PANACEA NETWORKING

G-CLOUD 15
SERVICE DEFINITION

Panacea Care

Managed Service Solutions for Extreme Networks

Panacea Networking

Lot 2a Infrastructure Software (I-SaaS)

1 Introduction

Company Overview

Panacea *"a solution or remedy for all difficulties"* is a specialist, dedicated Extreme Networks solution provider**.**

Panacea's sole focus on Extreme means every project benefits from deep expertise across the full portfolio. That specialism gives us a distinctive position in the market. By concentrating our time, expertise and resources on one platform, we provide support and insight that generalist providers often struggle to match.

The key to a successful Extreme Networks deployment is more than just installing hardware or following best practice. It's about understanding the entire ecosystem and how each component fits and operates together. Because our engineers are proficient across the full Extreme portfolio, we can shape solutions that are balanced, future-proof, and designed to maximise the value from your investment.

Our technical team includes engineers with Extreme's highest-level certifications, backed by decades of experience. This means the advice we give and the solutions we implement are grounded in deep product knowledge and proven in real-world environments.

Our track record includes some of the most demanding sectors in healthcare, government, and defence, where networks are as critical as they come. In these environments, we've delivered successful, referenceable deployments replacing entire infrastructures with minimal disruption. In fact, complete migrations have been achieved with downtime measured in single ping drops, thanks to our understanding of clinical requirements, service priorities, and the operational stakes involved.

With more than 20 years' experience and engineers holding Extreme Networks' highest technical accreditations, Panacea has built a reputation for delivering advanced enterprise infrastructures that maximise performance and value, giving customers confidence that they are working with a trusted safe pair of hands.

What sets us apart is an engineering-led, customer-first philosophy. Projects are led by seasoned Extreme professionals, ensuring advice is grounded in real-world expertise, solutions are tailored to client needs, and partnerships are built on transparency, trust, and consistent delivery.

Value Proposition

Modern organisations depend on networks that are more than just utilities, they are lifelines. Whether in healthcare, government, education, or enterprise, downtime directly affects people, services, and trust. In these environments, resilience, accountability, and security are non-negotiable.

What our customers value most is how personal our service feels. When something matters, you don't get passed through layers of support, management or unknown faces. You pick up the phone or open Teams and speak directly to the engineer who already knows your network inside and out, someone accountable, familiar, and ready to act. That instant access to real expertise builds confidence, because you know problems will be owned and resolved without delay.

Panacea brings together direct accountability with deep technical expertise. Our SLA-backed support, transparent pricing, and engineering-led delivery ensure critical infrastructures perform under pressure. The result is connectivity that is not only reliable and cost-effective, but supported by people you know and trust, a genuine safe pair of hands when it matters most, a phrase synonymous with Panacea.

What the Service Provides

Panacea delivers managed networking services built exclusively on Extreme Networks technologies. Our service combines technology, support, and outcomes to give organisations secure, scalable, and high-performance connectivity, with a constant focus on efficiency, automation, and reliability.

- **Technology** – Advanced cloud-managed switching, wireless, fabric, and SD-WAN solutions form the backbone of our services. Deployments are accelerated through zero-touch provisioning and automated configuration, reducing complexity and human error. We use automation, analytics, and (where available) AI-driven features to support continual optimisation and incremental efficiency gains. In addition, Panacea develops custom applications that automate processes, deliver faster deployments, and ultimately reduce costs while increasing reliability.
- **Support** – SLA-backed service tiers from business hours through to 24×7 cover, delivered directly by dedicated vendor-certified engineers who already understand your environment. Flexible Bolt-On Hours provide additional engineer-led consultancy, basic training, or migration support. Customers gain immediate access to the people accountable for their network, with no layers of delay.
- **Outcomes** – Resilient infrastructures that not only reduce risk and simplify management, but also save time and cost through automation and streamlined

processes. With engineering-led delivery from people who understand the challenges at the frontline, Panacea provides trusted connectivity for critical environments in healthcare, government, defence, and beyond. The result is a network that is more reliable, more efficient, and more sustainable to operate.

Technology

- Cloud-managed networking.
- Enterprise switching and routing (campus, edge, and data centre networks)
- Wireless LAN & mobility (Wi-Fi 6/6E/7 and beyond, designed for dense, high-stakes environments like healthcare, education, stadiums)
- Fabric networking (simplified, secure, automated segmentation and provisioning)
- SD-WAN and distributed enterprise (secure cloud-first connectivity across sites)
- Network security and access control (identity-driven policies, segmentation)
- Use of analytics and AIOps features.

Support

- **Tiered SLA-backed support plans** – Spanning Essential 8×5, Waking-16×5, Extended 8×7, Prime 16×7, and Complete 24×7, with defined Time to Acknowledge (TTA) and Time to Engage (TTE) targets for incidents, on-site dispatch times, and clear escalation paths. Each coverage tier is available as a Standard or Enhanced plan, as defined in the Panacea Care Pricing and Call-Off documents.

