COGNISYS SOC Powered by ARCTIC WOLF

Security Operations Platform

Service Description & Service Level Agreements

Document Version: January 2026
Based on Arctic Wolf Terms effective August 2025

Table of Contents

1. Executive Summary

Arctic Wolf provides a comprehensive security operations platform that combines 24×7 monitoring, managed detection and response, vulnerability management, security awareness training, and incident response capabilities. The platform is delivered through their Concierge Delivery Model, which pairs organisations with dedicated security experts who provide continuous, tailored guidance.

This document summarises the key service offerings, service level commitments, and contractual terms derived from Arctic Wolf's publicly available legal documentation at arcticwolf.com/terms/.

2. Platform Overview

2.1 Aurora Platform

The Arctic Wolf Aurora Platform is a cloud-native, open XDR platform that serves as the foundation for all Arctic Wolf security operations. The platform collects, enriches, and analyses security data from across networks, endpoints, and cloud environments. Key capabilities include:

- Broad data ingestion from 250+ integrations
- AI-driven threat detection (Alpha AI)
- Unlimited data ingestion included in core subscription
- 90-day default log retention (extended retention available)
- Customer Portal access for visibility and reporting
- ITSM ticketing integrations

2.2 Concierge Delivery Model

Arctic Wolf differentiates through its Concierge Security Team model. Customers are assigned dedicated security operations experts who provide:

- 24×7×365 Security Operations Centre (SOC) availability
- Regular security touchpoints (4-18 per year depending on tier)
- Customised security rules and workflows
- Quarterly business reviews
- Security Posture in Depth Reviews (SPiDRs)
- Guided remediation and containment support

3. Core Solutions

3.1 Managed Detection and Response (MDR)

Arctic Wolf MDR provides 24×7 monitoring of networks, endpoints, and cloud environments to detect, respond to, and remediate cyber attacks.

Components Included:

Component	Description
Software	Object form software including operating system, add-ons, and enhanced features
Equipment	Virtual appliances or physical sensors (vSensor 100 series included)
Services	Support, onboarding, and Security Services team assistance
Platform	Unlimited data ingestion, Customer Portal access, Arctic Wolf Agent, ITSM integrations, 90-day log retention

Key Capabilities:

- Network security monitoring via deployed sensors
- Endpoint visibility through Arctic Wolf Agent
- Cloud Detection and Response (CDR) for SaaS/IaaS environments
- Managed investigation and guided response
- Managed Containment workflow for threat isolation
- Data Explorer Lite for log search and investigation
- EDR solution integration capabilities

3.2 Managed Risk (MR)

Arctic Wolf Managed Risk enables organisations to discover, assess, and harden their environment against digital risks through continuous vulnerability management.

Key Capabilities:

- Asset discovery and profiling
- External network scanning
- Vulnerability prioritisation for remediation
- Cloud Security Posture Management (CSPM)
- Risk assessment against industry frameworks (NIST CSF, CIS Controls)
- Virtual appliances or physical scanners

3.3 Managed Security Awareness (MA)

Arctic Wolf Managed Security Awareness delivers employee cybersecurity training through continuous microlearning and automated phishing simulations.

Components Included:

Component	Description
Software	Phishtel Reporting Engine and Arctic Wolf Email Report Button
Content	Online access and download rights to learning content and Content Compliance Pack
Admin Dashboard	Cloud-based learning management tool with programme metrics
Services	Support, onboarding, and content modification services

Key Capabilities:

- Continuous microlearning delivery
- Automated phishing simulations
- Employee risk scoring and performance tracking
- Report cards and quiz assessments
- Industry-specific content focus (MA+ option)

3.4 Aurora Endpoint Security

AI-driven endpoint protection providing prevention, detection, and response capabilities to stop endpoint threats. Includes 24×7 monitoring, alert triage, response actions, and guided remediation.

3.5 Incident Response Services

Arctic Wolf provides incident response capabilities to help organisations recover from cyber attacks, including threat containment and business restoration.

Incident360 Retainer Includes:

- End-to-end coverage for one major incident (any attack type)
- IR Dashboard and Planner for emergency engagement initiation
- Cyber Resilience Assessment against NIST CSF and CIS Controls
- Incident-specific runbooks (ransomware, BEC)
- Customised tabletop exercise (Plus tier)
- Flat-rate coverage (up to 70% less than emergency IR)
- Insurance provider approval

4. Security Operations Bundles

Arctic Wolf offers three bundle tiers that combine solutions with varying levels of service and warranty coverage.

Component	Core	Plus	Total
MDR	✓	✓	✓
Data Explorer Lite	✓	✓	✓
Managed Risk (MR)	-	✓	✓
Managed Security Awareness	-	-	✓
Incident360 Retainer	-	-	✓

4.1 Security Operations Warranty Coverage

Arctic Wolf provides a no-cost Security Operations Warranty offering financial assistance for covered cyber events. Coverage levels depend on bundle tier and commitment term:

Bundle	1-Year Term	3-Year Term
Core	N/A	$100,000 USD
Plus	$500,000 USD	$1,000,000 USD
Total	$750,000 USD	$1,500,000 USD

Note: Two-year committed terms may qualify for warranty coverage at Arctic Wolf's discretion. Maximum warranty coverage available is up to $3M USD with additional solutions.

