G-Cloud 15

Service Definition

Arctic Wolf Managed Security Awareness

NG-IT

Lot 2b Software as a Service (SaaS)

1. Introduction

Company Overview

NG-IT are the UK's leading provider of next generation Private Cloud, Hybrid Cloud and Cyber Security services. We make digital innovation a reality by delivering flexible, always available, highly agile IT services using innovative, next generation technology solutions.

As a multi award winning business, NG-IT is dedicated to meeting the demands of today's business environment. Instead of taking legacy ideas, systems, processes, and technologies, we deliver an exceptional experience around the understanding, design, deployment, and management of next generation data centric and cyber security solutions.

It is critical to stay head of attackers, and our solutions work to identify both new technologies and new and emerging threats. At NG-IT, we understand how important these steps are to ensure that your business is secure against old and new Cyber security threats. This way we can improve your security posture, reduce the risk to your business and keep you where you should be - ahead of the cyber attackers.

NG-IT have deployed over 400 private cloud, hybrid cloud or cyber security solutions including migrating more than 60,000 applications and 32,000 TBs of data. Our professional services capability allows us to provide a full end to end service for our customers, to ensure a seamless working relationship from the initial engagement to the delivery of the chosen solution.

We continually review and assess leading and emerging technology vendors, and our expertise lends us to consider the best options for our customers. We've invested heavily in our people to bring you the very best working relationship and technical consultancy there is to offer.

Social Value

In an increasingly digital and fast-paced world, our Social Value Strategy reflects a deep commitment to people, communities, and the planet. We believe that technology should not only drive innovation but also foster trust, inclusion, and long-term wellbeing. Our legacy is built on a human approach, listening, guiding, and delivering solutions that leave lasting confidence.

Our mission is to be a trusted advisor and supplier of hybrid cloud, security, and data protection services. Our vision is to help businesses prosper through innovative technology, and our values centre on a customer-first culture powered by quality people.

Kickstart Economic Growth

Commitment
We support inclusive economic growth by investing in SMEs and VCSEs, promoting fair pay, and enabling local innovation through ethical procurement.

Initiatives & SMART Objectives

- SME & VCSE Spend Growth: Audit current spend and increase by 15% over 3 years, aligned with local authority targets.
- Fair Payment Code: Ensure 100% of suppliers are paid within agreed terms by Q4 2026.
- Metrics & Monitoring:
- Regular audits
- Supplier satisfaction surveys
- Spend tracking via finance systems

Governance & Ownership

- Led by our Finance Department
- Reviewed annually

Make Britain a Clean Energy Superpower

Commitment

We reduce our environmental footprint and promote sustainable digital practices that support the UK's Net Zero ambitions.

Initiatives & SMART Objectives

- Carbon Reduction Plan: We are currently gathering baseline data on our operational emissions to inform a measurable reduction strategy. Our goal is to identify key areas for improvement and set a science-based emissions reduction target by the end of 2026, with a focus on energy-efficient infrastructure and remote-first working practices
- Net Zero Roadmap: We are currently in the process of gathering baseline data on our carbon emissions across Scope 1, 2, and relevant Scope 3 categories. This data will inform the development of a science-based Net Zero strategy. Our aim is to set a formal Net Zero target by the end of 2026, including plans for verified offsetting of any residual emissions.
- ISO14001 Certification: Maintain certification through annual audits and continuous improvement.

Metrics & Monitoring

- Carbon accounting via Scope 1–3 reporting tools
- Annual sustainability reports
- Internal audits and external verification

Governance & Ownership

- Led by our Operations Manager
- Reported to the Board

Break Down Barriers to Opportunity

Commitment
We foster inclusion through education, skills development, and fair employment practices, empowering underserved groups and future talent.

Initiatives & SMART Objectives

- Digital Skills Outreach: Deliver workshops annually in underserved regions via charity partnerships.
- Careers Advice Programme: Provide virtual careers advice and mentoring to students from diverse backgrounds.
- Volunteering Leave: Provide 2 paid days per employee annually, with 80% uptake by 2026.
- Gender Pay Gap Transparency: Publish annual reports, regardless of company size.

Metrics & Monitoring

- Diversity metrics tracked via HR
- Workshop attendance and feedback forms
- Careers advice session participation and feedback
- Volunteering uptake reports

Governance & Ownership

- Led by Finance and HR and Management
- Supported by Management

Build an NHS Fit for the Future

Commitment
We contribute to a healthier workforce and community through mental health support, wellbeing initiatives, and responsible leadership.

Initiatives & SMART Objectives

- Able Futures Promotion: Increase internal awareness and usage by 30% over 12 months.
- MHFA Training: Train 10% of staff as Mental Health First Aiders by 2026.
- Wellbeing Surveys: Maintain 90% response rate and use feedback to shape quarterly wellbeing actions.