- **Scalable bolt-ons** – Support packages grow with your network. Extra professional services time, remote hours, or site visits can be added at fixed, predictable rates to match evolving requirements.

- **Engineering-led delivery** – Delivered by vendor-certified Extreme Networks engineers with decades of practical experience. We keep accountability tight, a named technical lead oversees the engagement, and the engineering team remains your day-to-day contact.

Outcomes

- Reliable networks designed to support critical public sector operations
- Minimal disruption during migrations, proven in healthcare, government, and defence environments where downtime tolerance is near zero
- Transparent pricing and predictable service costs
- Resilient, flexible, and compliant infrastructures aligned with national security and governance requirements
- Long-term partnerships built on trust, technical depth, and measurable performance improvements

Social Value

Panacea is a specialist SME, so our commitments focus on practical, measurable actions that we can reliably deliver. Social value activity will be proportionate to contract size and reported through agreed governance, such as service reviews and contract meetings.

Kickstart economic growth

Panacea contributes to economic growth by providing highly specialised Extreme Networks expertise into the public sector and by participating as an SME within larger supply chains.

- We offer fair and transparent commercial terms that make it easier for public sector buyers to engage a specialist SME.
- We support skills development in public sector networking, particularly around Extreme Networks and healthcare environments.

Objective

Over the life of any agreement, we will deliver at least one structured knowledge-sharing activity per year (for example a technical workshop or shadowing session) for NHS or wider public sector staff involved in our projects.

Metrics & monitoring

- Number of knowledge-sharing activities delivered per year
- Attendance numbers and short feedback from participants
- Summary reported in annual contract or service review meetings

Governance / policies

- Led by a Panacea Director or nominated Lead Engineer
- Supported by our internal Skills and Development approach (documented role profiles and training plans)

Make Britain a clean energy superpower

Panacea operates a remote-first delivery model wherever appropriate, which reduces travel and associated emissions while maintaining service quality.

- Our default is remote consultancy and support, with on-site attendance only where necessary for hands-on work, urgent support, call-outs or stakeholder engagement.
- Our Environmental Management System is accredited to ISO 14001 and is used to ensure that environmental aspects (including travel) are identified, monitored, and continually improved over time.

Objective

For contracts under any agreement, we will aim to maintain at least 60% of consultancy and support time delivered remotely over each 12-month period, unless a different balance is agreed with the customer.

Metrics & monitoring

- Ratio of remote vs on-site time, using our time-recording and scheduling tools
- Estimated travel mileage associated with on-site work
- ISO 14001 management reviews and audits, available on request

Governance / policies

- Managed through our ISO 14001 Environmental Policy and objectives
- Overseen by a Panacea Director with responsibility for environmental performance

Break down barriers to opportunity

We are a people-first, engineering-led business. Our focus is on capability, fairness, and giving engineers clear opportunities to develop and take ownership.

- Recruitment and progression are based on skills and capability, using consistent role profiles and interview criteria.
- All staff have access to relevant training and development, regardless of their background or location.

Objective

We will ensure that 100% of staff in core delivery roles receive at least one job-relevant training or development activity per year (for example vendor training, internal mentoring, or structured self-study).

Metrics & monitoring

- Training and certification records per staff member
- Internal check of training completion as part of annual performance reviews

Governance / policies

- Underpinned by our Equal Opportunities and Recruitment Policy
- Oversight by the Directors, with development plans owned by a named lead and reviewed with each team member regularly

Build an NHS fit for the future

Panacea has experience delivering resilient network solutions into NHS and healthcare environments, where service continuity directly impacts patient care.

- We design and support Extreme Networks solutions that improve reliability, visibility, and manageability of clinical and corporate networks.
- Our delivery model supports out-of-hours changes and remote support to minimise disruption to clinical services.
- We also contribute to the wider community. For example, we have designed, delivered, and continue to support a wired and wireless Extreme Networks solution for a charity providing horse and pony lessons for disabled children, free of charge.

Objective

- For each NHS customer under any agreement, we will hold at least one structured service review per year, focused on resilience, incident performance, and opportunities to support clinical service continuity.
- Over the term of any agreement, we will maintain at least one active pro bono or community support initiative aligned to our networking expertise, subject to viable opportunities.

Metrics & monitoring

- Number and outcomes of annual service reviews for NHS customers
- Priority 1 incident performance against agreed SLAs (where Panacea is responsible)
- Simple annual statement of pro bono / community initiatives and support effort provided

Governance / policies

- Social value delivery is overseen by Panacea's Directors
- Day-to-day responsibility sits with the named Lead Engineer for each contract, who coordinates delivery and acts as the primary point of contact
- Progress against the above objectives can be included as a standing item in contract or service review meetings

Overview of the G-Cloud Service

Panacea provides cloud-aligned managed support service for Extreme Networks environments. The service is delivered remotely using Extreme's cloud management and monitoring platforms, together with Panacea's vendor-accredited engineers, to keep customer networks secure, available, and compliant.

