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® Managed Security Awareness®

More Than Security Awareness Training

Every day, highly motivated threat actors target organizations via their employees who are unprepared to defend themselves. Despite the best efforts of security leaders to reduce their human-centric risk and create a strong security culture, employees are still falling victim to malicious links that cost millions of dollars due to business interruption, downtime, or ransom payments. Typical security awareness training programs simply aren't effective because the content is too long, too dry, and too repetitive.

Fully Managed, Bite-sized Content

Arctic Wolf Managed Security Awareness eliminates human risk by providing 100% relevant microlearning sessions that your employees will actually pay attention to.

We've also made it incredibly easy to deploy and maintain your security awareness program with a proven content delivery method to ensure that you get the best results.

With our fully managed approach, employees receive curated learning experiences immediately following a simulated phishing 'click.' This proven approach helps organizations build a security culture where employees can easily spot and teach them to report phishing attempts to remediate human risk.

Best of all, Arctic Wolf empowers you build and mature your human security posture to end human risk.

A More Efficient Approach to Human Risk Reduction

Move beyond fragmented learning experiences and endless admin efforts with a fully managed security awareness program. Built on microlearning and overseen by awareness experts, Arctic Wolf Managed Security Awareness prioritizes engagement and support to drive behavior change and achieve the security culture needed to reduce human risk.

36%

Arctic Wolf Managed Security Awareness Can Help Customers Reduce Breaches Related to Human Risk

On average, Arctic Wolf MDR customers who fully deployed Managed Security Awareness saw a **36% decrease in phishing-related incident tickets** within the first 4 months of their Managed Security Awareness subscription.

Engage

Educate and prepare employees to recognize and stop threats at the point of attack.

- 100% relevant content
- Microlearning
- Prepackaged phishing simulations
- Compliance training courses

Optimize

Leverage security experts and best-in-class data integrity to maximize the efficiency of your security awareness program.

- Fully managed — proven delivery model
- Phishing data integrity with TruClick™
- Threat level assignments with Phishtel Engine

Transform

Build a strong culture of awareness to reduce human risk at your organization.

- Security culture
- Program performance
- Employee performance

> **"By offering easy-to-understand microlearning, Arctic Wolf is directly improving the knowledge base of our employees."**
>
> *— Chris T., Executive Director*

The Arctic Wolf Difference

Arctic Wolf Managed Security Awareness is more than security awareness training. We don't rely only on training tools to change employee behavior. To be effective, security awareness training requires a holistic approach that includes engaging with the microlearning session, optimizing the efficiency of your security awareness program with groundbreaking technologies, and transforming the security culture by reducing the human risk for your organization.

The outcome of an effective awareness program results in fewer incidents related to human risk and builds stronger cyber resilience across your organization.

100% Relevant Microlearning Content

Arctic Wolf's Managed Security Awareness delivers timely, relevant content based on the latest threats and attack methods. With bi-weekly microlearning sessions, employees stay informed and engaged with short, focused training that fits seamlessly into their routines. This approach ensures ongoing security readiness, keeps teams up to date on emerging threats, and helps maintain compliance with security standards.

Fully Managed — Proven Content Delivery Model

Our fully managed content delivery model is easy to deploy and maintain.

Prepare, launch, and advance your awareness program without adding additional administrative overhead for you and your team. It delivers better outcomes with less administrative work.

Eliminate the Noise of False Positive

Minimize the need to investigate and address non-threatening issues — like training simulation emails — with TruClick™, the industry's first and only solution to separate real user clicks in phishing simulations from your data set.

Automatically Assigned Threat Levels for Reported Emails

Arctic Wolf's Phishtel Engine automatically analyzes and assigns a threat level to reported emails.

Admins can then sort reported emails based on threat level, giving them the ability to prioritize malicious emails and protect their organization faster.

Prepackaged Phishing Simulations

Measure and reinforce employee awareness with automated assessments and phishing simulations based on real-life attacks.

Phishing simulations include a prepackaged follow-up lesson if employees click to remediate the risk.

Employees can take an action to report phishing attempts and mature your security culture.