Metrics & Monitoring

- Programme usage analytics
- Training completion rates
- Survey dashboards and action logs

Governance & Ownership

- Led by our Wellbeing Lead and HR Manager
- Reviewed quarterly by the Employee Engagement Committee

This strategy aligns with:

- PPN 06/20: Delivering social value in procurement
- PPN 02/23: Carbon reduction plans and Net Zero
- PPN 09/21: Modern slavery risk assessments
- PPN 03/23: SME-friendly procurement practices

We ensure proportionality to contract size and maintain flexibility to tailor initiatives to specific project needs.

Overview of the G-Cloud Service

NG-IT take great care in selecting our service provider partners. We undertake a rigorous selection process that affords us the confidence to promote and justify Arctic Wolf as our key partner for delivering Fully Managed Cyber Security Services. Arctic Wolf provides essential insights and expertise across all types of environments and infrastructure, making them the ideal partner for our customers to engage and trust as the service provider for this proposed platform. NG-IT partners with Arctic Wolf to deliver managed security operations as a concierge service. Our Security Operations Cloud, built on an Open-XDR framework, spans on-premises, edge, public cloud, and SaaS. Modules include 24x7 threat detection and response, vulnerability management, security awareness training, and digital forensics with incident response.

Throughout this proposal it is our hope to demonstrate our unique approach of focusing on a Cyber Security Outcome that goes beyond and into a true extension of our customer's team, forming a close relationship committed to lowering Cyber Risk across the organisation. To ensure this response is understood correctly, it is prudent to communicate the roles of NG-IT and Arctic Wolf. Arctic Wolf is a 100% Channel Organisation Vendor, which means that procurement would be via NG-IT, a founding member of Arctic Wolf UK Partner program. NG-IT are the channel vendor introducer, billing agent and provider of any complimentary services where applicable. Arctic Wolf directly provides all core Security Operations Centre (SOC) services, Threat Intelligence and guided remediation.

The Solution

NG-IT have chosen to propose a suite of services from Arctic Wolf to address the challenges of delivering and maintaining adequate and effective protection from cyber-attack for the organisation, it's IT environment & critical data and the wider user community.

Managed Security Awareness

Arctic Wolf Managed Security Awareness is more than training and does not rely solely on training tools to change employee behaviour. To be effective, security awareness training requires a holistic approach that includes teaching, testing, and tracking progress toward defined goals. The outcome of an effective awareness program results in fewer incidents related to phishing and human error and builds stronger cyber resilience across your organisation. Our Microlearning ensures that employees are regularly informed about the latest threats and how to stop them at the point of attack. Awareness coaching provides expertise and guidance to security teams looking to mature their awareness program, sustain new, long-term employee behaviour, and foster culture of security within their organisation. Once employees are engaged, program effectiveness can be measured across individuals, teams, and the overall organisation. Quantifiable results identify areas for improvement and demonstrate on-going value of the program to upper management.

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.

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, analyse 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.

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.

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 analysed within your Administrator Dashboard and automatically remove such reported email from the User's inbox.

You can utilize the Report Email Button feature to analyse 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 analyses 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.

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.

Services Subscription

The above service is consumed as tiered bundles, each bundle offers increasing levels of technology, service features & assistance. The services proposed will be delivered directly by Arctic Wolf Triage, Concierge and Incident Response personnel and will provide increased levels of cyber defence and response, allowing for improvements in security standardisation, best practice and adhering to recognised cyber security frameworks such as NIST, NCSC Cyber Essentials and ISO27001.

Arctic Wolf will provide a team of assigned security experts that will study and understand the in-place IT and operations methodologies employed by your organisation and find ways to continually optimise cyber security posture specific to the IT environment and security goals. In addition, they will ingest and centralise all security event data into their cloud-native security analytics platform which will enable them to provide 24x7 correlation, analysis and investigation capabilities, whilst leveraging the in-place technology stack. This allows for unrivalled & broad visibility across all attack surfaces which will maximise effectiveness in preventing and eliminating potential cyber threats.

Your nominated concierge security operations expert works with your in-house teams to provide advice and guidance throughout the service to assess the current state of your environment and identify ways to continually improve cyber posture and reduce risk for the organisation as a whole.

By combining the capacity of the Arctic Wolf ground-breaking Aurora monitoring platform with the capabilities and industry leading skills of Arctic Wolf cyber analysts, response and engineering teams we aim to own the outcome of every critical cyber security event that may present itself to your business.

Principal to our service offering are four specific areas of focus:

- Service & outcome driven approach
- Reduced risk
- Reduced time to value
- Cost efficiency

These can be elaborated on as follows.

Service & outcome driven approach

- Unlimited incident response (incidents and time) with focus on outcome, not contract
- limits.
- Arctic Wolf Triage team own incident response, providing context, threat containment,
- active response and guided remediation.
- Your Concierge team is focused on your strategic security objectives, alignment with
- your chosen security framework and continuous improvement of security posture and
- reduction of cyber risk.