Panacea's service is delivered in conjunction with an active Extreme Networks support entitlement that provides access to GTAC for all in-scope hardware and software. This entitlement must be in place for the duration of the service and may be held directly by the customer or procured through Panacea. Panacea operates as an overlay or co-delivery partner and does not replace the vendor support contract, which remains the route for hardware replacement, bug diagnostics and other GTAC-level escalations.

In practice there are usually two separate third-party vendor charges in an Extreme environment: (1) subscriptions for the vendor management platforms used to operate and monitor the estate, and (2) manufacturer support entitlements for the in-scope hardware and software (for example GTAC access and hardware replacement cover).

Because these are set by the vendor (and may vary with exchange rate and vendor price changes), Panacea does not publish fixed prices for vendor items under this G-Cloud listing. The pricing in this Service Definition and the Care Pricing Schedule covers

Panacea's managed service and support overlay only. The Buyer is responsible for maintaining the required vendor subscriptions and support entitlements for the duration of the service, either held directly or procured separately.

Key service capabilities

The service is structured around clear SLA-backed support tiers:

- Essential 8×5 (Mon-Fri, 9am-5pm)
- Waking 16×5 (Mon-Fri, 8am-12am)
- Extended 8×7 (Mon-Sun, 9am-5pm)
- Prime 16×7 (Mon-Sun, 8am-12am)
- Complete 24×7 (All Hours)

Each tier defines Time to Acknowledge (TTA) and Time to Engage (TTE) targets for Priority 1–3 incidents, with progressively tighter targets and wider coverage at higher tiers.

Every coverage tier is available in two configurations:

- **Standard**
  - Reactive incident response backed by published SLAs
  - Access to Panacea's Extreme Networks engineers for diagnosis and remediation
  - Configuration backup and restore
  - Coordination with Extreme Networks GTAC where required
- **Enhanced**
  - All Standard features
  - Proactive monitoring and alert handling using Extreme's cloud management and analytics platforms for supported Extreme devices and licensed features. Where specific monitoring, analytics or KPI requirements exceed what these native platforms can provide, additional monitoring or reporting tooling can be agreed as a separately priced option at Call-Off.
  - Optional out-of-band access on critical devices where supported
  - Faster TTE targets for higher-severity incidents

Pricing is per device with volume discounts, so organisations can scale their Extreme Networks estates (for example switches and access points) in a predictable, unit-based manner as new sites and services are brought under cloud management.

Cloud characteristics and benefits

The service uses Extreme's cloud management platforms (for example ExtremeCloud IQ) and related SaaS tooling as the primary control plane for supported networks. These platforms provide:

- Cloud-hosted, multi-tenant management for Extreme devices
- Centralised configuration, policy, and firmware management
- Automated updates and controlled rollout of changes
- Telemetry, monitoring, and alerting across campus, branch, and remote sites
- AI/ML-assisted insight and diagnostics where available within the platform

Panacea's engineers operate through these cloud platforms to:

- Apply policy and configuration changes consistently across the environment
- Monitor health, performance, and availability in near real time
- Respond to incidents and service requests without requiring on-site presence in most cases
- Scale support across multiple customers while maintaining strict separation and governance between tenants

Security and governance are integral to the way the service is delivered. Role-based access control within the cloud platforms, network segmentation, and alignment with UK data protection requirements are standard. Panacea's operations are independently accredited to ISO 27001 (information security), ISO 9001 (quality management), ISO 14001 (environmental management), ISO 42001 (AI management), and Cyber Essentials Plus, providing assurance that the cloud management and support processes are controlled and audited.

Associated Services

Alongside our managed support services, Panacea provides a range of additional capabilities that organisations can draw on where needed. These associated services are delivered under our Panacea Consult offering. Within this document, the terms Panacea Consult, Tailored engagements, and Professional services are used interchangeably to describe the same pool of consultancy and project delivery capability. All such services are scoped and priced separately from the core Care service; please refer to our rate card / Panacea Consult pricing for detailed pricing.

- **Enhanced monitoring and alerting** – Deeper device and service visibility (availability, performance, interface health, configuration change detection, proactive alerting and reporting). Can include monitoring across multiple sites and agreed escalation workflows.
- **Remote out-of-band access management** – A resilient remote access method for network equipment that remains available during WAN or primary circuit outages (subject to site constraints). Includes design, configuration, secure access controls, and ongoing management.

- **Network documentation and topology reporting** – Automated discovery and maintenance of network inventory and topology, with exportable diagrams and structured documentation (for example, IP addressing, VLANs, device roles, and site layouts), kept current as changes are implemented.
- **Wireless surveys and advanced diagnostics** – Predictive and on-site survey work, validation testing, and targeted troubleshooting (coverage, capacity, interference, roaming, spectrum and performance analysis). Delivered with findings, recommendations, and supporting artefacts (for example heatmaps and remediation actions).
- **Extreme Networks certification-aligned training and knowledge transfer** – Structured training for operational teams through to advanced engineering topics, aligned to recognised certification pathways where required. Delivered remotely.

