DATASHEET

Aurora® Endpoint Security

BATTLE PROVEN, AI-POWERED ENDPOINT SECURITY

Aurora Adaptive Threat Protection

Aurora® Adaptive Threat Protection (AATP) unlocks AI-powered, intent-based detection to identify and disrupt ransomware, credential theft, and other attacks early in the attack chain and then rolls back the full chain of malicious activity.

The Endpoint Security Landscape

Security leaders are already fighting ransomware and credential theft at record levels. Traditional endpoint tools were built to reduce mean-time-to-respond after a threat occurs, not to close the gap before detection. Attackers live in exactly that gap, a gray zone of valid credentials, native admin tools, and single-use payloads that buys them time in the environment before they are detected. And that gap keeps widening, as AI accelerates attacker reconnaissance, exploitation, and evasion.

Detects Intent, Not Just Signatures

The Aurora Intent Agent continuously maps the activity on an endpoint, so it can detect intent anywhere along the attack chain, not just by assessing the latest event, disrupting attacks whose individual steps would look harmless at any single checkpoint.

Complements What You Already Have

Aurora Adaptive Threat Protection deploys as a complementary layer alongside your existing EPP and EDR to add intent-based detection to your stack. No rip and replace.

Disrupt, Evict, Rollback with One-Click

Agentic Threat Eviction disrupts a confirmed threat the moment malicious intent is identified. Smart Rollback then enables you to reverse the entire attack chain to the state before persistence was established, not just the file that triggered detection, with a single click.

AI-Powered Intent Detection, Built to Disrupt AI Era Threats

Aurora Intent Agent

Analyzes and maps endpoint activity, not just the latest event, to identify malicious intent before damage occurs.

Agentic Threat Eviction

Automatically disrupts and evicts a confirmed threat without waiting on human intervention.

Smart Rollback

Reverses the entire attack chain with one-click to the state before persistence.

Attack Map

Visualizes the full attack chain from initial access through every step of the attack.

Works With What You Have

Deploys alongside any existing EDR or EPP as a standalone purchase, no rip and replace.

Minimal Performance Impact

Lightweight, on-device AI with no material effect on endpoint performance, memory, or CPU.

Standalone or Bundled

Available now as a standalone purchase and to complement any endpoint solution.

Preemptive by Design

Built for AI-accelerated attacker speed, not only today's human-paced threats.

Powered by the Swarm of Experts

Draws on intelligence from millions of investigations across the Arctic Wolf platform to recognize intent earlier, not just react to it.

©2026 Arctic Wolf Networks, Inc., all rights reserved. | Public

Behavioral EDR Alone Isn't Defense Against Intent-Based Attacks.

Features	EPP/EDR	AATP
Provides endpoint attack surface management controls	●	–
Proactively blocks malware pre-execution	●	–
Detects known malware and matches signatures	●	–
Policy-based approach to response actions	●	–
Detects behavior after execution occurs	●	●
Continuously maps endpoint activity, to predict outcomes and detect intent early in the attack chain	–	●
Tracks causal relationships across months, surviving gaps and object destruction	–	●
Visual Attack Map of the full kill chain, from initial execution through persistence	–	●
Automated, agentic eviction the moment malicious intent is confirmed	–	●
Rollback with precision to the state before persistence, not to a moment before a detected threat	–	●
Deploys as an added layer alongside your existing endpoint tools	–	●
Built specifically for AI-accelerated attacker speed	–	●

Learn more about our Endpoint Security Portfolio and which solutions are right for you.

Speak to your Arctic Wolf Sales Representative.

ARCTIC WOLF

©2026 Arctic Wolf Networks, Inc., all rights reserved. Arctic Wolf, Arctic Wolf Platform, Arctic Wolf Security Operations Cloud, Arctic Wolf Managed Detection and Response, Arctic Wolf Managed Risk, Arctic Wolf Managed Security Awareness, Arctic Wolf Incident Response, Arctic Wolf Concierge Security Team, and Aurora are either trademarks or registered trademarks of Arctic Wolf Networks, Inc. or Arctic Wolf Networks Canada, Inc. and any subsidiaries in Canada, the United States, and/or other countries.

AW_DS_AATP_1026

The Threat Landscape

AI-Accelerated Attacks

Threat: Frontier AI models are accelerating attacker reconnaissance, exploitation, and evasion.

Scope of Threat: Organizations spend over $20 billion a year on endpoint security, yet the average breach still costs $5.08M.

Breach Disclosure on the Rise

Threat: Ransomware disclosures keep climbing even as detection tooling multiplies.

Scope of Threat: 24.9% year-over-year increase in reported ransomware disclosures.

Ransomware

Threat: Attackers increasingly skip malware entirely, using legitimate tools and stolen credentials to blend into normal activity.

Scope of Threat: 44% of Arctic Wolf's own incident response cases involved ransomware.

Credential Theft

Threat: Stolen credentials fuel initial access without ever tripping a malware alert.

Scope of Threat: 1.7 billion credentials harvested from 7.4 million infected devices.

System Requirements

Windows

Supported at general availability

macOS and Linux

Planned for a future release