Reduced risk

- Named Concierge Security Team aligned to you to drive Proactive / Strategic security objectives
- 24/7/365 SOC with ~1000 Security Analysts/Engineers/Forensics/Detection Engineers
- Continual platform optimisation, detection rule addition, feature additions included seamlessly in service.
- 400+ R&D team to support “mega events” like Log4JShell.
- ~10,000 customers for crowd sourced threat intelligence – see once and inoculate everyone approach.
- Robust and comprehensive incident planning with defined response times, dedicated incident Director and digital forensics.

Reduced time to value

- Cloud native Security Operations Cloud platform detects threats immediately and replaces need for in-house SIEM tool and the effort to implement, configure, detection rule writing, threat intelligence addition & curation, and runbook writing.
- Onboard and live within 30 to 60 days. Implementation project managed by Arctic Wolf and aligned Professional Services team.
- Tuned and customised response actions to your precise needs by your Concierge team.

Cost efficiency

- Unlimited access to aligned Concierge Team, not constrained by contractual hours or maximum number of incidents/requests.
- Achieve world class SOC platform and service at ~20% the cost of DIY SIEM / SOC build out.

- Virtually extend your organisation security and/or IT operations team through named Concierge Team and Triage teams.
- 99.9% true positive tickets – remove practically all the noise generated by security tools and time spent investigating alerts. Allow your organisation to focus only on verified and actionable security events.
- Unlimited security log data ingestion – broad visibility with no trade-off between visibility and cost, thereby delivering predictable pricing for you.
- No need to rip and replace existing security tools – Vendor neutral approach with integration into existing tools from day one.

Associated Services

NG-IT can provide Professional Services to install and configure the proposed solution. Data migration services are available if required

2. Data Protection

Information Assurance

- Cyber Essentials Plus
- We are certified under the Cyber Plus scheme, demonstrating our commitment to protecting against common cyber threats across our remote working environment.
- ISO 9001 – Quality Management
- This certification ensures our virtual service delivery is consistent, customer-focused, and continuously improving.
- ISO 14001 – Environmental Management
- Reflects our commitment to sustainability through digital-first operations, reduced travel, and energy-efficient cloud-based tools
- Information Management Process:
- Secure Cloud Platforms: All internal and client communications are conducted via encrypted cloud-based systems with strict access controls.
- Remote Access Security: Employees use multi-factor authentication, VPNs, and endpoint protection to securely access company resources.
- Data Handling Policies: We comply with GDPR and the Data Protection Act 2018, ensuring lawful and transparent data processing.
- Incident Response: We maintain documented procedures for breach detection, escalation, and resolution, aligned with industry best practices.
- Supplier Vetting: All third-party vendors are assessed for compliance with security, ethical, and sustainability standards

Data Back-Up and Restoration

NG-IT Limited recognises that the efficient management of its data and records is necessary to support its core business functions, to comply with its legal, statutory, and regulatory obligations, to ensure the protection of personal information and to enable the effective operation and management of the organisation.

To guarantee that, we have a Data Backup Policy that applies to all staff within the Company with a purpose of safeguarding information belonging to us, any third parties and clients. We do not hold business critical data within a traditional on-premises network or managed data centre, all line of business application data and unstructured file data is located within cloud storage, owned and managed by the relevant application vendor the data is specific to.

This business systems technology model allows for continuous replication of data from production cloud platform to secondary storage or an alternative cloud platform, effectively providing always available, fully comprehensive, granular backup with quick restore capabilities.

Backup Model

- Full backups of all data are performed weekly. Full backups are retained for 3 months before being overwritten.
- Backups are stored in secure locations. A limited number of authorised personnel have
- Backup of data held within Database Systems have data backup routines which ensures database integrity is retained

NG-IT adopts the best security practices by defining security controls applicable to the entire organisation. Additional security measures identified through risk analysis, legal, regulatory, and/or contractual concerns, and/or specific standards -shall be addressed accordingly. Security controls and best practices are be considered and implemented as appropriate to the risk level

Business continuity statement/plan

Business continuity is not simply a matter of contingency, it is a core component of delivering consistent, reliable service in a competitive and fast-evolving industry. As an IT reseller/security and service provider operating with a fully remote workforce and reliant on only on cloud-based systems with no corporate network, NG-IT Ltd recognises the importance of being prepared for unforeseen disruptions, whether technical, operational, or external.

We have a Business Continuity Plan that outlines measures to ensure that our operations remain stable and responsive during periods of disruption. It defines the procedures, responsibilities, and safeguards that enable us to continue supporting our clients, maintain supplier relationships, and uphold our professional standards. The plan reflects our commitment to resilience and readiness, and will be reviewed regularly to ensure it remains aligned with our business needs and the expectations of those we serve

This Business Continuity Plan sets out the procedures and responsibilities required to ensure the continued operation of NG-IT Ltd in the event of a disruption. It applies to all employees and covers both the reselling of IT services, hardware and software distribution. The plan is designed to safeguard client relationships, maintain service delivery, and protect the company's reputation.

