security Investigation, Arctic Wolf will:

- Provide validation of a Security Incident as detected through the Arctic Wolf Platform.
- Participate in calls with your in-house and/or third-party incident response team.
- Provide findings of data captured pertaining to the Security Incident within the Arctic Wolf Platform.
- Provide a report of findings for the Security Investigation upon request.
- Provide recommendations, documentation, and best practices relevant to the Security Investigation.

Notification

The Arctic Wolf SOC is responsible for notifying you of discovered Security Incidents.

The SOC's notification process is done through a security alert ticket via our ticketing system to you, as specified in the escalation paths you have in place within your escalation policies. In the case of an emergency the SOC will also attempt to call customer contacts in priority order and will leave voice mails if necessary.

Security Incident notifications will/may include a description of the Security Incident, the level of exposure, any actions taken prior to the notification, and the suggested remediation steps remaining.

Notifications service is supported in multi-tenant environments. A parent customer can customize notifications and limit it to its own members or extend it to some or all sub-tenants its affiliated with.

Guided Remediation

The Arctic Wolf SOC and other members of your Arctic Wolf security team, if applicable, will provide remediation guidance to return your environment to operational status if there is a compromise (e.g., by providing action-oriented guided remediation instructions that you can perform). A typical example of guided remediation would include written or verbal instruction delivered via a security alert or via a call, to remove such malicious applications as persistence mechanisms or malware. If you should require further assistance, you may separately engage Arctic Wolf's Incident Response Team, subject to the terms and scope in an agreed upon statement of work (SOW).

Threat Hunting

Arctic Wolf will, on an ongoing basis, collect artifacts and information within the Customer's environment to facilitate hunting of potential security threats. Should a security threat be identified, Arctic Wolf will inform you of these findings.

Reporting

Through the Arctic Wolf Portal, you have access to several pre-defined dashboards as well as the ability to create new dashboards to surface data appropriately for your business. In addition, and if necessary, your CST, if appropriate, may assist in the creation of other regular reports.

The reports will either be automatically generated and sent to you by the Solution, created and reviewed by your CST and issued to you, or available in the Arctic Wolf Portal as a PDF or as a live dashboard.

Advisory Services

The Advisory Services program is a software maintenance service of Aurora Managed Endpoint Defense, and Aurora Endpoint Defense technologies for Customers that have already completed Onboarding Services. The Advisory Services program builds off the Onboarding Services to assist customers in achieving optimal configuration and security benefits. The objective of the Project is to report, assess, and review the existing configuration and status of Aurora Managed Endpoint Defense, and Aurora Endpoint Defense solutions. The service is delivered on a quarterly basis presenting the Health Check Report.

The findings of the Health Check Report are the focus of this service. In cases where the Health Check Report classifies Customer as being in good standing, the Arctic Wolf team will seek to identify additional areas to enhance Customer's security posture by performing auditing or additional training. In cases where the Health Check Report

classifies Customer as not in good standing, the Arctic Wolf team will identify areas of noncompliance with or deviations to the Arctic Wolf acceptable security configuration settings, and any other recommendations to assist Customer in optimizing Aurora Endpoint Defense.

Advisory Services include one (1) or more of the following, as determined between Customer and Arctic Wolf during quarterly check-ins:

- Health Check Review
  - Report card review with associated recommendations to identify drift from or deviations to Arctic Wolf acceptable security configuration settings
- Advanced Settings, Audit, and Recommendations
  - Audit and recommendations
  - Upgrade recommendations and guidance
- Additional Training
  - Additional training on new features, best practices, and maintenance routines
  - Working session(s) for questions and answers regarding Customer-driven use cases

Roles and Responsibilities

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

Customer

Activity	Arctic Wolf	Customer
Deployment		
Agent installation		X
Policy Tuning	X	
Escalation path purpose communication	X	
Escalation path definitions		X
Response policy definitions		X
Restricted countries definition		X

Activity	Arctic Wolf	Customer
Select opt-in alerts		X
Site configuration		X
Contacts definition		X
Ongoing		
Response Actions configuration	X	X
Initiate and conduct Response Action(s)	X	
Provide guided remediation	X	
Enact remediation recommendations		X
Alert Escalation-remediation		X
Alert tuning	X	
Alert suppressions	X	X
Custom Detections configuration and remediation	X	X
Maintain Endpoint configuration health and protection coverage	X	X

MSP Partner

Activity	Arctic Wolf	MSP Partner
Deployment		
Agent installation		X
Policy Tuning		X
Escalation path purpose communication	X	
Escalation path definitions		X
Response policy definitions		X
Restricted countries definition		X
Select opt-in alerts		X
Site configuration		X

Contacts definition		X
Tenant Validation	X	
Ongoing		
Response Actions configuration	X	X
Initiate and conduct Response Action(s)	X	
Provide guided remediation	X	
Enact remediation recommendations		X
Alert Escalation remediation		X
Alert tuning	X	
Alert suppressions	X	X
Custom Detections configuration and remediation	X	X
Maintain Endpoint configuration health and protection coverage	X	X