Company Overview

AT A GLANCE

FOUNDED:

2012

EMEA HEADQUARTERS:

Newcastle upon Tyne, UK

GLOBAL CUSTOMERS:

10,000+

SOLUTIONS:

- **Endpoint Security**
- **Managed Detection and Response**
- **Managed Risk**
- **Managed Security Awareness®**
- **Incident Response**

AWARDS

CNBC DISRUPTOR 50

Great Place To Work. Certified JUL 2024-JUL 2025 UK

500 Technology Fast 500 2024 NORTH AMERICA 30 YEARS OF INNOVATION Deloitte. WINNER

Gartner Peer Insights Customers' Choice 2024

THE CHANNEL CO. CRN PRODUCTS OF THE YEAR 2024

The Importance of Security Operations Solutions

Arctic Wolf ends our customers' cyber risk by making security work. Our unique approach to security operations combines purpose-built technology, security expertise, and risk transfer solutions to achieve the security outcomes our customers are striving for at an unprecedented scale.

Organisations Face Fundamental Security Challenges

TOO MUCH NOISE

Alert fatigue, tool fatigue, and compliance and regulation fatigue — the journey never ends

SECURITY SKILLS SHORTAGE

Recruiting and retaining cybersecurity talent is hard, sometimes impossible

COST OF RESPONSE TIME

The longer it takes to respond to an incident, the more expensive it is to remediate

Arctic Wolf Security Operations

Arctic Wolf® is a global leader in security operations, delivering the first cloud-native security operations platform to end cyber risk. Built on open XDR architecture, the Arctic Wolf Aurora™ Platform operates at a massive scale and combines the power of artificial intelligence with world-class security experts to provide 24x7 monitoring, detection, response, and risk management. We make security work.

THE LEADER IN SECURITY OPERATIONS

The Arctic Wolf Aurora Platform

SOLUTIONS

Endpoint Security

AI-driven prevention, detection, and response to stop endpoint threats before they disrupt your business.

Managed Detection and Response

Quickly detect, respond, and recover from advanced threats.

Managed Risk

Discover, assess, and harden your environment against digital risks.

Managed Security Awareness

Engage and prepare employees to recognise and neutralise social engineering attacks.

Incident Response

Recover quickly from cyber attacks and breaches, from threat containment to business restoration.

DATASHEET

Arctic Wolf Incident360 Retainer

Are You Prepared for a Major Cyber Attack?

It's no longer a question of if, but when a severe cyber attack will occur. As such, organizations need to be prepared for serious incidents with a proven response plan as well as access to a full-service incident response (IR) team to remediate the issue and get them back to business as quickly as possible.

Although traditional incident response retainers provide access to critical IR capabilities, organizations struggle to determine how many service hours they'll need to pre-purchase to ensure that they can respond to and recover from a severe incident. This challenge is further complicated by the need for organizations to allocate those service hours between proactive, readiness activities and possible emergency response.

A Better Retainer: Arctic Wolf Incident360

End-to-end IR coverage for one incident, no matter the incident type

Up to 70% savings on emergency incident engagements for Arctic Wolf customers

Incident preparation without sacrificing the ability to respond to an event

Full incident readiness including IR planning, a security assessment, and a tabletop exercise

Incident360 Retainer

The Arctic Wolf Incident360 Retainer is one-of-a-kind as it combines the ability to complete advanced incident readiness activities with end-to-end coverage for one incident. Organizations can rest easy knowing that no matter the incident type, they'll receive the remediation and recovery support that they need to get back to normal as quickly as possible.