The key aims of this plan are to:

- Ensure continuity of service provision to clients.
- Minimise delays in hardware fulfilment and vendor coordination.
- Maintain secure and effective communication with customers and suppliers.
- Uphold contractual obligations and regulatory compliance.

The following functions are considered critical to the business and must be maintained during any disruption:

- Vendor liaison and procurement
- Order processing and fulfilment
- Customer support and issue resolution
- Financial operations including invoicing and payments
- Internal communication and collaboration

All our staff members have defined roles in the event of a disruption. The Managing Director is responsible for overseeing the implementation and maintenance of this plan. The Operations Manager and Finance Manager manages supplier relationships and hardware sourcing. The Technical Director and Cyber Lead ensure access to systems and data security. The Account Managers handles customer communications, and the Finance Officer ensures continuity of financial operations

All our business systems are cloud-based and configured for daily automated backups. Access is controlled via multi-factor authentication and role-based permissions. A centralised password manager is used across the organisation. Security audits are conducted quarterly to ensure compliance with data protection regulations and best practice.

Internal communications during a disruption will be conducted via internal messages and email, with SMS or telephone used for urgent alerts. External communications with clients and suppliers will be managed via email and telephone.

In the event of a disruption, recovery procedures will be activated immediately. Alternative suppliers may be engaged to maintain service continuity. Clients will be informed of any delays or changes to service provision. Staff availability will be managed through cross-training and flexible working arrangements. Any cybersecurity incidents will be addressed by isolating affected systems, restoring data from backups, and notifying relevant stakeholders.

This plan will be tested annually through structured exercises. Supplier performance and supply chain reliability will be reviewed in line with our ISO management system. Contact lists and standard operating procedures will be updated accordingly. Following any real disruption, a post-incident review will be conducted to identify areas for improvement.

Privacy by Design

We are committed to embedding privacy into every aspect of our service delivery. As an IT reseller, we do not process personal data directly through proprietary platforms, but we ensure that all technologies we recommend, resell, or support meet GDPR standards and respect user privacy from the outset.

- Privacy by Design: We assess privacy risks during the initial selection and onboarding of any suppliers. This includes reviewing data handling practices, encryption standards, and access controls before recommending solutions to clients.
- Supplier Vetting: All vendors we work with are evaluated for GDPR compliance, including their use of data processors, sub-processors, and data residency policies.
- Minimal Data Handling: We store minimal personal data (e.g., names and email addresses) solely for communication and support purposes. This data is handled securely, in line with GDPR principles, and is never used for profiling, marketing, or shared with third parties without consent.

3. Using the service

Ordering and Invoicing

To order services from our organisation, you can simply send an email to gcloud@ng-it.co.uk to discuss your requirements in more detail and initiate the process. We recommend including key information in your email such as your organisation name, a brief description of the services needed, preferred start date, expected outcomes, and any relevant procurement references. Once we have reviewed your request, we will assist you in completing the Order Form, which formalises the agreement under the framework and becomes the Call-off Contract. This includes support with service scope, pricing, and terms to ensure everything aligns with your expectations. Our fees are invoiced monthly in arrears, and payment terms are 30 days net from the date of invoice receipt.

Availability of Trial Service

At the present, complimentary trial of the Arctic Wolf Managed Security Awareness Solution cannot be offered, as the nature of the Service involves fully managed security operations that cannot be replicated in a short period and standalone trial environment. As an option to the trial and upon request, we can offer a product demo and a Proof of Concept (POC). The POC will give you a good view of the Product capabilities and how the service aligns within your environment, allowing an applied assessment, and the demo can provide an overview of core functionalities.

On-Boarding, Off-Boarding, Service Migration, Scope etc.

Once the Managed Service Contract is signed and we have the confirmation of your order, the onboarding process begins, and a designated team is assigned within the Service Provider to coordinate all aspects of your contract and provide a smooth onboarding process. As the IT Reseller, NG-IT will assign a dedicated Service Delivery Coordinator, that will look after your contract and lease periodically with the Service Provider during the whole lifetime of your service. At this point, your dedicated Service Delivery Coordinator will make sure that the Service Provider will follow the steps outlined in their onboarding process.

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

1) **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 Managed Security Awareness.

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.

2) 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.

3) 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.

4) Decommissioning Phase

Decommissioning is the process of terminating your Solution subscription and detaching you from the Arctic Wolf Platform.

Please have in mind that this is not a static process and the steps and timeframes may vary according to the environment sizing and complexity. A detailed implementation plan can be provided to the buyer on request.

