

G-Cloud 15

Service Definition

Arctic Wolf Aurora Managed Endpoint Defence (MED/MDR)

NG-IT

Lot 2a - Infrastructure Software as a Service (iSaaS)

1. Introduction	3
Company Overview.....	3
Social Value	3
Overview of the G-Cloud Service	7
Associated Services	11
2. Data Protection	12
Information Assurance.....	12
Data Back-Up and Restoration.....	12
Business continuity statement/plan	13
Privacy by Design	14
3. Using the service.....	15
Ordering and Invoicing.....	15
Availability of Trial Service	15
On-Boarding, Off-Boarding, Service Migration, Scope etc.	15
Training	16
Service Management	17
Service Constraints.....	18
Service Levels	21
Outage and Maintenance Management.....	24
Financial Recompense Model for not Meeting Service Levels	24
4. Provision of the service	25
Customer Responsibilities.....	25
Technical Requirements and Client-Side Requirements.....	26
After-sales Account Management	27
Termination Process	28
5. Our experience	28
Case Study.....	28
Clients.....	30
Contact Details.....	31

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.

Arctic Wolf Aurora Managed Endpoint Defense (MED/MDR)

The Arctic Wolf Aurora Managed Endpoint Defense (MED/MDR) Solution provides a 24x7x365 managed endpoint detection and response offering in which Arctic Wolf SOC analysts monitor and manage Customer threats using Aurora Endpoint Defense (including email and web interactions) and closed-loop communications with direct phone access to Arctic Wolf SOC analysts. Arctic Wolf SOC analysts help Customer navigate incidents and provide regular updates on overall threat prevention status, analysing and responding to data log feeds from Aurora Protect and Aurora Endpoint Defense, and provide regular reporting access through the Portal.

In addition to the core technologies offered to all Arctic Wolf solutions that are listed here, the below Arctic Wolf Technology item sets forth, in general, the Arctic Wolf Technology and the various features and tools that may be included as part of the MED 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 an ordering document (i.e., Order Form).

Aurora Protect Arctic

Wolf Aurora Protect is a next-generation AI-driven endpoint protection solution designed to prevent malware and ransomware attacks before they execute. Originally known as Cylance PROTECT, Aurora Protect delivers autonomous threat prevention without relying on traditional signatures or frequent updates. By leveraging a machine learning engine trained on billions of file features, it stops known and unknown threats with high efficacy and low system impact.

Aurora Protect provides organisations with:

- Preventive Security at the Endpoint: Stops malicious executables, scripts, and exploits before they run.
- Autonomous Protection: Works online or offline, with minimal need for cloud lookups or user interaction.
- Low Operational Overhead: Reduces alert noise and eliminates the need for frequent signature updates or definition management.
- Consistent Protection Across Operating Systems: Supports major desktop and server OSes including Windows, macOS, and Linux distributions.
- Seamless Integration with Arctic Wolf's Security Operations (where applicable): Enabling threat correlation, enriched response actions, and better context when used alongside other Arctic Wolf offerings.

Aurora Endpoint Defense

Aurora Endpoint Defense builds on the capabilities outlined in Aurora Protect, combining AI-powered prevention with endpoint detection and response. In addition to machine learning-based malware prevention and layered controls, AED leverages the Aurora Focus Agent to provide behavioral threat detection, telemetry collection, and response actions— enabling organizations to detect, investigate, and respond to threats from a single interface.

Aurora Focus Agent

The Aurora Focus Agent enhances endpoint protection with autonomous detection, investigation, and response—executed directly on the device. It continuously monitors system activity, applies behavioural detection logic locally, and enforces automated responses without relying on cloud connectivity. Operating alongside the Aurora Protect Agent as part of Aurora Endpoint Defense, it delivers rich telemetry and actionable insights in real time, even in offline or low-connectivity environments.