Compliance Training With Compliance Content Pack

Quickly add comprehensive compliance training to your security awareness program to address HIPAA, PCI, FERPA, anti-discrimination, and other important topics.

Prefer To Use Your LMS?

Arctic Wolf content is downloadable and compatible with your existing learning management systems.

ARCTIC WOLF

SOC2 Type II Certified

AICPA SOC

ISO 27001 CERTIFIED
CYBERGUARD COMPLIANCE

Product Description[1]

Arctic Wolf Managed Security Awareness (MA)

Arctic Wolf MA solution (Solution or Product) supports you to build a strong culture of security within your organization by enabling your employees to recognize, protect, and neutralize social engineering attacks, and creating awareness of security risks caused by human error.

By working to deliver ongoing security awareness content, quizzes, and phishing simulations, our goal is to provide consistent content and training that will keep human risk top of mind.

[1] This Product Description was formerly referred to as the MA Solutions Terms.

Table of Contents

Arctic Wolf Technology Overview

The MA Solution is maintained, monitored, and managed through your configured Administrator Dashboard. Defining your security awareness training program (Program) consists of configuring a series of training content (Content), quizzes, and phishing simulations, the delivery and reporting of which is controlled by you. By hosting your Program centrally within the MA Solution, your program administrator, and your Concierge Security Team (CST), if included with your subscription, can oversee your Program performance, pull reports, analyze user and organization training metrics, configure your Program settings, and control frequency of sessions and communications.

The below Arctic Wolf Technology Overview sets forth, in general, the Arctic Wolf Technology and the various features and tools that may be included as part of the MA Solution. The availability and use of any such Arctic Wolf Technology, features, and tools by you is dependent upon the specifics of your subscription and reflected in the ordering document pertaining to such subscription (Order Form). Any CST involvement and participation in the Solution will be as defined by your Concierge Security Tier (CST Tier), if any, selected by you as part of your subscription. If your subscription does not include CST Tier, Solution support will be as set forth in the Product Support section below.

Administrator Dashboard

MA includes access to the Administrator Dashboard which provides you with real-time visibility into your Program performance, showing the health of your security culture, session statistics, user analytics, session schedule and details, and failed and reported phishing simulations. The Administrator Dashboard focuses on providing the tools that you need to monitor your organization's cybersecurity awareness training journey with real time feedback from within the Solution.

Arctic Wolf offers two subscription types for the Solution, MA and MA+. Specific features provided as part of each applicable version of the Solution include:

Feature/Functionality:	MA	MA+
Microlearning awareness sessions that address deception tactics used, common red flags that should be recognized, escalation and response duties, and leadership responsibilities	X	X
Comprehension quizzes to track basic security posture and your users' (Users) comprehension of the Arctic Wolf developed training content (Content)	X	X

Availability of Industry Tracks to provide Content tailored to your Industry as part of your managed program	-	X
Managed phishing simulation built to represent threat vectors that Users are likely to encounter	X	X
Leaderboard point earning system for Users	X	X
Calculation of your Secure Culture Score	X	X
Access to reporting and account management	X	X
Dark web (Account Takeover) monitoring of your domains	X	X
Arctic Wolf Report Email Button (M365, or however rebranded by Microsoft, deployment required)	X	X
Reported Email Details, included in Phishtel Data, available for reporting within the Administrator Dashboard, including, date and time email reported, email address of reporting User, Microsoft Graph API ID	X	X
Access to licensed Content, including learning materials and additional resources contained in the Administrator Toolkit by you	X	X
Reported Email Analytics which may be produced using Phishtel Data within the Arctic Wolf Phishtel Engine, including reported simulation details, analysis, and threat level, to aid in malicious email prioritization and management	-	X
Access to licensed Content, including learning materials and additional resources contained in the Content Library within the Solution that can be assigned to your Users	-	X
Ability to download certain Arctic Wolf designated Content from the Solution from an Arctic Wolf designated platform	-	X
Group-based Content assignment	-	X
If separately purchased, custom professional and/or production services (“Custom Services”)	-	Optional Add-on for additional fees*
Content modifications (“SCORM”) reasonably necessary to conform the Content to your business format and standards, which shall be performed by Arctic Wolf, and are subject to the Arctic Wolf’s Trademark usage requirements	Optional Add-on for additional fees*	Optional Add-on for additional fees*

If licensed, access to Content Compliance Pack ("CCP"), an optional add-on module which includes compliance course content for common compliance topics that your Program Administrators can download and/or assign to your Users	Optional Add-on for additional fees	Optional Add-on for additional fees

* Feature and/or functionality is not available to Customer if license to Solution is purchased online.