Training

As a reseller, we provide buyers with access to the service provider's comprehensive training and onboarding resources. These include online help documentation, knowledge bases, and guided assistance to support orientation with the new service. Introductory onboarding sessions are available to ensure buyers understand how to configure, monitor, and manage the cyber security platform effectively. Where required, we facilitate access to the provider's customer success team for tailored onboarding support. Our role is to ensure buyers are connected to the appropriate resources and that any queries are escalated promptly to the service provider for resolution.

To guarantee a seamless and smooth environment transition and data migration, the Service Provider will provide support and guidance as part of the Service onboarding. You will receive all the instructions to help you migrating and setting up your Service. Service Provider will provide training around the Arctic Wolf systems, either via training materials or walk-throughs, to ensure that you have all necessary information to navigate through Arctic Wolf with confidence. You will also have access to Webinars and Education Sessions, and an extensive learning content library available on the customer portal.

As part of our service we include, as standard, the Concierge delivered Security Journey. The security journey is unique to you and tailored to achieve your security objectives, for example: cybersecurity compliance, secure cloud adoption, improved security posture. The journey can be delivered at a cadence that supports your team and your CST owns scheduling meetings and driving the outcome at

a pace suitable for your organisation. Your CST team will prepare and own the delivery of each Security Journey session - SPIDR (Security Posture in depth Review).

We encourage customers to attend these sessions to understand the recommendations your CST outlines to improve your security posture and reduce your cyber risk. Each security journey session typically lasts an hour.

You will also count with 24x7 support team, that can be contact via email, phone or ticket and will be available not only to assist you with incidents and technical related issues but answering any questions you may have on how to use the Service Provider features.

Service Management

We take an integrated approach when it comes to the management of Services as we understand that an effective service delivery relies on a balanced integration of expert personnel, mature ITIL v4 aligned processes and technology. From a workforce perspective, our team possess both technical and behavioural competencies required. This includes not only the commercial knowledge of our products and solutions, but technical proficiency to build the service architecture, relying on a Team of experienced Solution Architects that holds the accreditations necessary to support the delivery of our Services.

In alignment with the technical team, we have a Service Delivery process in place that maps out the level of Service that is expected and provide operational consistency and governance throughout the delivery of the Service. This includes a Team of dedicated Coordinator that hold ITIL v4 Certification and is assigned to reinforce a customer-centred approach and guarantee that all aspects of your contract are being provided accurately. This process guidelines are outlined based on ITIL Framework, which set the basis for all the procedures followed to guarantee the delivery of IT Services that meet customer's needs.

This process counts with clear escalation paths, service level agreements and communication protocols to safeguard service continuity and accountability. We also count with a well-structured continuous improvement procedure, including post incident review with the customer and the Service Provider, and trend analysis that will help us to identify and tackle any systemic issue and enhance our client experience and satisfaction. These processes help us to set the standards of what we do as the IT Reseller but also direct what we expect from the Service Provider Partner.

Service Constraints

The Service Provider do not count with a published Uptime Guarantee as the solutions include outside factors that are outside their control including use of hosting providers. They also ingest data from 3rd party sources which could be delayed due to items outside of Arctic Wolf control and result in an inability to notify/detect threats for a given telemetry source. It is also important to say that Arctic Wolf has architected its solution for high availability aligned to the six pillars of the AWS Well Architected Framework, including replication in AWS availability zones for recovery purposes. While Arctic Wolf does not publicly publish uptime numbers, the percentage of uptime measures the functional availability of Arctic Wolf products and services, specifically how many logs they successfully ingest within their platform. Their typical uptime SLO is at least 99.75%.
Rest assured that, as your IT Reseller, we will make sure that the Service Provider will notify you of any outages with a portion of its solution and provide a recovery time estimate.

Service Levels

Arctic Wolf monitor and manage the technology components required to deliver 24/7 MDR SOC service. This includes upgrades, uptime, status monitoring, etc. As well as monitoring their own infrastructure we also monitor the feeds / agents / sensors etc. from our customers environments that are ingested into their environment. Should there be an issue with any of the customers components, the Service Provider will engage with them to resolve based on the defined escalation paths in the system. Arctic Wolf staffs all its worldwide SOCs on a 24/7 basis, services for UK customers would be provided by their EMEA SOC's based in Germany and Ireland.

Incident Response Time
Arctic Wolf's current Service Level Objective for emergencies is 30 minutes. However, this is 30 minutes to receive an alert, triage an alert (providing information such as what, where, when, why and how and remediation actions) and provide a ticket to our customers. Caution should be exercised when measuring metrics in isolation with mean time to ticket or mean time to respond (e.g. MTTD and MTTR). If the alert is serious enough the triage engineer will have already acted in the form of host containment, session closure or user disabling as per the agreed engagement action with the customers prior agreed requirements. As a standard practice, Arctic Wolf provides response time SLOs which are incorporated into the contracts.
Standard response time SLOs are as follows:

- Emergency escalated via phone to Arctic Wolf's Security Services (inbound notice) - Arctic Wolf will respond within five (5) minutes
- Escalation of any Emergency (outbound notice) - Thirty (30) minutes of Arctic Wolf's discovery
- Acknowledgement of any schedule request submitted by Customer to security@arcticwolf.com One (1) hour from receipt of request
- Notification and escalation of any Security Incidents (outbound notice) - Two (2) hours of Arctic Wolf's discovery

What defines an emergency is jointly agreed between Arctic Wolf and the customer.
Emergencies - Following transition from the deployment team to the Core Support Team (CST), Customer and the CST will agree on and document which Security Incidents will be defined as an "Emergency". Emergencies will typically include the discovery of ransomware and other alerts that could cause degradation/outage to Customer's infrastructure security. Arctic Wolf will escalate Emergencies to Customer within thirty (30) minutes of Arctic Wolf's discovery of the Emergency.

As mentioned, NG-IT as your IT Reseller, throughout its Service Delivery Process and according to the ITIL v4 Framework guidelines, will make sure that the Service Levels will be followed by the Service Provider according to what has been agreed on the Service Agreement signed by all parties. As part of this, you will be able to count with a dedicated NG-IT Service Delivery Coordinator that will conduct period checks to all support tickets that you might have opened with the Service Provider and action on whatever is required to guarantee the effective delivery of the service.

Outage and Maintenance Management

Service Provider will monitor and manage the technology components required to deliver 24/7 Service. This includes upgrades, uptime/status monitoring, etc. As well as monitoring their own infrastructure we also monitor the feeds / agents / sensors etc. from our customers environments that are ingested into their environment. The Provider, to the extent possible, will notify the Customer about scheduled or emergency maintenance through the Provider's Account Management Application and portal. The Provider, to the extent possible, will notify the Customer about scheduled or emergency maintenance through the Provider's Account Management Application. The Provider will constantly update the Account Management Application information to advise the Customer when a maintenance is completed.

NG-IT as your IT Reseller, throughout its Service Delivery Process and according to the ITIL v4 Framework guidelines, will make sure that the Service Levels will be followed by the Service Provider according to what has been agreed on the Service Agreement signed by all parties. As part of this, you will be able to count with a dedicated NG-IT Service Delivery Coordinator that will conduct period checks to the Service Provider state and promptly address any outages and request ad-hoc service if applicable. Root Cause Analysis and Service Improvement Plans will also be requested whenever is appropriate.

Financial Recompense Model for not Meeting Service Levels

While us, as your IT Reseller and the Service Provider, aim to meet all proposed Service Levels, there may be occasions where performance falls short of circumstances outside of our direct control as outlined in the Service Constraints and Outage and Maintenance Management sessions of this document. The SLAs is an important way of measuring service quality rather than to trigger financial compensation, therefore, there is no financial credit available or refund.

In case of a failure from Service Provider on achieving the agreed SLAs, as your IT Reseller we will focus on addressing the issue with Arctic Wolf and providing you with clear answers and, when applicable, formal root cause analysis. We will also work collaboratively to ensure that a Service Improvement Plan is put in place and, if necessary, apply any change to prevent the failure from happening again in the future.

We are confident that this approach helps us maintain a strong and transparent partnership with our clients and service partner, keeping the service reliable, issues visible and improvement actions transparent.

4. Provision of the service

Customer Responsibilities

To deliver the best service and guarantee efficiency on the Service implementation and consistent service delivery, we operate under a shared-responsibility model, where all parties contribute and work in partnership during the lifetime of your contract. As our client, for service delivery effectiveness, we kindly ask your collaboration on:

- Providing the most accurate information during all phases of the Service Delivery
- Promptly notifying us of any significant business and technical changes that may affect the Service performance
- Providing timey responses to the Service Provider queries, incident responses and approval requests
- Adhering to agreed change-management processes, including approvals, lead times and risk assessments
- Submitting requests using approved channels
- Participating in Services Reviews
- Honouring contractual payment terms

Customer must identify the administrative users for its account which may include Customer's and its Affiliates' authorized (email authorization sufficient) third party service providers and agents ("Administrators"). Each Administrator will receive an administrator ID and password and will need to register with Arctic Wolf.

Customer is responsible for registering and updating its Administrators, or notifying Arctic Wolf, as applicable, about changes to Administrators, including but not limited to termination, change of authority, and the addition of Administrators. Customer acknowledges and agrees that Administrators will be able to view all Solutions Data and other traffic and activities that occur on Customer's network and that Customer is responsible for all activities that occur under Administrator accounts. Administrator IDs are granted to individual, named persons and cannot be shared or used by more than one Administrator but may be reassigned from time-to-time to new Administrators. Notwithstanding anything contrary herein, Customer understands and agrees that transmission of Solutions Data to Arctic Wolf may be impacted by in-country technical issues and requirements. Arctic Wolf will provide reasonable assistance to Customer in such instances but is not liable if the Solutions Data cannot be transmitted outside of such country.