2 Data Protection

Information Assurance

Panacea operates to the highest recognised standards for information assurance and service management. Our operations are independently accredited to:

- **ISO 27001** – Information Security Management
- **ISO 9001** – Quality Management
- **ISO 14001** – Environmental Management
- **ISO 42001** – AI Management
- **Cyber Essentials Plus** – UK government approved baseline security.

Data Backup, Restoration and Disaster Recovery

Panacea operates a structured Business Continuity and Disaster Recovery (BCDR) approach to protect customer and internal data against loss, corruption, or unavailability. Our policies and processes are aligned to ISO 27001 (Information Security) and Cyber Essentials Plus, ensuring that data protection and recovery are governed by independently audited security controls.

Backup Approach

- We adopt a multi-layered backup strategy, ensuring at least two independent copies of all critical data are maintained at any given time.
- Data is stored across Microsoft 365 services (SharePoint, OneDrive, Exchange, Intune) with cloud-native versioning and retention.
- Additional copies are held on secure Panacea operated Synology storage to provide local resilience and rapid access.

- This combination provides redundancy across cloud and local systems, protecting against vendor service issues or location specific disruption.

Processes and Frequency

- Microsoft 365 platform-native retention and recovery capabilities are used, and we support configuration and restore actions where required.
- Local Synology devices maintain the more than one copy baseline approach, keeping a live mirror image of cloud data.
- Encryption is applied in transit and at rest.

Restoration and Testing

- Restoration procedures are documented, regularly tested, and reviewed in line with ISO 27001 requirements.
- Test restores are carried out on a scheduled basis to validate data integrity and recovery times.
- Disaster Recovery plans are reviewed and updated annually or following material changes in the infrastructure.
- Options for Out-of-Band (OOB) management and GSM failover are available at the Enhanced support tier.

Contingency and Governance

- Business Continuity and Disaster Recovery (BCDR) plans are maintained and available to customers on request.
- Governance controls define responsibilities, escalation procedures and target Recovery Time Objectives (RTOs) and Recovery Point Objectives (RPOs) for our internal services.
- Client specific requirements relating to backup, retention or restoration of project artefacts can be discussed prior to an order being placed and then documented in the Order Form as agreed between both parties.

This approach ensures that Panacea can recover data quickly and reliably, while providing customers with assurance that data is being protected and managed under stringent governance at all times.

Business Continuity Statement/Plan

Panacea maintains a formal Business Continuity and Disaster Recovery (BCDR) plan to ensure that essential functions continue with minimal disruption in the event of an incident. The plan is designed to provide a flexible response so that we can:

- Respond effectively to a disruptive incident.
- Maintain delivery of critical activities and services during the incident.

- Resume “business as usual” as quickly as possible.

Scope and Key Areas

The plan covers all core business operations including Microsoft 365 services (Outlook, OneDrive, Teams), telephony (main number and mobiles), premises, laptops and desktops, network infrastructure, backups, website, personnel, and accountancy.

Critical Functions and Acceptable Downtime

Our target recovery time objectives are:

- Microsoft 365 and main phone number: target recovery within 2 hours.
- Network infrastructure and data backups: target recovery within 4 hours.
- Laptops/desktops: target recovery within 1 day.
- Mobile phones: target recovery within 1 day.
- Premises, personnel, and accountancy: target recovery within 48 hours.
- Website: target recovery within 1 day.

These objectives describe how we design and test our internal resilience. Contractual SLAs for the managed service are defined separately in the Service Levels section and the Call-Off Agreement.

Dependencies

The plan identifies dependencies across cloud platforms (Microsoft 365, OneDrive), local infrastructure (routers, switches, Synology NAS backups, and secondary connectivity such as satellite or 4G/5G), suppliers, and subcontractors.

Outline Plan

- **Emergency response** - initial assessment, staff communication (Teams, mobiles), and continuity using remote work and backup internet (for example secondary ISP or 4G/5G tethering).
- **Recovery actions** - hot spare equipment (routers, switches, laptops, mobile phones), Synology and Microsoft cloud backups, and documented processes for redirecting telephony.
- **Ongoing operations**: relocation to remote/home working if premises unavailable, continued client contact via mobiles/Teams/email, and prioritisation of critical functions by agreed recovery timeframes.
- **Governance**: the plan is reviewed annually, tested through drills, and updated following any major change.

A more detailed plan can be provided to the Buyer on request.

Privacy by Design

Panacea embeds privacy by design and by default into all of our services and operations, in line with GDPR requirements. From the outset of any service, we ensure that the protection of personal data is built into processes, technologies, and governance, rather than treated as an afterthought.