For a more detailed description of sub-features noted above, refer to the table below.

Feature	Description
Overview of Secure Culture Score and Program metrics	Provides visibility into your Program performance, health of your organization's security posture, specific session statistics, and User training history.
Downloads	Provides access to download CSV reports from the Secure Culture Dashboard or Administrator Dashboard containing lists of incomplete Users, low scoring Users, failed Users, and overall User history performance.
Session and user statistics	Enables you to evaluate your organization's Program performance from a high-level view with completion rates, average quiz scores, and fail rates. You can also take a closer look by viewing session by session statistic metrics across your User population.
Session maintenance and program configuration	Enables you to preview and mute the upcoming training sessions, as required. You can also perform the following tasks: • Control Program settings such as delivery day, sending only phishing emails, sending only sessions • Change the Industry Track • Customize private labeling • Enable TruClick (see below) • Determine frequency of Incomplete Session Reminders
User Performance	Allows you to be involved with your Program as an administrator by monitoring organization and User performance. You can also assign additional Content to Users or resend sessions, as needed.
Leaderboard	Provides a way to gamify the Program with your organization by tracking points based on User participation. Administrators can offer recognition by

	identifying top performers or Users who are actively earning points.
Program Maturity Self-Assessment	This tool is a helpful way for administrators to reflect on the efficiency and maturity of their Program. By answering a series of quick questions about your organization's security awareness, administrators will receive an excel spreadsheet analyzing their responses and providing the recommended minimum and target scores.
Additional content	Allows you to assign specific sessions to Users to support security awareness learning objectives within your organization, or for Users who need additional training to improve such Users' quiz scores or phishing simulation failure rate. Additional Content can be assigned by User or through the Content Library depending on your MA license (see above).
Resources	You can use the Administrator Toolkit as a reference and guide to run your Program. You can also pull additional planning documents such as email templates, videos, and posters to support your role as an administrator and your organization's Security Journey.

Compliance

Annual long format courses to meet your compliance requirements may be included in your subscription and, if so, will be reflected on your Order Form.

Feature	Description
Overview of Compliance metrics	Provides visibility into your Compliance performance, specific course statistics, and User training history.
Session maintenance and program configuration	Compliance courses are assigned on demand, with additional controls to determine frequency of Incomplete Session Reminders.
Compliance Downloads and Report	Provides access to download CSV reports from the Compliance Dashboard containing lists of incomplete Users, and overall User history performance. A Compliance PDF report is also available.

Custom Content

There are two types of custom content that may be included in your subscription and, if so, will be reflected on your Order Form.

SCORM: You may request and purchase custom SCORM (SCO) modules, subject to agreement on a separate Statement of Work (SOW). SCO modules may include, but are not limited to, Arctic Wolf approved customizations such as (a) your specific branding to be included on Content, (b) inclusion of video assets provided by you, (c) reference or inclusion of your specific policies, action items, links, questions, quizzes, and other learning and development related requests, and (d) any available and required language subtitle files (.srt).

Custom Services: Custom Services are any requests by you to change, edit, customize, or produce from scratch, existing or undeveloped Arctic Wolf Content, artifacts or deliverables, and/or any professional services or consulting. All Custom Services will be quoted and billed in accordance with an executed and agreed upon SOW on a fixed fee basis.

TruClick®

You can enable Arctic Wolf TruClick® User detection to eliminate false positive responses in response to phishing simulation emails. Phishing simulation false positives can be caused by technology, such as email gateways or virus scanners, in your environment which inspect the phishing simulation email resulting in a clicked link. TruClick recognizes the difference between a User-initiated link execution and a device-initiated link execution. This feature can be enabled or disabled by a toggle through your Administrator Dashboard.