Customer is responsible for implementing appropriate internal procedures and oversight to the extent it utilizes the configuration of workflows and processes, including but not limited to containment actions, and similar functionalities in conjunction with the Services. Arctic Wolf may recommend Customer, depending on the scope of the deployment, implement software and services to enable features of the Solutions or to permit increased visibility into Customer's environment.

Customer is responsible for making such determinations in its discretion and Arctic Wolf has no liability for Customer's decisions related thereto. Customer acknowledges that any changes Customer makes to its code, infrastructure, or configuration of the Solutions after initial deployment may cause the Solutions to cease working or function improperly or could prevent Arctic Wolf from delivering the

Solutions and Arctic Wolf will have no responsibility for the impact of any such Customer changes. Customer understands that depending on the Solution deployed, a Solution may consume additional CPU and memory in Customer's environment while running in production.

Public Entity Customers
If Customer is a public entity, Customer acknowledges and agrees this Agreement is the sole set of terms governing the delivery of the Solutions to Customer and for the avoidance of doubt, terms related to acceptance related to any services or work product shall not apply. The terms of any request for proposal(s), request for information, invitation to qualify, purchasing agreement or cooperative contract, or similar agreement Customer is using to purchase the Solutions (as defined below) from an Authorized Partner do not apply to Arctic Wolf. Further, Customer understands, and hereby consents, that Solutions Data may be accessed and processed by Arctic Wolf and its non-US Affiliates and their non-US citizen employees and Arctic Wolf's authorized third-party service providers in the United States, Europe, or other locations around the world. Notwithstanding anything contrary in any other agreement or purchasing contract, Customer understands and agrees that during the Subscription Term, Arctic Wolf will maintain security controls and processes no less restrictive than those set forth in its SOC 2 Type II report and ISO 27001 certification.

Customer is responsible for determining if Arctic Wolf's controls and processes comply with Customer's data handling and security policies. Customer represents that in purchasing the Solutions, (i) Customer is not relying on Arctic Wolf for performance of a federal prime contract or subcontract and (ii) Customer is not receiving federal funds to purchase the Solutions. If Customer does intend to rely on Arctic Wolf Solutions to fulfil its obligations under a federal prime contract or subcontract or utilize federal funds to purchase the Solutions, Customer agrees to provide Arctic Wolf advance written notice of that intention, and Arctic Wolf shall have the option to terminate this Agreement. Arctic Wolf Technology is a "commercial item", "commercial computer software" and "commercial computer software documentation," pursuant to DFARS Section 227.7202 and FAR Sections 12.211-12.212, as applicable. All Arctic Wolf Technology is and was developed solely at private expense and the use of Arctic Wolf Technology by the United States Government are governed solely by this Agreement and are prohibited except to the extent expressly permitted by this Agreement.

Detailed Service Terms and Conditions, including the Contractual Customer Responsibilities will be addressed in the Service Agreement.

Technical Requirements and Client-Side Requirements

To determine the details about the exact technical and client-side requirements to deliver the service, it is essential that we have a full understanding of your current environment, operational needs and challenges you may be facing. This initial assessment will help us to guarantee the correct application of the Arctic Wolf Managed Security Awareness solution. Therefore, many of the technical requirements and client-side requirements will be discussed prior to an order being placed, but also during the onboarding and implementation stages, where all parties will work together to refine connectivity, security, access and workloads considerations. All requirements discussed prior to the order being placed shall be documented in the Order form and agreed between the parties. We consider that this approach ensures that the technical prerequisites are mapped out accurately and are aligned to the customer needs and expectations.

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	

After-sales Account Management

As the IT Reseller, we are not only committed to offering the best solution but also to build strong relationships with our clients, working with you closely, not only during the initial phase of the project but also after the Service is delivered and implemented. This is pivotal to us, as a Company, to work with you on a full end to end service and make sure your expectations regarding the Service are meet during the whole lifetime of your service. Unlike some specialist integrators, we are not just about selling a product, we are more interested in providing the right solution and we are committed to our customer's satisfaction.

As part of your service, you will have a designated Account Manager that will work closely with you on period reviews of our environment and will guarantee that you are being offered the most suitable solution/ service. You will also count with a Service Delivery Team that will liaise with you and the Service Provider on a regular basis, addressing all aspects of your service delivery and serving as your advocate to all your related service matters.

The Service Provider will also schedule Quarterly Business Reviews (QBRs) with your CST team and your Customer Success Manager. The purpose of these sessions is to review the last 3 months of service and your cyber risk status, review your security objectives, and share roadmap and service updates. The QBRs typically last an hour.

