Arctic Wolf Managed Detection and Response

Delivered by an Industry-Leading SOC-as-a-Service

A security operations center (SOC) is the most essential element of modern security. But SOCs are expensive, complicated, and far beyond the reach of most small to midsize enterprises. Many take the easy route and invest in products, though investment in new security products is no guarantee of security.

Arctic Wolf™ Managed Detection and Response (formerly AWN CyberSOC) differs from traditional managed security services. It is a dynamic combination of a world-class Concierge Security™ Team (CST), advanced machine learning, and comprehensive, up-to-the-minute threat intelligence. Your CST conducts both routine and non-routine tasks to protect you from known and emerging threats.

Arctic Wolf Managed Detection and Response Capabilities

Network Inspection

Managed IDS, flow creation, network security monitoring

Log Analysis and Search

Aggregation and correlation

Threat Intelligence

Multiple sources leveraged to identify potential IOC or IOA

Cloud Monitoring

IaaS/SaaS configuration, user/admin anomalies

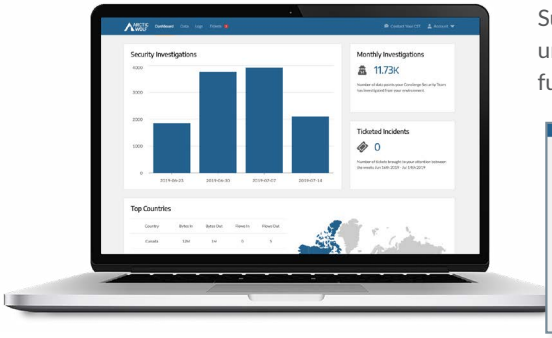
Endpoint Visibility

Operational metrics, asset data, endpoint detection and response

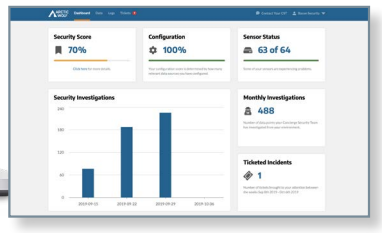
Managed Containment

Detect indicators of compromise and prevent the spread of threats

Arctic Wolf Customer Portal — Tactical and strategic insights



Summary and customized reports to understand your security posture and fulfill compliance needs



Concierge Security Team

- Customer-dedicated primary point of contact
- Actionable security improvement and remediation recommendations

Advanced Threat Detection

- Machine learning with adaptive tuning for efficiency and scale
- Proactive hunting and remote forensic analysis

Security Incident and Crisis Support

- Prioritize security incidents with actionable intelligence
- Required steps for response and remediation

Log Retention and Search

- Log retention of 90 days standard (longer periods available)
- Logs searchable via Concierge Security Team and directly with optional Log Search service

Cloud Monitoring

- 360-degree visibility across customer's on-premises and cloud resources
- Public cloud infrastructure
- SaaS applications
- Security services

Managed Containment

- Prevent hosts devices from communicating externally, and with other devices on your network
- Monthly reporting into the containment actions take over previous periods

Simple, Predictable Pricing

- Fixed recurring price
- Unlimited data collection
- Custom reports with no extra cost

The Arctic Wolf Difference

Concierge Security Team

The Concierge Security Team (CST) is your single point of contact for your Arctic Wolf Managed Detection and Response service. Your CST serves as your trusted security advisor and an extension of your internal team, and:

- Conducts daily triage and forensics
- Customizes service to your needs
- Provides actionable remediation recommendations

Customized Rule Engine (CRulE)

CRulE provides unlimited flexibility to tailor our services to the specific needs of every customer. It allows the Concierge Security Team to apply your exact security and operational policies and update them as needed to align expeditiously with your changing business needs, including:

- Unlimited security policy customization
- Unlimited rules granularity or generalization
- Unlimited situational rules customization
- A curated set of detection logic (CRulEs) brings enhancements to improve the signal-to-noise ratio, while the agent brings increased monitoring and threat detection capabilities, especially around Windows Event logs.