Our policies cover access control, data security, breach notification, privacy, and mobile use. These ensure that data is handled under strict governance, with role-based access, the principle of least privilege, secure device management, encryption, and proactive monitoring forming part of our everyday operations. We also apply document and data classification, so that information is categorised by sensitivity and managed with appropriate controls throughout its lifecycle. Where incidents do occur, our breach notification process provides a clear framework for reporting, escalation, and communication, including meeting the 72-hour ICO notification requirement.

All services are delivered within the scope of Panacea's accredited management systems, ISO 27001 for information security, supported by Cyber Essentials Plus, ensuring external oversight of our controls. Regular policy reviews, staff training, and annual penetration testing keep our approach current and effective.

For customers, this means privacy is considered throughout consulting engagements. Data is only collected and retained where necessary, processed transparently, and stored securely within UK-based data centres or approved cloud platforms. Customers retain full rights over access, correction, and deletion of their personal data.

3 Using the service

Ordering and Invoicing

Orders for Panacea's G-Cloud services can be placed by contacting gcloud@panacea-networking.co.uk. Buyers should provide a brief outline of requirements, including the chosen support tier (Essential, Waking, Extended, Prime, or Complete), any expected Bolt-Ons (for example additional devices or remote hours), and the required service start date.

Panacea will work with the Buyer to confirm scope, dependencies, and service levels. Once agreed, Panacea will prepare a G-Cloud Call-Off Order Form detailing the services, SLAs, timescales, and charges. The Order Form, once signed by both parties and accompanied by a purchase order, forms the contractual basis of the engagement.

Third-party vendor items (for example Extreme platform subscriptions and manufacturer support entitlements) are quoted at the time of order and are typically time-limited. Because these costs are vendor-set and may vary with exchange rate, they are not published as fixed prices in this G-Cloud listing. Where the Buyer asks Panacea to assist with ordering or renewals, Panacea will confirm the approach and any chargeable Bolt-on time in the Call-Off.

Invoices are issued in line with the Call-Off Contract terms (typically annual or quarterly in advance). Invoicing is transparent and linked to the agreed SLA tier and any agreed Bolt-Ons, ensuring predictable costs.

Availability of Trial Service

Panacea does not typically offer free trials, pilots, or proof-of-concept engagements. Where a Buyer requests a pilot, we will consider the requirement on a case-by-case basis and take a view based on commercial viability, delivery risk, and the clarity of the objectives and scope.

We otherwise provide assurance through relevant references (including from public sector customers, where permission is available) and through alignment with Extreme Networks, including case examples demonstrating successful outcomes in comparable environments.

Where appropriate, Panacea may offer a limited, paid engagement (for example time-and-materials or a short fixed-scope activity) to meet procurement requirements or support evaluation. Any such arrangement would be agreed in advance and documented within the Call-Off Order Form.

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

On-Boarding

Panacea's onboarding process is built around direct engagement with the engineers who will be supporting the service. From the outset, we prioritise becoming fully familiar with the customer's environment so that support is fast, accurate, and effective.

This typically involves:

- Working alongside the customer's IT team to review existing documentation and processes.
- Planned time on site and/or remote sessions to validate infrastructure, capture relevant configurations, and understand operational priorities.

- Documenting the environment to the level necessary to deliver the Care service, typically including high-level topology, key access details, and escalation paths.

Creation of comprehensive low-level design packs or full estate documentation is not included within the standard Care service. Where a more detailed, estate-wide record is required, Panacea can provide enhanced network mapping and documentation as a separately scoped and separately priced associated service.

This approach ensures Panacea's support team understands the environment in depth, so responses are informed and immediate rather than reliant on lengthy fact-finding.

Off-Boarding

If a customer decides to exit the service, Panacea supports a controlled and transparent transition. Standard off-boarding typically includes:

- An agreed exit plan and timeframe.
- All documentation, designs and deliverables produced during the engagement are handed over in an organised package.
- Secure revocation of Panacea access at the end of service.

Where a Buyer requires more support, Panacea can provide structured exit engagements as an optional, chargeable service. This may include joint design reviews, detailed transition documentation, and extended shadowing with an incoming supplier or in-house team. These activities are delivered on a time-and-materials basis using Panacea's Bolt-On rates.

Supported Estate

For the purposes of this service, the Supported Estate is the set of devices, sites, circuits and services listed in the Call-Off Order Form (or attached inventory) and confirmed during onboarding. Support under this service applies to the Supported Estate only.

Where the Buyer adds new sites, materially increases device counts, or introduces new technology domains, Panacea will agree the updated scope, any additional onboarding activity, and any resulting commercial changes in advance.

Service Migration

Where Panacea assumes support from another supplier, we focus on establishing a complete and accurate understanding of the environment. This may involve reviewing available historic records, validating current configuration, and conducting targeted health

checks to baseline performance. By working directly with customer staff, we support a seamless transition with minimal risk to ongoing operations.