Note: *Some capabilities may not be available in all versions of the Aurora Focus Agent or on all supported operating systems. Refer to the product documentation for a complete understanding of these dependencies.*

Behavioural Threat Detection

Identifies malicious activity based on suspicious behaviours, tactics, and execution flows— without relying on traditional IOCs or signatures. Continuous Endpoint Telemetry Captures detailed telemetry on the endpoint to support investigations, threat hunting, and retrospective analysis by monitoring the following event types:

- Application
- Device
- File
- Memory
- Network
- Process
- Registry
- Scripting
- SharedObjects
- System

- Threat

User Note: Available sensors may vary based on Agent version, platform, and platform version. Check product documentation for your configuration.

Local Detection and Policy Response

Executes detection logic locally and enforces automated responses such as process termination, file deletion, or user logoff based on defined policies.

Hunting and Investigation

Support Enables security teams to explore endpoint activity, trace attack paths, and validate threats using high-fidelity data enriched with context.

Integrated Response Capabilities

Allows rapid remediation actions—including isolating hosts or applying custom remediation scripts—without requiring third-party tooling.

Data Retention

Arctic Wolf's Endpoint defense standard log retention is thirty (30) days

Managed Endpoint Defense Workbench

The Arctic Wolf Managed Endpoint Defense Workbench is a self-service tool, that can be accessed stand-alone or via the Arctic Wolf Unified Portal, that provides a single point of access to your licensed Aurora Endpoint Security Solutions and a channel to collaborate with your Security Team.

As part of Aurora Managed Endpoint Defense, the Workbench allows you to perform the following tasks:

- View Security Alerts (aka Escalations)
- View configuration health score and details on the configurations
- Access dashboards and reports
- Update contacts
- Manage permissions, and organizational profile information.
- Manage Aurora Endpoint Defense security policy.

We have two primary interfaces for Aurora Endpoint Security:

1. Managed Endpoint Defense Workbench, will have all the features above for single tenant customers
2. Multi-Tenant Managed Endpoint Defense Workbench will have all the features above for multi-tenant customers (e.g. MSP Partners, Conglomerates). Multi-Tenant customers will have a consolidated view for its own tenant and all affiliated subtenants including Security Alerts (aka Escalations) health score, and dashboards.

If your subscription includes a CST Tier, your CSTs involvement and participation in the Solution will be enhanced in accordance with the specifics of the CST Tier selected by you for your subscription. The following may be included with your MED subscription:

- Solution Management – Arctic Wolf may manage policy settings within the Solution to facilitate better detection and response readiness.
- Endpoint1 Detection and Response – Alerts generated by security events from the Solution will be detected, triaged, researched, and responded to in accordance with the approved actions.
- Threat Hunting, Reporting, and Advisory Services.

Services Subscription

The above services are 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 AW Aurora Managed Endpoint Defence (MED-MDR) 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

As a starting point, you will receive a Welcome Email from the Service Provider and an invitation to schedule a kick off call. This serves as a formal starting point and you will be introduced to the team that will work with you during the implementation period. During the kick off call, it is expected that the Service Provider walks through the initial scope of the service, get a mutual understanding of what is included and outline next steps.

- The effort required to onboard to the service is minimal, but there are a few activities below that are required by the customer IT team:
- Attend the Onboarding and Technical Kick Off calls (1 hour each)
- Add required information in Customer Portal (30 mins)
- Connect the MDR Network Sensor (30 mins in firewall site)
- Download and deploy Managed Risk internal scanner (30 mins)
- Deploy Arctic Wolf agent (typically automated through software deployment tool like SCCM)
- Configure syslog sources to forward to network sensors (30 mins)
- Attend handover call to Concierge team (1 hour)

We have outlined a timeline of the process to facilitate its comprehension:

Phase 1 - Onboarding Kick off (Day 1)

Phase 2 - Technical Kick off (Day 2 to 5)

Phase 3 - Sensor/Scanner install (Day 5 to 25)

Phase 4 - Essentials (Day 25 to 35)

Phase 5 – Readiness (Day 35 to 40)

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.