Account Takeover

Account Takeover (ATO), also known as Dark Web monitoring, identifies the risk of your Users' accounts being compromised through third-party breaches and notifies your administrator when there is a report that a User's email account is involved in a third-party breach. With MA, you can request to receive an ATO report through the product support channels. If your subscription includes an External Vulnerability Assessments (EVA) report, such as is included with the Managed Risk solution, the EVA report will include the ATO report.

Reporting

Through your Administrator Dashboard, you can access both CSV downloads and PDF reports to stay on top of User performance and the overall health of your organization's security posture.

You can download and utilize the reports to get a closer look at what actions need to be taken as an administrator, and to communicate any needs with your CST, if included with your subscription, or to report to your management.

For more information about the information contained within CSV downloads and PDF reports, refer to the table below.

Report type	Description
CSV Downloads	Contains the following information: • *Incomplete Sessions* – Users who have received a session, and the session assigned is marked as "not started" or "in progress". • *Low Scoring Users* – Users who received a score of 60% or lower on any assigned quiz. • *List of Users Who Clicked* – Users who received a phishing simulation email and clicked on the associated link in the body of the email. • *Incomplete Remediations* – Users who clicked on a phishing simulation link and did not complete the follow up remediation assigned. The remediation is marked as "not started" or "in progress". • *Full Session History* – A compilation of all Users and their session history to-date. This report will show the User details, session title, sent date, and completion status.
PDF Reports	Contains the following information: • *High Risk Users Report* – Provides the total high risk User disposition by using three unique pie charts to show the percentage of Users who have less than 60% of their sessions complete, the percentage of Users who have an average quiz score of less than 65%, and the percentage of Users who have more than 35% phishing simulation failure rate. • *Phishing Simulations Report* – A high-level report showing the percentages of clicked and not clicked phishing simulations, as well as the percentages of completed and incomplete phishing remediation sessions. • *Security Awareness Program Status* – A compilation of your organization's Program status showing your overall session and quiz status, phishing simulation and remediation results, and a closer look at the completion and click rates of the last three sessions, quizzes, and phishing simulations. • *Security Awareness Program Trends* – A quick view of the last several months on line graphs showing the history of session completion, quiz scores, and phishing simulations.

Phishing Analytics

Integration and deployment of the Arctic Wolf® Report Email Button into your Microsoft 365 service enables your Users to report an email as a phishing attempt and have it tracked and analyzed within your Administrator Dashboard and automatically remove such reported email from the User's inbox.

You can utilize the Report Email Button feature to analyze both reported emails and phishing simulations:

- **Reported Email Details** – View and acknowledge emails that were reported and take a closer look at such email details including:
    - Date and time reported
    - Reporter
    - Graph Message ID – Unique message ID of the email reported
    - From email address
    - Subject
    - Threat Level – Arctic Wolf's Phishtel Engine automatically analyzes and assigns a threat level to reported emails. Additional report management capabilities may be provided in certain subscriptions. For example, administrators can sort reported emails based on threat level to prioritize malicious emails and take action to protect your organization even faster.
- **Reported Email Analytics (if included in your subscription)** – View detailed analytics about the phishing simulation emails that were reported by Users in your organization. The analytics provide:
    - A graph that summarizes the percentage of Users that:
        - Ignored
        - Reported
        - Clicked
    - A table that lists the phishing simulation emails that were reported by Users, including:
        - Date and time reported
        - Title of phishing email simulation
        - Username
- **Phishing Button Settings** – View, integrate, and edit the Report Email Button settings and permissions.

Security Expertise: Overview of Security Teams

The Arctic Wolf Teams engage with you to support you and to ensure Arctic Wolf has a complete understanding of your unique IT environment right from the start. Support by the Security Delivery Teams is provided remotely.

For a full description of the Arctic Wolf Security Teams and the scope of activities performed by each Security Team across all Arctic Wolf Products, please see the Scope of Service document (here). The specific scope of activities handled by the pertinent Security Teams related to the MA Solution can be found in the MA Solution Overview section below.