Training and Knowledge Transfer

Panacea provides a practical service induction as part of onboarding. This focuses on how to engage support and operate the in-scope Extreme Networks environment day to day, including ticket logging, escalation, communications, and reporting.

More structured technical training is available as an associated, chargeable service. Sessions can be tailored to operational topics such as incident handling, configuration workflows, and management platform use. Where certification-aligned training is required, this can be provided as a separately scoped engagement.

Panacea can also signpost customers to official Extreme Networks resources, including product documentation, knowledge bases, and learning materials, to support ongoing skills development.

Vendor resources – Customers are also supported with access to official Extreme Networks resources, including documentation, knowledge bases, and Extreme Academy materials, which Panacea can signpost as part of training and onboarding.

Implementation Plan

A detailed implementation plan can be provided to the Buyer on request. The specifics, including timelines and customer-specific dependencies, will be finalised at the Call-Off stage.

Panacea follows a structured approach to service implementation to ensure a smooth and controlled transition into managed cloud support. A typical plan will include the following stages:

- **Kick-off and discovery** – initial meetings with the customer's stakeholders to confirm scope, selected service tier, in-scope environments, and escalation and contact details.
- **Environment familiarisation** – Panacea engineers work with customer IT staff to review existing documentation and management platforms and, where required and agreed, spend planned time on site or in remote sessions to capture infrastructure and configuration baselines.
- **Documentation and mapping** – the supported environments are documented at the level required to deliver the Care service, creating a reliable baseline for ongoing support (for example high-level network diagrams and key configuration references).

For more complex estates, and where the Buyer requires a detailed estate-wide record, this may include engagement, on a separately quoted basis, with our network mapping and documentation partner.

- **Service activation** – service desk access is enabled, SLAs and severity definitions are confirmed, and monitoring and alerting are configured using the agreed cloud management and support tools.
- **Handover into BAU** – the service moves into steady-state operation with SLA-backed incident response, proactive monitoring (where included in the chosen tier and supported by the in-scope platforms), and reporting as agreed.

This structure is then tailored at Call-Off to reflect the Buyer's specific environment, any prerequisite activities, and the target go-live date.

Service Management

Panacea manages its services through a structured, engineering-led model designed to ensure accountability, responsiveness, and transparency. Service delivery is governed by our tiered SLA framework, with clearly defined Time to Acknowledge (TTA) and Time to Engage (TTE) targets for different priority levels. All support requests are logged and tracked in our support platform, giving customers full visibility of progress, history, and escalation paths.

Customers work directly with the engineers who know their environment, helping ensure issues are owned end-to-end and resolved without unnecessary delay. Escalations are automated within our systems and can be directed to senior engineers or leadership for critical incidents, providing clear accountability at every stage.

Our processes are reinforced by regular service reviews, continuous improvement activities, and proactive monitoring (within the capabilities of the in-scope vendor platforms) to identify and address issues before they affect operations. This combination of SLA-driven performance, transparent tracking, and direct accountability gives customers confidence that services are being managed effectively and consistently, while maintaining flexibility to adapt to changing requirements.

From time to time, and at the customer's request, Panacea may provide assistance during incidents that is clearly outside the agreed managed support scope, where doing so is in the interests of restoring service. Examples include project-style implementation work, remediation of customer-led configuration changes, or extended fault-finding on inherited design issues. Where this occurs, the activity will be logged as reactive Bolt-On usage or

professional services time and charged at the agreed rates, with a clear post-incident breakdown shared with the customer before invoices are raised.

Continuous improvement activities focus on service operation, recommendations, and prioritisation. Delivery of improvement work (beyond minor changes required to resolve incidents) is provided via Bolt-On Hours or a separately scoped engagement.

Service Constraints

Panacea's managed support service is delivered in line with the chosen SLA tier, which defines the hours of cover and the TTA/TTE engagement targets for incidents. Service availability is aligned to these tiers, ranging from 8×5 business hours through to full 24×7 cover.

Incident vs planned work: The core service is focused on incident response, triage, fault isolation, and restoration of service. It includes reasonable troubleshooting and targeted configuration changes required to resolve incidents. It does not include project work such as estate-wide upgrades, lifecycle refresh, migrations, redesigns, or large-scale remediation, which are delivered via Bolt-On Hours or a separately scoped professional services engagement.

