Product Description[1]

Arctic Wolf Aurora Endpoint[2] Defense (AED)

Arctic Wolf Aurora Endpoint Defense (AED) combines the robust prevention capabilities of Aurora Protect (AP)[3] with advanced endpoint detection and response (EDR) to deliver a comprehensive, AI-driven solution for modern endpoint security.

AED includes all the autonomous, signature-less prevention capabilities outlined in Aurora Protect, formerly CylancePROTECT, and extends them with powerful detection, investigation, and response capabilities through the Aurora Focus agent, formerly CylanceOPTICS, under a unified platform.

With AED, organizations benefit from:

- **Prevention + Detection in One Solution**: AED integrates prevention and detection in a single solution, reducing complexity while expanding visibility into endpoint activity.
- **Autonomous, AI-Driven Protection**: Leverages machine learning to stop malware before execution with additional behavioral analysis and attack context to identify emerging threats.
- **Behavioral Detection and Telemetry**: Adds EDR functionality, enabling detection of living-off-the-land (LotL) techniques, suspicious process chains, and unauthorized system modifications.
- **Investigation and Threat Hunting**: Supports rich investigation workflows and threat hunting through contextual insights into endpoint behaviors.
- **Response Capabilities**: Includes tools for remote remediation, containment, and policy enforcement to help teams respond quickly and confidently.

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

[2] "Endpoints" means wireless devices, desktops, computer systems and any other endpoints with which the Solution operates.

[3] The Aurora Protect Product Description can be found here

Table of Contents

Technology Overview

Aurora Endpoint Defense builds on the capabilities outlined in the *Aurora Protect Product Description – Technology Overview*, 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.

For more information see the following URL on our Arctic Wolf Help Documentation site.

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.

Aurora Endpoint Security Console

With Aurora Focus added to Aurora Endpoint Defense, the console evolves into a powerful platform for detection, investigation, and response. In addition to prevention controls, it now enables advanced threat hunting, enriched detection management, and deep endpoint response—all from a unified cloud interface.

Policy Management

Device policy now includes configuration of rich detection and response settings in addition to prevention. Administrators can define how data is collected from a broad array of behavioral sensors and tailor detection rules to align with MITRE ATT&CK techniques. Policy options also include response automation and data retention settings.

Threat Hunting

A built-in threat hunting interface enables analysts to query endpoint telemetry using EQL (Event Query Language). With 30-day telemetry retention (available for 3.x agents and later) and fully cloud-hosted data, security teams can proactively identify threats, investigate anomalies, and track adversary behavior at scale.

Attack Story

The console offers an interactive attack story view that visualizes process trees and correlated activity captured by the Aurora Focus Agent. Analysts can drill into each node in the attack chain to understand the behavior of individual processes, the sequence of actions taken, and the broader context of the incident.

Alpha AI Security Assistant

The Alpha AI Security Assistant is available for use with Aurora Focus Alerts from within the unified Alerting experience in the console. This allows simple point-and-click interaction points to have the assistant aid in the understanding of system information and threat context to speed up decision making and improve accuracy.

Custom Script Deployment

Administrators can securely deploy custom Python scripts to endpoints for advanced response actions. These packages are used for tasks such as targeted remediation or forensic data collection, extending the platform's response capabilities with fully customizable automation.

Remote Response

Provides secure, audited terminal access to endpoints directly from the console. Analysts can conduct live investigations, run commands, and perform containment or remediation tasks without requiring physical access or third-party remote tools.

Device Lockdown

Enables remote containment of compromised devices to prevent further spread while preserving investigation access. Lockdown behavior is configurable, allowing trusted IPs and ports to remain open so third-party tools can continue to operate during containment.

Deployment and Coverage Considerations

To ensure maximum effectiveness of Aurora Endpoint Defense, the following deployment considerations and configurations should be addressed by the customer:

Deployment Requirements

- **Agent Installation**
  The Aurora Focus agent must be installed on all endpoint devices intended for protection. Installation packages and deployment tools are available via the administrative console. Aurora Focus requires Aurora Protect to be installed first.
- **Policy Configuration**
  Default policies are provided; however, tuning based on the organization's risk

tolerance, environment type (e.g., server vs. workstation), and application needs is strongly recommended.

- **Update Cadence**
  While Aurora Endpoint Defense does not require traditional definition updates, periodic policy review and product updates are essential to maintain optimal protection.

Integration Requirements

- **Cloud Console Access**
  Internet access is required for the administrative console and reporting. If using Arctic Wolf Managed Services in tandem, integration APIs or connectors may be provisioned for threat intelligence sharing and proper service delivery.
- **Optional Integrations (if applicable)**
  Customers may choose to enhance the Aurora Endpoint Defense offering by integrating with additional Arctic Wolf products (MDR, SOAR, etc) or other third-party tools via supported APIs and/or connectors.

Support and Documentation

Engaging with Arctic Wolf Support

Technical support service options and details for Aurora Endpoint Defense can be found here.

Aurora Endpoint Defense Documentation

Documentation for Aurora Endpoint Defense can be found here.[2]

Self-serve support resources and knowledge base articles can be found here.[2]

Roles and Responsibilities

The customer is responsible for:

- Deploying agents across their environment
- Ensuring the correct Agent version is in support for the deployed operating system
- Ensuring that the Agents are kept up to date with an appropriate, supported version
- Configuring policies in alignment with business and security requirements
- Monitoring and responding to events in the Aurora Endpoint Defense console

Arctic Wolf may offer onboarding, tuning, and proactive support services through separate service entitlements or managed service offerings. In these cases, Arctic Wolf may aid the customer in some responsibility areas.