Escalation Paths and Policies

Escalation paths and policies include details to tell the SOC and CST who should be contacted within your organization, in the event of a Security Incident or Emergency.

You are encouraged to have at least two escalation paths defined and your Deployment Security Team (DST) will help you navigate the right escalation processes for your organization during onboarding. There are no limits to the number of escalation paths that you can define, and you can change, add, or remove them via self-service in the Unified Portal or by collaborating with your CST following onboarding.

Escalation policies may support different escalation paths based on incident type – for example, all endpoint incidents can be routed to one contact, while all email incidents can be routed to another.

Escalation policies support multi-tenant environments. A parent customer can customize the policies and limit escalations to its own members or extend it to some or all subtenants its affiliated with.

Response Action Policies

Response Action policies tell the SOC and your CST, if applicable, when they can contain or action on an identified threat. As part of MED, Arctic Wolf will use reasonable efforts to perform Response Actions which include, but are not limited to, the following:

Response Actions	Description
Application Logs	The agent logs detection events to the Windows application log.
Delete Files	The agent permanently deletes any file artifacts that are identified as an artifact of interest (AOI).
Delete Registry Keys	The agent permanently deletes the entire registry key of any AOI that are identified as registry artifacts.
Delete Registry Values	The agent permanently deletes the registry value of any AOI that are identified as registry artifacts.
Dump Detection to Disk	The agent creates a detection data file in the Aurora Endpoint Defense application data directory.
Log Off All Users	The agent logs off all interactive and remote users.
Log Off Users	The agent logs off the specified users.
Log Off Interactive Users	The agent logs off all users that are currently physically interacting with the device.
Log Off Remote Users	The agent logs off all users that currently have a remote session established on the system.
Notification Window	The agent displays a notification window with the detection notification message that you specified, using the native OS notification box instead of the Aurora Protect agent.
Suspend Processes	The agent suspends any process artifacts that are identified as an AOI.

Response Actions	Description
Suspend Process Trees	The agent suspends the entire process tree of any process artifacts that are identified as an AOI. The AOI is treated as the root of the tree
Terminate Processes	The agent terminates any process artifacts that are identified as an AOI.
Terminate Process Trees	The agent terminates the entire process tree of any process artifacts that are identified as an AOI. The AOI is treated as the root of the tree.
Whitelist Processes	This option excludes the specified processes from being observed by Aurora Focus.
Remote Access for Custom Actions	Remote connection to Endpoint for custom actions (subject to customer approval)

The default Response Action policy is “always enable Response Actions” to allow the Arctic Wolf SOC to stop threats and threat actors, minimizing the impact of a Security Incident. Your DST (during onboarding) and your CST (after deployment) can help you document the Response Actions policy that is best for your organization.

Based on (i) the information you provide to your CST following deployment, (ii) a mutually agreed upon escalation policy, the SOC may remotely isolate your endpoint device(s) that show evidence of compromise or other suspicious activity. When the Security Services Team identifies certain indicators of attack on an endpoint the Response Action will be initiated in accordance with the agreed upon escalation policy to rapidly quarantine the suspected compromised system or account.

The indicators of attack that may drive Response Actions include those relating to ransomware (and other types of malware), malicious command-and-control (C2) activity, or active data exfiltration attempts.

The endpoints participating in the Response Actions will receive a notification and the Response Actions will be detailed in an incident ticket. The Security Services Team is available to you to answer questions or provide detailed information on any endpoints participating in the Response Action.

In multi-tenant environment, response actions can be customized per tenant or globally across all tenants.