5. Concierge Security Tiers

Arctic Wolf offers three Concierge Security tiers that determine the level of engagement and services provided by the dedicated security team.

Feature	Silver	Gold	Platinum
Concierge Security Team	✓	✓	✓
SOC 24×7×365 Availability	✓	✓	✓
Security Touchpoints/Year	4	12	18
Quarterly Business Reviews	4	4	4
Additional Touchpoints	0	8	14

5.1 SPiDR Library by Tier

Security Posture in Depth Reviews (SPiDRs) are tailored security assessments available at each tier:

Silver Tier SPiDRs:

- MDR Customisation
- MR Customisation
- MA Configuration
- Security Best Practices
- Cloud Security Posture Management
- Pentest Response
- Breach Recovery

Gold Tier SPiDRs (includes Silver plus):

- Comprehensive assessments
- Cloud/SaaS reviews
- Threat & Attack analysis
- Compliance assessments
- BEC (Business Email Compromise)

Platinum Tier SPiDRs (includes Gold plus):

- Cloud Apps (specific integrations)
- Decoy technologies
- Anomalous Traffic Analysis
- Executive/Board Focused Reports

6. Service Level Agreements

6.1 Incident Response SLAs

Service	Response Time SLA
Incident360 Retainer (Standard)	3-hour response time
Incident360 Retainer Plus	1-hour response time
IR JumpStart Retainer	1-hour guaranteed response
Critical threat detection	Contact within minutes

6.2 Security Monitoring SLAs

Arctic Wolf provides 24×7×365 security monitoring through the Security Operations Centre. When a threat is identified:

- The Arctic Wolf Security Services Team will contact the organisation within minutes
- Execute the response strategy including targeted remediation guidance and containment activities
- Incidents are created automatically with detailed information about affected sites, systems, and remediation steps
- Incidents are managed by the CST until closure

6.3 Data Breach Notification SLAs

Per Arctic Wolf's Technical Measures documentation:

- **Breach notification:** Within 72 hours of confirmed fraudulent or malicious activity
- **Information requests:** Response within 2 hours (to extent known)
- **Root cause analysis:** Performed immediately upon breach discovery
- **Ongoing updates:** Regular notification throughout incident resolution

6.4 Platform Availability

Arctic Wolf's Solutions Agreement states that solutions shall substantially perform as described in the Documentation. The platform is provided "as is" with no warranty that operation will be uninterrupted or error-free. However, Arctic Wolf maintains:

- SOC 2 Type II certification
- ISO 27001 certification
- Business continuity plans for critical operations (exercised annually)
- Disaster recovery testing at least annually
- Resilient design for critical service components

6.5 Vulnerability Management SLAs

Arctic Wolf commits to the following vulnerability management practices for their own systems:

- Critical security vulnerabilities resolved within 30 days
- Anti-virus/anti-malware maintained and current on all systems
- Standard patch management processes in place
- Regular vulnerability scanning of networks

7. Security Operations Warranty Terms

7.1 Covered Events

The Security Operations Warranty provides financial assistance for the following event types:

- **Ransomware Event:** Coverage for ransomware-related incidents
- **Business Email Compromise (BEC):** Coverage for BEC-related losses
- **Business Income Event:** Lost revenue and operating expenses affected by incident
- **Compliance Event:** Regulatory compliance-related costs
- **Cyber Legal Liability Event:** Legal defence and settlement costs from privacy/security breaches

7.2 Claim Requirements

- Minimum claim threshold: $5,000 USD
- Claims submitted via arcticwolf@cysurance.com
- Must be enrolled in warranty programme (separate from contract execution)
- Event must occur during Enrollment Term

7.3 Key Exclusions

Recovery services will NOT be provided if:

- Solutions not actively deployed in the environment where the event occurred
- Failure to undertake preventative maintenance including up-to-date patching
- Failure to deploy industry-standard anti-virus/prevention tools on endpoints
- Failure to implement cloud or other backup measures (for Ransom Events)
- Arctic Wolf not receiving supported security-relevant telemetry from environment

8. Technical & Organisational Security Measures

8.1 Security Certifications

- SOC 2 Type II certified
- ISO 27001 certified
- EU-U.S. Data Privacy Framework self-certified
- UK Extension and Swiss-U.S. Data Privacy Framework compliant

8.2 Logical Access Controls

- Unique user identifiers with complex passwords
- Clear-text credentials prohibited
- Role-based access on need-to-know basis
- Immediate access removal upon separation/role transfer
- Two-factor authentication for remote administrative access

8.3 Data Protection

- Data encrypted at rest: 256-bit symmetric, 2048-bit asymmetric
- Data encrypted in transit via SSL, SFTP, SSH, IPSec
- Data segregation from other customers
- NIST 800-88 compliant media sanitisation
- No selling or solicitation use of personal data

