





# Arctic Wolf Managed Detection and Response™

## Delivered by the Industry's Fiercest SOC-as-a-Service

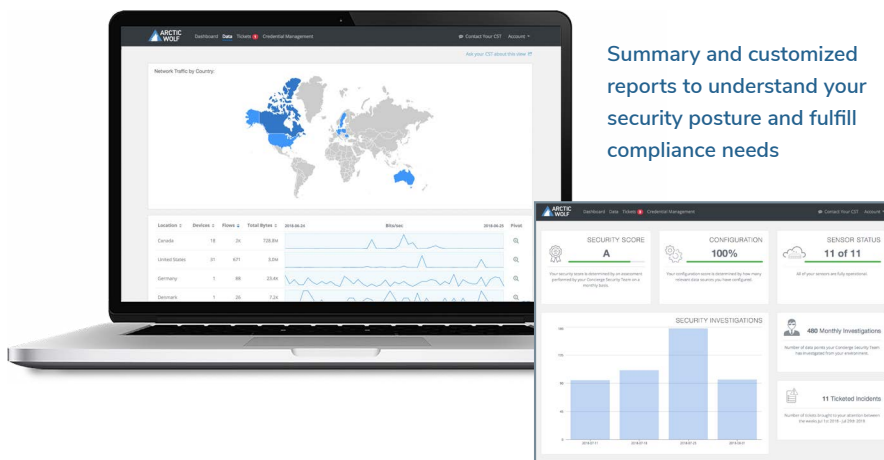
A security operations center (SOC) is the most essential element of modern security. But SOC's are expensive, complicated, and far beyond the reach of most small to midsize enterprises. Many take the easy route and invest in products, though investment in new security products is no guarantee of security.

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

 <p><b>Network Inspection</b></p> <p>Managed IDS, flow creation, network security monitoring</p>	 <p><b>Log Analysis &amp; Search</b></p> <p>Aggregation and correlation</p>	 <p><b>Threat Intelligence</b></p> <p>Multiple sources leveraged to identify potential IOC or IOA</p>
 <p><b>Cloud Monitoring</b></p> <p>IaaS/SaaS configuration, user/admin anomalies</p>	 <p><b>Endpoint Visibility</b></p> <p>Operational metrics, asset data, endpoint detection and response</p>	 <p><b>Compliance</b></p> <p>Reports and audit support</p>

## Arctic Wolf Customer Portal — Tactical and Strategic Insights



### 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

### Compliance

- Log management and compliance reporting
- Periodic external vulnerability scanning to support compliance requirements
- Concierge Security Team support reduces time and costs of audit preparation

### 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 (CRuE)

CRuE 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

## 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.

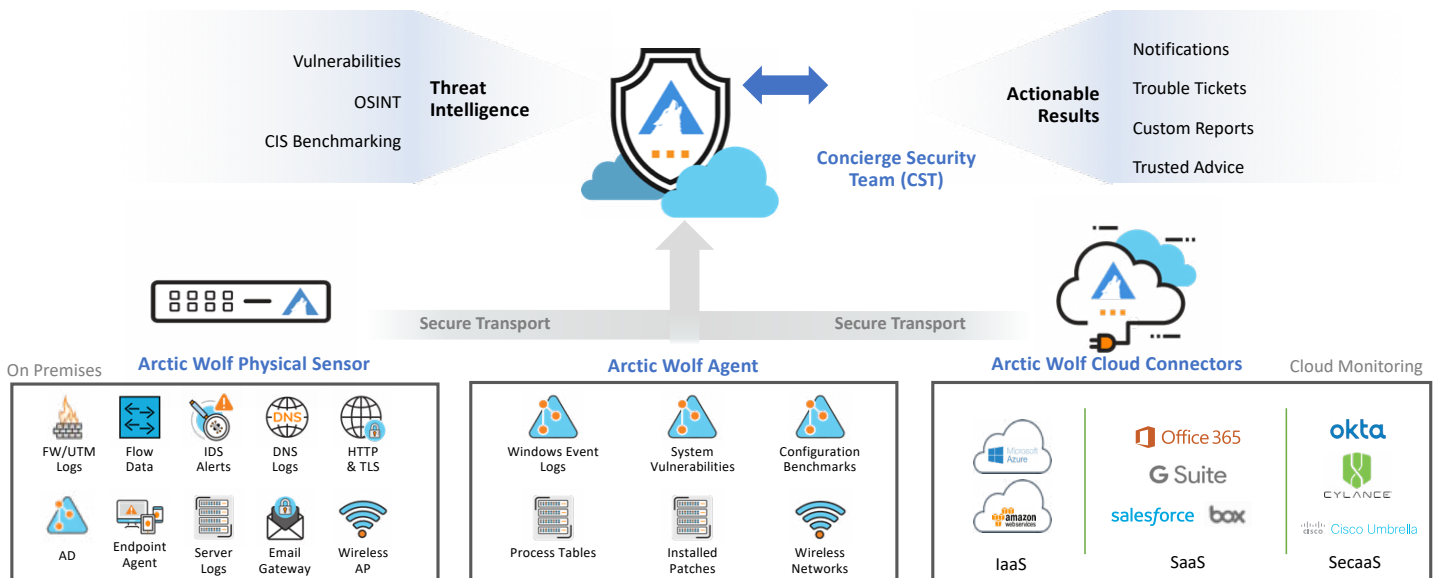
- 10X better threat detection
- Human intelligence and intuition
- Machine scale and efficiency

## Security Optimized Data Architecture (SODA)

SODA unifies the ingestion, parsing, and analysis of network traffic and log data. It provides the foundation for the security analytics that give our security engineers deep pervasive visibility into your security posture.

- On-demand access to the relevant security data for incident investigation
- Instrumented for cybersecurity data science
- Immediately operational with zero setup time

## Arctic Wolf SOC-as-a-Service



©2019 Arctic Wolf Networks, Inc. All rights reserved. Arctic Wolf Networks, AWN and the Arctic Wolf Networks logo are trademarks of Arctic Wolf Networks, Inc. in the United States and/or other jurisdictions. Other names used in this document are for identification purposes only and may be trademarks of their respective owners.

SOC2 Type II Certified



ISO 27001 CERTIFIED  
CYBERGUARD COMPLIANCE

Contact Us

arcticwolf.com  
1.888.272.8429  
ask@arcticwolf.com