Incident Investigation, Notification, and Guided Remediation

Security Investigations and Security Incidents

The telemetry data accepted and ingested by Arctic Wolf that is deemed critical and/or is interesting and relevant from a security perspective, may prompt further analysis by the Arctic Wolf Platform and/or a member of the SOC— this is called a Security Investigation. During the Security Investigation, the SOC may collaborate with you to do further investigation, detail Response Actions, remediate the discovered issue(s), and/or provide a detailed report of the Security Investigation – if these events occur, we identify this as a Security Incident.

You may also request that Arctic Wolf conduct a Security Investigation for data and/or situations that Arctic Wolf does not deem critical and/or interesting and relevant. As part of any Security Investigation, Arctic Wolf will:

- Provide validation of a Security Incident as detected through the Arctic Wolf Platform.
- Participate in calls with your in-house and/or third-party incident response team.
- Provide findings of data captured pertaining to the Security Incident within the Arctic Wolf Platform.
- Provide a report of findings for the Security Investigation upon request.
- Provide recommendations, documentation, and best practices relevant to the Security Investigation.

Notification

The Arctic Wolf SOC is responsible for notifying you of discovered Security Incidents.

The SOC's notification process is done through a security alert ticket via our ticketing system to you, as specified in the escalation paths you have in place within your escalation policies. In the case of an emergency the SOC will also attempt to call customer contacts in priority order and will leave voice mails if necessary.

Security Incident notifications will/may include a description of the Security Incident, the level of exposure, any actions taken prior to the notification, and the suggested remediation steps remaining.

Notifications service is supported in multi-tenant environments. A parent customer can customize notifications and limit it to its own members or extend it to some or all subtenants its affiliated with

Guided Remediation

The Arctic Wolf SOC and other members of your Arctic Wolf security team, if applicable, will provide remediation guidance to return your environment to operational status if there is a compromise (e.g., by providing action-oriented guided remediation instructions that you can perform). A typical example of guided remediation would include written or verbal instruction delivered via a security alert or via a call, to remove such malicious applications as persistence mechanisms or malware. If you should require further assistance, you may separately engage Arctic Wolf's Incident Response Team, subject to the terms and scope in an agreed upon statement of work (SOW).

Threat Hunting

Arctic Wolf will, on an ongoing basis, collect artifacts and information within the Customer's environment to facilitate hunting of potential security threats. Should a security threat be identified, Arctic Wolf will inform you of these findings.

Reporting

Through the Arctic Wolf Portal, you have access to several pre-defined dashboards as well as the ability to create new dashboards to surface data appropriately for your business. In addition, and if necessary, your CST, if appropriate, may assist in the creation of other regular reports.

The reports will either be automatically generated and sent to you by the Solution, created and reviewed by your CST and issued to you, or available in the Arctic Wolf Portal as a PDF or as a live dashboard.

Advisory Services

The Advisory Services program is a software maintenance service of Aurora Managed Endpoint Defense, and Aurora Endpoint Defense technologies for Customers that have already completed Onboarding Services. The Advisory Services program builds off the Onboarding Services to assist customers in achieving optimal configuration and security benefits. The objective of the Project is to report, assess, and review the existing configuration and status of Aurora Managed Endpoint Defense,

and Aurora Endpoint Defense solutions. The service is delivered on a quarterly basis presenting the Health Check Report.

The findings of the Health Check Report are the focus of this service. In cases where the Health Check Report classifies Customer as being in good standing, the Arctic Wolf team will seek to identify additional areas to enhance Customer's security posture by performing auditing or additional training. In cases where the Health Check Report classifies Customer as not in good standing, the Arctic Wolf team will identify areas of noncompliance with or deviations to the Arctic Wolf acceptable security configuration settings, and any other recommendations to assist Customer in optimizing Aurora Endpoint Defense. Advisory Services include one (1) or more of the following, as determined between Customer and Arctic Wolf during quarterly check-ins:

- Health Check Review
 - ✓ Report card review with associated recommendations to identify drift from or deviations to Arctic Wolf acceptable security configuration settings
- Advanced Settings, Audit, and Recommendations
 - ✓ Audit and recommendations
 - ✓ Upgrade recommendations and guidance
- Additional Training
 - ✓ Additional training on new features, best practices, and maintenance routines o Working session(s) for questions and answers regarding Customer-driven use cases

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 SOC's on a 24/7 basis, services for UK customers would be provided by their EMEA SOC's based in Germany and Ireland.