MA Solution Overview

The below MA Solution Overview sets forth, in general, the Arctic Wolf Technology and the various features and tools that may be included as part of the MA Solution. The availability and use of any such Arctic Wolf Technology, features, and tools is dependent upon the specifics of your subscription and reflected in the Order Form. Any CST involvement and participation in the Solution will be as defined by your CST Tier purchased as part of your subscription, if any. If your subscription does not include a CST Tier, MA support will be as set forth in the Product Support section below.

The following may be included with your MA subscription:

MA Activities

Recognize

Micro-learning Sessions

Your Users will receive unique three-minute or less sessions each month during your subscription which are designed to increase Users' memory strength and exposure to various security awareness topics. Assorted styles of delivery are used, such as animation, expert insights, live action, and interactive. Timely reactive Content is also used to address major cybersecurity events and keep your organization up to date on the current threat landscape. If purchased with your subscription, Content may be assigned to a group of Users in addition to individual User(s).

Quizzes

Quizzes are scheduled to go out periodically to provide knowledge checks for your Users. These are typically formatted to be 2-3 questions with true or false prompts and/or multiple choice.

Phishing Simulations

Every month, a phishing simulation is scheduled to go out to your Users. Alternative templates are provided, and each simulation represents current threats or trends. If a User clicks a phishing simulation link, they are presented with a remediation session tailored to the simulation that was clicked.

Protect

Secure Culture Dashboard

By monitoring User participation and performance in your Program, the Secure Culture Score is included on your Administrator Dashboard and indicates for illustrative and informational purposes the strength of security awareness within your organization based on session completion, average quiz score, phishing simulation clicks, and User remediation training completion metrics.

The Secure Culture Dashboard within the Administrator Dashboard allows you to monitor your Users by downloading reports on Users with incomplete trainings, low scores, and clicked phishing simulations. The statistics presented on this dashboard may be used to encourage User participation in your Program. Your CST, if applicable, will use your Secure Culture Score to suggest tools to improve your Users phishing simulation failure rates.

Reports

Reports available within MA allow you to compile key components of your Program so that you can accurately share your organization's progress with your leadership team. These PDF reports represent your Program's status while giving a closer look at Program trends and high-risk Users.

Incomplete Session Reminders

MA permits you to control the number of email reminders your Users receive for incomplete sessions. Send out daily, weekly, bi-monthly, or monthly reminders by using the scheduler in your Administrator Dashboard. By utilizing this tool, you can encourage Users to stay up to date on their sessions, keeping human risk top of mind.

Additional Content

Additional assignable Content is available for individual Users or groups of Users. It provides additional education or training for low scoring Users or groups of Users who require more tailored Content.

Program Maturity Self-Assessment

The Program Maturity Self-Assessment reflects the efficiency and maturity of your Program. This tool enables you to assess your Program's current maturity score and utilize

this score to measure improvements over time and set targets. Once you complete the self-assessment, the tool provides an excel report displaying your results.

Neutralize

Phishing Remediations

Remediation sessions are custom-made for each individual phishing simulation. The remediation session reviews "red flags" to watch out for in suspicious emails, as well as specific details that were included in the phishing simulation received by your Users. Each time a User fails a phishing simulation, the User will be redirected to complete a remediation session to increase their knowledge of what to watch out for next time.

Reported Simulations and Emails

If you are a Microsoft 365 customer, your organization will have access to the Report Email Button features. By integrating the Report Email Button, Users can report any suspicious email, including simulations, and it will be recorded live in your Administrator Dashboard on the Reported Phishing dashboard. Your Reported Phishing dashboard will allow you, as an administrator, to view reported phishing simulation emails and self-reported phishing emails where you can take a closer look at the User reporting such emails, threat level, and email details.

Administrator Toolkit

As an administrator, you can stay on top of your Users' engagement and communicate with your Users by utilizing the additional resources in the Administrator Toolkit. Resources include strategy and planning guides, videos, posters, background templates, and User and stakeholder email communication templates.

Process

There are four phases that the Solution covers to ensure it can be leveraged to effectively deploy, configure, activate, and manage your Program.