8.4 Physical Security

- Access-controlled data centres
- Appropriate alarm systems and monitoring
- Fire extinguishing systems
- Temperature control systems
- Video surveillance in key areas
- Visitor management and escort requirements

8.5 Network Security

- Firewalls operational at network perimeter
- IDS/IPS systems configured and monitored
- Network segregation
- Network threat protection systems

9. Key Contractual Terms

9.1 Term and Renewal

- Subscription terms as specified on Order Form From Cognisys Group Ltd
- Automatic renewal for same period (maximum 12 months)
- 60-day notice required to opt out of auto-renewal
- Renewal at then-current terms and pricing

9.2 Payment Terms

- Fees non-cancellable and non-refundable
- Delinquent amounts: 1.5% monthly interest (18% annual)
- 10-day cure period after non-payment notice before suspension
- Customer responsible for all indirect taxes

9.3 Limitation of Liability

Arctic Wolf's liability is limited to:

- Total fees paid/payable for the 12-month period prior to the event
- Excludes indirect, special, incidental, or consequential damages
- Excludes lost revenues, profits, data, or goodwill

9.4 Warranties

- Solutions substantially perform as described in Documentation
- No infringement of third-party IP rights
- Compliance with applicable laws
- No guarantee of finding all threats, vulnerabilities, or malware
- No warranty of uninterrupted or error-free operation

9.5 Termination

- Either party may terminate for material breach
- 10-day advance notice and cure period required
- Customer must cease use and return/destroy Arctic Wolf technology
- Equipment return required within 90 days or replacement cost charged
- Arctic Wolf deletes confidential information within 120 days of termination

9.6 Governing Law

- State of California law (without conflict of law provisions)
- Arbitration in Santa Clara County, California per JAMS rules
- One-year statute of limitations on claims

10. Data Processing & Privacy

10.1 Data Residency

Solutions Data storage locations are specified in the Solutions Terms. Data may be accessed and processed by Arctic Wolf's non-US affiliates and authorised third-party service providers globally.

10.2 Data Retention

- Default: 90-day log retention
- Extended retention available for additional fee
- Data destroyed per NIST 800-88 guidelines upon termination

10.3 Compliance Frameworks

Arctic Wolf solutions support compliance with:

- GDPR (UK and EU)
- CCPA/CPRA (California)
- Canadian privacy laws
- Australian Privacy Act
- POPIA (South Africa)
- HIPAA (via Business Associate Addendum)
- PCI DSS
- NIST CSF 1.1/2.0
- CIS Controls v8
- NIS2 (EU)

10.4 Subprocessor Management

- Subprocessor list available at arcticwolf.com/terms/sub-processors/
- Due diligence conducted on critical vendors
- Contractual security requirements for vendors

11. Summary of Key SLAs

Service Level	Commitment
SOC Availability	24×7×365
Critical Threat Contact	Within minutes of detection
Incident Response (Standard)	3-hour response time
Incident Response (Plus)	1-hour response time
Data Breach Notification	72 hours from confirmation
Information Request Response	2 hours (to extent known)
Critical Vulnerability Resolution	30 days (AW systems)
Security Touchpoints (Silver)	4 per year
Security Touchpoints (Gold)	12 per year
Security Touchpoints (Platinum)	18 per year
Log Retention (Default)	90 days
Warranty Coverage (Max)	Up to $3M USD

Appendix A: Source Documentation

This document has been compiled from the following Arctic Wolf legal and terms documentation available at arcticwolf.com/terms/:

1. General Terms (Solutions Agreement)
2. Security Operations Bundle & Tier Descriptions (October 2025)
3. MDR Supplemental Product Terms
4. MR Supplemental Product Terms
5. MA Supplemental Product Terms
6. Incident360 Retainer Supplemental Product Terms
7. Aurora Endpoint Supplemental Product Terms
8. Security Operations Warranty Subscriber Terms
9. Product Data Processing Addendum (November 2024)
10. Product Technical Measures (February 2025)
11. Processing Details (February 2025)
12. Acceptable Use Policy

Important Notice: This document is prepared for informational purposes and represents a summary interpretation of Arctic Wolf's publicly available terms. Customers should review the actual contractual terms and seek clarification from Arctic Wolf or legal counsel before entering into agreements. Terms are subject to change; refer to arcticwolf.com/terms/ for current documentation.

Appendix B: Glossary

Term	Definition
MDR	Managed Detection and Response - 24×7 security monitoring and threat response service
MR	Managed Risk - Vulnerability discovery, assessment, and hardening service
MA/MA+	Managed Security Awareness - Employee security training and phishing simulation
CST	Concierge Security Team - Dedicated security experts assigned to each customer
SOC	Security Operations Centre - 24×7 monitoring facility
SPiDR	Security Posture in Depth Review - Tailored security assessment reports
CDR	Cloud Detection and Response - Monitoring for SaaS/IaaS environments
XDR	Extended Detection and Response - Unified platform for threat detection across environments

BEC	Business Email Compromise - Email-based fraud/attack type
DXA	Document-relative Units (1440 DXA = 1 inch)

Appendix C: Cognisys Service Overlay - TBA, (Discussion)