All Security Incidents are assigned a severity level2 as follows:

Severity Level	Description	Example
Urgent	An active threat requiring immediate action. Incidents of this severity pose a high risk of data loss, service disruption, or significant financial/legal consequences.	• Ransomware attack encrypting large portions of critical infrastructure • Zero-day Exploit
Severity Level	Description	Example
		• Massive Data Exfiltration
High	A considerable threat that could lead to significant compromise or disruption if left unaddressed. Incidents of this severity require immediate attention.	• Malware/Botnet Detected • HTTP Download of Malicious Payload
Medium	Security Incidents with this severity level generally involve a security vulnerability or suspicious activity that may require attention.	• Individual host or Widespread targeting but no sign of compromise
Low	Security Incidents with this severity level involve security posture issues with low impact or benign activities that don't pose a significant threat.	• Individual host or non-critical user

The response time service levels for the specified inquiries, Security Incidents, and Emergencies are as follows:

Action	Service Level
Acknowledgement of any schedule request submitted by you to security@arcticwolf.com	One (1) hour from receipt of request.
Acknowledgement of receipt of any Security Incident (inbound) submitted by you to security@arcticwolf.com	One (1) hour from receipt of request; Security Services will follow up with you with an estimate of response time determined by scope, size, and urgency.
Notification and escalation of any Security Incidents (outbound notice)	Two (2) hours of Arctic Wolf's discovery.
Escalation of any Emergency (outbound notice)	Thirty (30) minutes of Arctic Wolf's discovery.
Action	Service Level
Emergency escalated via phone to the SOC (inbound notice)	Arctic Wolf will respond within five (5) minutes; you will be required to describe the Emergency. In the unlikely event that your call goes to Voice Mail, the caller must leave a message to receive a reply.

Emergencies generally include any Urgent Severity Security Incident and other Severity Security Incidents at the discretion of the analyst that could cause degradation or an outage to your systems and infrastructure. Arctic Wolf's standard Security Incident (as defined below) notification process is through a ticket to your administrator(s); however, we may agree to alternate notification processes. Security Incident notifications will include a description of the Security Incident, the level of exposure, and a suggested remediation strategy.

Note:

- *Solution delivery, including specifically, notification of Emergencies or Security Incidents, will commence once deployment is complete.*

- *Remediation services for Security Incidents, the re-imaging of your systems, or change of policy settings is outside the scope of MDR.*

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 timely 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 AW Aurora Managed Endpoint Defence (MED-MDR) 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.

To ensure that full value of MED is received, each party's roles and responsibilities are defined in the table below.

Activity	Arctic Wolf	Customer
<i>Deployment</i>		
Agent installation		X
Policy Tuning	X	
Escalation path purpose communication	X	
Escalation path definitions		X
Response policy definitions		X
Restricted countries definition		X

Activity	Arctic Wolf	Customer
Select opt-in alerts		X
Site configuration		X
Contacts definition		X
<i>Ongoing</i>		
Response Actions configuration	X	X
Initiate and conduct Response Action(s)	X	
Provide guided remediation	X	
Enact remediation recommendations		X
Alert Escalation-remediation		X
Alert tuning	X	
Alert suppressions	X	X
Custom Detections configuration and remediation	X	X
Maintain Endpoint configuration health and protection coverage	X	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 met 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

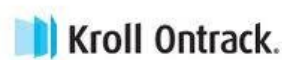
Who we do it for – Public Sector/Charities



University of
Sunderland



Who we do it for - Commercial



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.