End-to-End Incident Coverage

Coverage for one incident, including:

- **Containment:** to stop the spread of the attack
- **Forensics:** to determine the root cause
- **Remediation:** to eliminate the threat
- **Threat Actor Communication:** to negotiate with threat actors
- **Restoration:** to bring systems back to a pre-incident state

Advanced Incident Readiness

Minimize the impact of security events by completing critically important readiness activities. Including:

- Tabletop exercise
- IR Plan review
- Security assessment review

JumpStart Retainer

FEATURES:

- 4-hour response time SLA
- $325 hourly IR rate
- IR Planner
- Incident-specific runbooks
- Cyber Resilience Assessment

Incident360 Retainer

INCLUDES
JumpStart Retainer

FEATURES:

- Coverage for 1 Incident
- 3-hour response time SLA

Emergency Services Included:

- Forensics, containment, active monitoring, threat actor communication, remediation, and restoration*

Threat Intelligence

- Monthly updates on new threats and vulnerabilities

Incident360 Retainer Plus

INCLUDES
JumpStart Retainer
Incident360 Retainer

FEATURES:

Incident Readiness

- 3 Readiness touchpoints
  - Tabletop exercise
  - IR Plan review
  - Security assessment review

Rapid Response ADD-ON

- 1-hour response time SLA
- $295 hourly IR rate

*Up to 30 hours of Restoration is included

About Arctic Wolf

Arctic Wolf® is a global leader in security operations, enabling customers to manage their cyber risk via a premier cloud-native security operations platform. The Arctic Wolf Aurora™ Platform ingests and analyzes more than eight trillion security events a week to help enable cyber defense at an unprecedented capacity and scale, empowering customers of virtually any size across a wide range of industries to feel confident in their security posture, readiness, and long-term resilience. By delivering automated threat protection, response, and remediation capabilities, Arctic Wolf delivers world-class security operations with the push of a button.

For more information about Arctic Wolf, visit **arcticwolf.com**.

ARCTIC WOLF

Incident360 Retainer

Product Description

Document ID	I360-PD
Document Version	1.5
Last Updated	2025.11

Document Change History

Version	Date	Summary of Changes
1.5	2025.11	Updated IR Service Engagement for clarity of forensics scope.
1.4	2025.10	Changed CRA and IR Planner descriptions to reference appropriate external product description documents; Added Data Storage section.
1.3	2025.05	Minor changes to wording to account for general terms and conditions updates.
1.0	2025.04	Initial release

Product Description[1]

Incident360 Retainers

The Arctic Wolf Incident360 Retainer ("I360") Solutions provide proactive and reactive capabilities to ensure you are prepared in the event of a cybersecurity incident.

Table of Contents

[1] This Product Description pertains to purchases of the Incident360 Retainer offerings described herein and subject to the Incident360 Retainer Agreement located at https://arcticwolf.com/terms/. For the avoidance of doubt, customers who have subscribed to the Incident Response Jumpstart Retainer Agreement, as reflected on an Order Form, shall remain subject to the terms of the applicable agreement located at https://arcticwolf.com/terms/.

Arctic Wolf Technology Overview

This Arctic Wolf Technology Overview sets forth, in general, the Incident360 Retainers ("I360") and the various features and tools that may be included as part of your chosen I360 subscription. The availability and use of any such features and tools by you is dependent upon the I360 offering included within your subscription as reflected in an ordering document (i.e., Order Form) either as a standalone or as part of a Bundle.

I360 Solution Overview

This I360 Solution Overview sets forth, in general, the various features and tools that may be utilized as part of delivering your chosen I360 Solution. The availability and use of any such features and tools, along with IR Team involvement, is dependent on the specifics of your chosen I360 subscription.

Description	JumpStart Retainer	Incident360 Retainer	Incident360 Retainer Plus
Response Time SLA for scheduling of scoping call at time of cybersecurity incident	4 hours	3 hours	3 hours
Hourly IR Services Engagement[2]	Yes	Yes	Yes
Covered Incident IR Services Engagement[3]	0	1	1
Preferred Service Hourly rate of $325[4]	Yes	Yes	Yes
Access to Unified Portal	Yes	Yes	Yes
Access to Incident Response ("IR") Planner[5]	Yes	Yes	Yes

[2] Subject to separately agreed upon Statement of Work and Services Agreement.
[3] Subject to the inclusions and exclusions set forth herein and execution of a separate Statement of Work and Services Agreement.
[4] The hourly rate charged for any agreed upon IR services engagement will be $325 USD/hour (or equivalent in the applicable foreign currency as set forth on an Order Form). Any hourly IR Services engagement, including but not limited to Business Email Compromise ("BEC"), must be for a minimum of twenty-five (25) hours.