Termination Process

The Service Agreement shall be in effect for the Subscription Term, to be specified in the Order Form. Unless otherwise set forth on the Order Form, the Subscription Term for the Solutions, in its entirety, will automatically renew at the end of the initial Subscription Term for the same period of time as the initial Subscription Term, but in no event more than a twelve (12) month term, and subject to the then-current terms and price at the time of renewal; provided however, if either party would like to opt out of automatic renewal of the Subscription of the Solutions or reduce Subscription scope, then such party must notify the other party no less than sixty (60) days prior to the expiration of the then-current Subscription Term.

As a subscription Solution, Arctic Wolf does not allow for termination for convenience. Arctic Wolf relies on committed subscription terms, in part, to manage our dedicated CST resource model. Either party may terminate this Agreement for cause if the other party commits a material breach of this Agreement, provided that such terminating party has given the other party ten (10) days advance notice to try and remediate the breach. Upon termination, Customer agrees to cease all use of the Arctic Wolf Technology, installed or otherwise, and permanently erase or destroy all copies of any Arctic Wolf Technology, including all Content and virtual Equipment, that are in its possession or under its control and promptly remove and return all physical Equipment to Arctic Wolf. Except as otherwise required by law, Arctic Wolf will remove, delete, or otherwise destroy all copies of Confidential Information in its possession upon the earlier of (i) the return of the Equipment, if applicable, to Arctic Wolf, or (ii) one hundred-twenty (120) days following termination. Notwithstanding anything contrary in the Agreement, should Customer fail to return any Equipment within ninety (90) days following discontinuation of use of the Equipment or termination or expiration of the Agreement, Customer will be liable for the replacement cost of the Equipment, which shall be due and owing upon receipt of the invoice from Arctic Wolf or the Authorized Partner, and Customer shall be liable for any breach of the Confidential Information and Arctic Wolf Technology contained within the unreturned Equipment. Sections 6 through 13, 14, and 15 will survive the non-renewal or termination of the Agreement.

5. Our experience

Case Study

Security Operations Service for a Large UK Education Organisation

Overview

A major UK education institution with over 35,000 users—a mix of students, academic staff, and administrative teams—faced escalating security risks across a highly distributed, multi-site environment. With critical teaching, research, and operational services at stake, the organisation required a modern security operations service that could deliver full visibility, integrate with existing technologies, and operate within tight public-sector budget constraints.

Challenges

- **Complex, multi-site estate:** The organisation operated multiple campuses and satellite locations, each with differing levels of maturity and legacy infrastructure.

- **Highly sensitive data:** Research outputs, student records, financial information, and regulated datasets demanded robust protection and rapid incident response.
- **Limited visibility:** Fragmented tooling and inconsistent logging meant the internal team lacked a unified view of threats across endpoints, networks, cloud services, and identity systems.
- **Public-sector budget pressures:** The institution needed a predictable, fixed-cost model that avoided unexpected overages or consumption-based volatility.
- **Operational noise:** High volumes of low-value alerts were overwhelming internal IT teams, reducing their ability to focus on genuine threats.
- **Varied service needs:** Different departments and services required different response times and coverage windows, from 24/7 monitoring for critical systems to business-hours support for administrative services.

Solution

The organisation partnered with NG-IT to select a specialist Security Operations provider to deploy a **fully managed SOC service** built around the following capabilities:

- **Unified visibility:** Integration with existing endpoint, network, and cloud security tools created a single, correlated view of activity across the entire environment.
- **Technology-agnostic approach:** The service was designed to work with the institution's current investments—including EDR, email protection, networking equipment, cloud and identity platforms—avoiding costly rip-and-replace programmes.
- **Predictable pricing:** A fixed annual subscription model aligned with public-sector budgeting cycles, ensuring transparency and long-term affordability.
- **Noise reduction:** Automated and human triage enrichment filtered out false positives, ensuring that only genuine, high-fidelity security alerts were escalated to IT teams.
- **Customisable service levels:** Tailored SLAs allowed the organisation to match response times and operating hours to the criticality of each system or service, optimising service delivery & resources without compromising protection.
- **Multi-site coverage:** The SOC provided consistent monitoring and response across all campuses, regardless of local infrastructure differences.

Conclusion

- **Reduction in alert noise**, enabling internal teams to focus on strategic security improvements rather than reactive firefighting.
- **An outcome focussed service**, by incorporating environment specifics and context with an enhanced level of detection logic and alert efficacy the team were able to concentrate their efforts more effectively.
- **Full estate visibility** across multiple campuses and inclusive of on-premises & cloud, environments, significantly improving threat detection and response times.

- **Improved compliance posture** for data protection and alignment with regulatory requirements.
- **Cost predictability** that aligned with public-sector financial planning and avoided unexpected operational expenditure.
- **Enhanced resilience** across critical teaching, research, and administrative services through tailored SLAs and 24/7 monitoring where required.
- **Stronger security culture** as internal teams gained confidence in the clarity, accuracy, and relevance of escalated alerts.

Clients

Contact Details

For any questions regarding this offer, please send an email to ***gcloud@ng-it.co.uk*** and we will respond as quickly as possible to assist with your request.