Hybrid AI

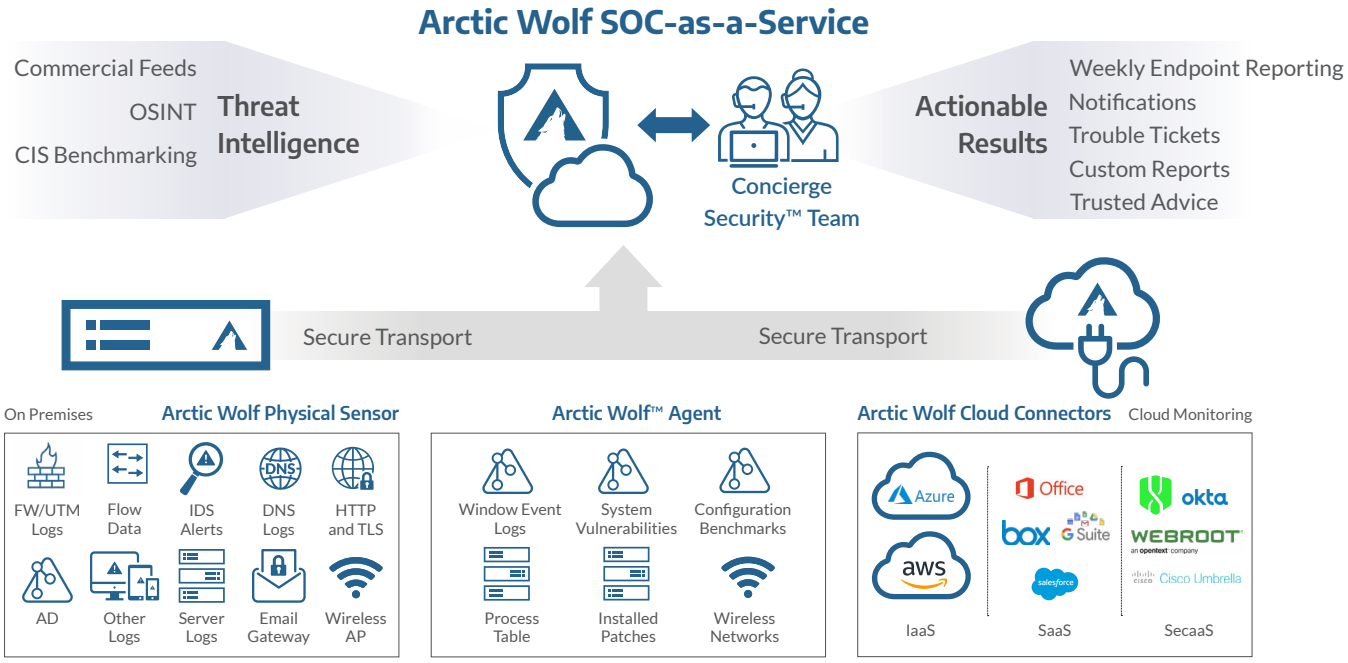
Hybrid AI demonstrably identifies attacks, reduces false positives, and speeds up the time between detection and response. It augments a security team's expertise with the efficiency and productivity of artificial intelligence.

- 10X better threat detection
- Human intelligence and intuition
- Machine scale and efficiency

Endpoint Threat Detection and Response

The included Arctic Wolf Agent provides endpoint intelligence and enhanced threat detection capabilities that give our security engineers deep pervasive visibility into your security posture.

- Sysmon event monitoring provides east/west visibility into the lateral movement of threats
- Weekly endpoint reporting
- Managed containment



ARCTIC WOLF

SOC2 Type II Certified

AICPA SOC

ISO 27001 CERTIFIED CYBERGUARD COMPLIANCE

Contact Us

arcticwolf.com
1.888.272.8429
ask@arcticwolf.com