[5] Access to the IR Planner Module with a Jumpstart Retainer or I360 Retainer does not include an IR plan review with the Arctic Wolf IR Team.

Access to Cyber Resilience Assessment ("CRA")	Yes	Yes	Yes
Incident Specific Runbooks	Yes	Yes	Yes
Access to Threat Intelligence Reports	No	Yes	Yes
Readiness Touchpoints[6]	0	0	3

Rapid Response add-on

Available for purchase with any I360 Retainer:

Description	Rapid Response Add-on
Response Time SLA for scheduling of scoping call at time of cybersecurity incident	1 hour
Preferred Service Hourly Rate of $295[7]	Yes

Features and Tools Overview

IR Planner

The IR Planner capabilities are described in the IR Planner Product Description document found at https://docs.arcticwolf.com/. An IR360 subscription includes access to the full IR Planner capabilities defined within that description.

Cyber Resilience Assessment

The CRA capabilities are described in the CRA Product Description document found at https://docs.arcticwolf.com/. An IR360 subscriptions includes access to the full CRA capabilities defined within that description.

[6] Only one Tabletop Exercise may be used during each annual period of a Subscription Term.
[7] The hourly rate charged for Rapid Response upon IR services engagement will be $295 USD/hour (or equivalent in the applicable foreign currency as set forth on an Order Form).

Incident Specific Runbooks

Incident Specific Runbooks display the full response workflow for a variety of incident engagements including a general runbook applicable to all incident types. They include the response teams needed for a successful response, communication workflows to follow, phases of an incident, signs and symptoms of an attack, investigation and remediation steps, recovery and restoration, and understanding your report and lessons learned.

Arctic Wolf Portals

Unified Portal

The Arctic Wolf Unified Portal is a self-service tool that provides a single point of access to your licensed Arctic Wolf products and a channel to collaborate with the appropriate Security Services Teams.

As part of the I360 Solution, access to the Unified Portal allows you to perform the following tasks:

- Access the IR Planner Dashboard
- Create a detailed IR Plan
- Request a Readiness Touchpoint, if applicable
- View any Readiness Touchpoints that may be available with your subscription
- Review and download Incident Specific Runbooks
- Access dashboards and reports
- Update contacts
- Manage your permissions and organizational profile information

Cyber Jumpstart Portal[8]

For certain customers, Cyber Jumpstart Portal provides access to IR Planner, Incident Specific Runbooks, and CRA. These Modules are migrating to the Unified Portal over time and, once complete, the Cyber Jumpstart Portal will be end of life and access to these Modules will be available through the Unified Portal.

Threat Intelligence

Threat Intelligence Threat Reports are security research intelligence reports generated by the Arctic Wolf Threat Research team and, if available with your subscription, can be accessed within the Unified Portal under the Security Bulletins tab in the reporting section.

[8] To the extent applicable for access to the Modules, use of the Cyber JumpStart Portal (fka Cyber Essentials) and the applicable Modules is subject to the Cyber JumpStart Portal Subscription Agreement located at https://arcticwolf.com/terms/.

Incident Response ("IR") Service Engagements[9]

If you experience a cybersecurity incident during your I360 Subscription Term, you may engage with Arctic Wolf on an incident response services engagement on an hourly basis or, if available with your subscription, you may use your Covered Incident benefit, as more fully described below. With respect to any IR Services engagement, Arctic Wolf will identify and collect necessary evidence pertaining to your incident for the purposes of the forensic analysis investigation, as determined relevant by the IR Team as described herein and in the IR Product Description.

Hourly IR Services Engagement

If, at time of incident and based on your scoping call with the IR Team, you elect to engage Arctic Wolf for IR Services, the IR Services engagement will be provided at the Preferred Hourly Service Rate applicable to your I360 subscription. A description of the IR Services offering can be found in the IR Product Description.