Out of scope

The following activities are not included within the core support fee, unless explicitly included in the Call-Off and delivered via Bolt-On Hours or a separately scoped project:

- Estate-wide or multi-device change programmes (for example firmware rollouts, major version upgrades, and coordinated configuration deployments across large parts of the estate)
- Lifecycle refresh, hardware procurement, sparing, and physical replacement of devices
- Network redesigns or major remediation (for example readdressing, re-segmentation, major topology changes, or fabric rebuilds)
- Migrations, platform transitions, or introduction of new technology domains not already in use (for example new SD-WAN, NAC, or new fabric designs)
- New site turn-ups or significant expansions beyond the Supported Estate baseline
- Creation or maintenance of detailed estate-wide documentation sets (for example rack-level inventories, cabling schedules, or CMDB population)
- Bespoke reporting development or deployment of additional monitoring and analytics platforms
- Exit migration work (moving to a new provider/platform), beyond standard handover described in the Termination Process

Follow-up or preventative work that can reasonably be scheduled, such as permanent remediation, firmware upgrades across an estate, design changes or optimisation, is treated as planned activity and is scheduled separately so it can be delivered at an agreed time with the right approvals. The existence of a vendor advisory or firmware update does not, by itself, create an obligation for Panacea to perform estate-wide upgrades under the core support fee or on an out-of-hours basis.

The service assumes that, where reasonably practicable, customer networks are designed with appropriate redundancy so that, once service has been maintained or restored, necessary upgrades can normally be carried out during standard business hours without material user impact. Where a customer requires planned remediation or estate-wide changes to be performed outside their contracted hours (for example evenings, weekends or UK public holidays), this work is delivered using pre-purchased Bolt-On Hours, rather than being included in the core support fee. This keeps the standard service focused on day-to-day incident cover while still allowing flexibility for additional work when needed.

Some constraints are determined by Extreme Networks' platforms and roadmaps. Extreme controls product lifecycles, firmware availability and the deprecation or removal of features. Panacea monitors these changes and, where practicable, will advise customers in advance of material impacts and recommended mitigation options. Panacea cannot prevent or delay vendor decisions on feature deprecation or end of support.

Planned maintenance

Planned maintenance, including security patching, firmware upgrades and system updates, is scheduled in advance by mutual agreement to minimise impact. It is normally carried out during standard business hours or within agreed maintenance windows. For larger, estate-wide activities, Panacea will typically provide planning, guidance and remote support. Where out-of-hours work is required at scale, the customer's IT staff will usually execute the changes, with Panacea supporting remotely.

If customers require Panacea engineers to deliver significant out-of-hours maintenance (for example rolling upgrades across many devices in evenings, weekends or UK public holidays), this is scoped and delivered using Bolt-On Hours, and is not included in the core support fee.

In genuinely exceptional cases where immediate action outside standard windows is necessary to address a critical vulnerability or stability issue, Panacea will agree an appropriate approach with the customer and, where reasonably practicable, confirm any additional charges in advance.

Where firmware or patching implementation requires an estate-wide rollout, a major-version uplift, or a coordinated multi-device change, it will be delivered only where agreed and funded as Bolt-On Hours or as a separately scoped project.

Service customisation and non-standard requirements

Customisation of the service is limited to the support scope, devices and features specified in the Call-Off Contract. Non-standard configurations, additional features, or wider consultancy requirements are handled via associated services such as Bolt-On Hours.

Where on-site attendance is required beyond any standard allocation in the support tier, this is available as a chargeable option using Bolt-On Hours and is subject to the travel and working-time rules set out in the Care Pricing Schedule.

Inherited environments and remediation

Inherited environments may contain legacy design decisions, technical debt and historic changes that increase incident volumes and the effort required to resolve issues. The managed support service covers reasonable day-to-day operation of such estates, but significant remediation of underlying design or configuration problems is delivered through Bolt-On Hours and is not included within standard support fees.

Where an inherited environment is found to be unstable or materially more complex than anticipated, Panacea may recommend (and require) a separate remediation engagement to bring the network to a supportable baseline. Use of Bolt-On Hours, including any out-of-hours uplifts, follows the rules set out in the Care Pricing Schedule.

Service Levels

Each coverage tier is available as a Standard or Enhanced plan. Standard plans provide reactive, SLA-backed support aligned to the agreed TTA/TTE targets. Enhanced plans add proactive monitoring, optional GSM out-of-band access on critical devices, and tighter engagement targets, as detailed in the Care Pricing and Order Form.

Panacea's managed support service is delivered under defined SLAs that specify scope of cover, support hours, and Time to Acknowledge (TTA) and Time to Engage (TTE) targets by incident priority and coverage tier. Priority 1 incidents in higher tiers receive rapid acknowledgement and engineer engagement within tight timeframes, with lower-priority incidents aligned to business hours and operational need.

Performance and availability are measured against these service levels. Customers benefit from transparent reporting via our service desk platform, which tracks ticket response and

resolution times, and from regular service reviews where performance against SLA is assessed.

These service levels apply to the managed Extreme Networks environment and support activities under Panacea's control. End-to-end application performance and overall service availability also depend on factors such as third-party providers, customer-side systems, and local infrastructure that may sit outside the scope of this service.

Service levels are agreed with each customer at the Call-Off stage and documented in the Order Form. Where additional requirements exist, Panacea can adjust service levels by agreement, ensuring that support arrangements reflect the operational priorities of the organisation.