Phase	Details
Deployment Phase	The Deployment Security Team (DST) is available to work with you to help you integrate your Users, complete allowlisting steps, configure your Program settings and deploy MA. ***User and Report Phishing Integration*** *User Integration* To begin setting up your Administrator Dashboard and Solution, you will first integrate or upload your Users. You can add or remove Users through integration with Microsoft Entra ID, Microsoft 365 Active Directory, or Google Workspace. You will manage groups

	through your designated email solution but complete the integration through the User Management tool in your Administrator Dashboard. Users can also be added to your Program through a CSV upload instead. *Report Phishing Integration* As an optional feature, if your organization uses Outlook and would like to utilize the Report Email Button to view analytics regarding reported phishing emails and reported phishing simulations, then you can configure and deploy this feature during onboarding, and DST will assist as needed. ***Allowlisting*** After your Users are added to your Program, you will need to add IP addresses, email headers, and domains to your email provider's allowlists. This enables your Users to receive emails from your Program. ***Onboarding and Integration Call*** As a final step in the deployment phase, your CST, if included, may provide guided assistance, or your Customer Success Manager (CSM) within the Customer Success Security Team may assist with the completion of any integration or allowlisting steps that remain.
Configuration Phase	During this phase, you will be provided with a self-serve video walkthrough, or your CST, if applicable, can provide a demo walkthrough, of your Administrator Dashboard, with further guidance on the configuration options for your Program within the Solution settings, to ensure that your Program has been turned on with the desired delivery day selected. ***Program Configuration*** Before your Program begins, you will need to configure your Program. During onboarding, DST is available to answer any questions that you may have throughout the configuration process. Configuration settings may include: ○ Session Delivery Day (Monday-Friday) ○ Send Phishing Simulation Emails Toggle (ON/OFF) ○ TruClick User Detection (ON/OFF) ○ Send Awareness Sessions (ON/OFF) ○ Industry Track (for MA+ customers) ○ Private Labeling (ON/OFF) ○ Selecting Communication Languages

	○ Incomplete Session Manager (Frequency) ***Program ON*** Once you have configured the Solution settings for your Program and confirmed that you are ready to start your Program, you can activate it with assistance of your CSM or CST, as applicable. The first session, the QuickStart, will be sent and delivered to your Users on the next scheduled delivery day.
Active Phase	The Active phase is continuous and on-going throughout your subscription as you and your organization participate in the Program with almost weekly delivery of sessions, quizzes, or phishing simulations. Program statistics are tracked at the organizational and User level. If CST is included, your CST may be involved in supporting you through your Security Journey. ***Ongoing Content Delivery*** Once the Program is live in your environment, all Users will receive sessions, quizzes and phishing simulations according to the upcoming session schedule found in your Administrator Dashboard. Administrators can monitor your Program Content as needed. Your CST, if applicable, is available to assist your administrator with these activities.
Decommissioning Phase	Decommissioning is the process of terminating your Solution subscription and detaching you from the Arctic Wolf® Platform.

Technical Support Options

You can contact Arctic Wolf for assistance at 888-272-8429 x2 or the toll-free number found at https://arcticwolf.com/toll-free/ for your location. You may also access the Arctic Wolf Support Center via email at support@arcticwolf.com. Any automated maintenance and update cycles to the Solution will be performed remotely by Arctic Wolf.

Roles and Responsibilities

The MA Solution is managed both by Arctic Wolf and your administrator. To ensure that the full value of the Solution is received, each party's roles and responsibilities are defined in the table below.

Activity	Arctic Wolf	Customer
Integrate Users		X
Integrate Report Email Button		X

Complete allowlisting instructions for successful email delivery		X
Configure MA Solution settings		X
Program Activation ON	X	
Deliver bi-monthly awareness sessions and/or quizzes	X	
Deliver monthly phishing simulation with remediation session	X	
Deliver incomplete session reminders	X	
Provide metrics and reporting	X	
Provide Report Button metrics and data		
Provide Account Takeover report	X	
Development and provision of additional resources and tools for administrators	X	
Update and maintain Content library	X	
Monitoring your Security Journey (if applicable)	X	
Management of Program participation		X
Management of User status (active/inactive)		X
Annual renewal of compliance courses (if applicable)	X	
Assignment of compliance courses (if applicable)		X
Creation of Custom Content (if applicable)	X	