Covered Incident IR Services Engagement

You may, at time of incident based on the scoping call with the IT team, elect to engage Arctic Wolf for the provision of IR Services, subject to the terms of this Section, and use your one (1) Covered Incident, if available with your I360 subscription and if available, one (1) Covered Incident is available during each annual period of your committed Subscription Term. With respect to the Covered Incident, IR Services include up to thirty (30) hours of Restoration and Recovery services but explicitly exclude Data Mining, Compromise Assessments, and proactive services.

Readiness Touchpoints

If included with your I360 subscription, Readiness Touchpoints are delivered digitally or through a meeting conducted virtually with the IR Team to collaborate on activities that deliver proactive security value. Readiness Touchpoints must be scheduled at least thirty (30) days before the end of each annual period during your then-current subscription term. Any meeting will be scheduled at least ten (10) business days following the request to provide ample time for availability and Readiness Touchpoint preparation. In the event you need to reschedule a Readiness Touchpoint meeting, 24 hours' notice of cancelation must be provided to Arctic Wolf. Arctic Wolf will use reasonable efforts to reschedule any such meeting or exercise, subject to the requirements stated herein. If less than 24 hours' notice is not provided, Arctic Wolf may deem the Readiness Touchpoint used and has no obligation to reschedule. Unused Readiness Touchpoints are available during each annual period of your Subscription Term, but any unused Readiness

[9] All IR Services are completed remotely. On-site coverage is excluded.

Touchpoints do not carry over to any future annual period or any renewal Subscription Term. For more information on Readiness Touchpoints, refer to the table below.

Readiness Touchpoint Type	Description
Tabletop Exercise	A Tabletop exercise is a 1-to-2.5-hour cybersecurity incident simulation exercise delivered by an IR Consultant that is designed to test and improve your executive and IT team's ability to respond to a cybersecurity incident. Using the information your team has input into the IR Planner, a Tabletop Exercise will be developed by your IR Consultant that will focus on working through the various considerations and decisions of a real-world cybersecurity incident. After the Tabletop Exercise, a final report detailing your team's overall performance and recommendations on improving your incident response plan will be provided by the IR Consultant to you. Only one Tabletop Exercise may be used during any annual period of any Subscription Term.
IR Planner Review	An IR Planner Review is a 30-minute to 1 hour activity with an IR Consultant to review your company information and IR Plan your team has input into the IR Planner. This review will ensure all fields are filled out correctly, and your team has a solid plan in place in case of a cybersecurity incident. This will also be an opportunity for the IR Consultant to provide general security recommendations and considerations based on the information reviewed in your IR Planner.
Cyber Resilience Assessment Review	A Cyber Resilience Assessment Review is a 30-minute to 1 hour meeting to review your company's tracked responses to the various industry-standard cybersecurity frameworks and provide guidance on any gaps identified.

Data Storage

All Cyber Resilience Assessment data location is determined by the solutions included within your subscription and are described in the Data Storage Location document located at https://docs.arcticwolf.com/.

Security Expertise: Overview of Security Teams

The Arctic Wolf Security Teams engage with you remotely to support your use of the I360 Solutions and ensure Arctic Wolf has a complete understanding of your unique IT environment. For a full description of the Arctic Wolf Security Teams and the scope of activities performed by each team across all Arctic Wolf Products, please see Scope of Service Description.

Working with Arctic Wolf Security Services

During your Subscription Term, you may engage with the IR Team for Readiness Touchpoints or a cybersecurity incident. The interaction with the IR Team will be dependent on the I360 Retainer offering purchased.

For requests to schedule a Readiness Touchpoint, the IR team is available Monday through Friday from 8:00 a.m. - 5:00 p.m. C.T. To contact them, submit a request through the Unified Portal. If you are experiencing a cybersecurity incident, you may select the “Report a Breach” button on the Incident Response Overview page in the Unified Portal and submit the form. This will connect you to the IR Team to schedule your scoping call. If your subscription includes the Managed Detection and Response Solution or the Aurora Managed Endpoint Defense Solution and you are experiencing a cybersecurity incident, follow the escalation path outlined for such Solution.