Outage and Maintenance Management

Panacea minimises the risk of outages through proactive planning and continuous monitoring. Service performance is reviewed against defined SLA targets, and all incidents are tracked through our service desk to provide full visibility of downtime, response, and resolution.

Outage Avoidance

- Use of vendor cloud platforms (for example ExtremeCloud IQ) designed for high availability, subject to the vendor's published SLAs and current service status.
- Proactive monitoring of customer environments, using telemetry and alerts from Extreme's cloud management platforms and any agreed monitoring tooling, to detect issues early.
- Regular review of vendor security advisories and firmware guidance, with recommendations to mitigate known vulnerabilities.
- Configuration review and baselining during onboarding to identify significant single points of failure and agree remediation options.

Maintenance

- Routine maintenance (for example patching and updates), where Panacea is engaged to deliver it, is scheduled within agreed change windows to minimise disruption and is subject to the Buyer's approval and the service constraints.
- Emergency maintenance may be recommended in response to critical vulnerabilities. Where action is agreed, the Buyer is notified as early as reasonably practicable and changes follow appropriate change control.
- Where Panacea is delivering updates under an agreed change plan, Panacea engineers apply vendor best practice and formal change controls to deliver updates safely and consistently.

Measuring and Reporting

- All downtime, whether planned or unplanned, is recorded within our service desk system.
- Service performance is measured against SLA targets and reviewed with customers as part of ongoing service management.

Ad hoc needs

- Where customers require urgent changes or support outside of the standard scope, Panacea can deliver this flexibly through Bolt-On Hours.
- This ensures organisations can respond quickly to unforeseen requirements without compromising ongoing stability.

Service Credit Model for Not Meeting Service Levels

Panacea links financial accountability to service performance through a structured service credit model. Where Panacea fails to meet the agreed Priority 1 Time to Engage (TTE) targets within the contracted coverage hours, and where no clock-stop or customer-side dependency applies, service credits may be applied as a percentage of the monthly base charge for the affected service.

The exact thresholds, percentages, and caps are set out in the Care Pricing document and the Call-Off Agreement, including bands based on the number of qualifying Priority 1 incidents and a maximum credit cap per month. Credits are only available where Panacea has direct accountability for the delay, are applied to future invoices rather than paid in cash, and represent the Customer's sole financial remedy for failure to meet the applicable Priority 1 TTE target.

4 Provision of the service

Customer Responsibilities

To enable Panacea to deliver managed support services effectively under Lot 2a, the following responsibilities apply to the customer:

- **Access and Information** – provide Panacea with appropriate access to supported systems, infrastructure, and documentation as reasonably required to perform support. Information supplied must be accurate and kept up to date.
- **Incident Reporting** – raise incidents via the agreed service channels (email, portal, or phone) in a timely manner, with sufficient detail to allow investigation. Nominate key staff for escalation and service review.

- **Change Notification** – inform Panacea in advance of any planned changes that could affect supported services, and follow the agreed change process. Customers may choose to carry out their own configuration changes or onboard new devices directly; however, any design, build, implementation, or troubleshooting effort associated with those customer-led changes is outside the core managed support scope and will be billed using Bolt-On Hours. Where Panacea identifies that an incident has been caused or materially contributed to by an unauthorised or uncommunicated change (for example ad-hoc CLI or GUI changes), the time spent investigating and remediating that issue will be chargeable at the prevailing Bolt-On rates and will be excluded from SLA performance and service credit calculations.
- **Third-Party Coordination** – where incidents involve other suppliers or services (e.g. applications, ISPs), the customer must facilitate coordination to allow Panacea to investigate and resolve efficiently.
- **Vendor subscriptions and support entitlement** – the Buyer must maintain, for all in-scope devices, the required Extreme platform subscriptions used to manage and monitor the estate and an active Extreme Networks manufacturer support entitlement (GTAC) for the in-scope hardware and software. These are third-party costs set by the vendor and are not included in Panacea's published G-Cloud prices. The Buyer may hold these directly or, where requested, Panacea can assist with procurement or renewals as a chargeable activity using the published Bolt-On rates, with third-party costs billed separately at the vendor/distributor quoted price in force at the time of order.
- **Security Practices** – maintain internal controls aligned to Panacea's policies and ISO 27001 principles, including secure handling of credentials, user awareness, and compliance with GDPR and UK data protection requirements.
- **Facilities** – where on-site attendance is required, provide safe and suitable access to premises, connectivity, and working conditions for Panacea engineers.
- **Commercial Obligations** – comply with contractual obligations in Panacea's Terms & Conditions, including timely payment of invoices and cooperation in good faith.

Technical Requirements and Client-Side Requirements

To ensure effective delivery of Panacea's managed support service, the following client-side and technical requirements must be in place:

- **Connectivity** – reliable internet access is required for cloud-hosted services, remote monitoring, and support.

- **Infrastructure Access** – customers must provide Panacea with secure remote access (e.g. VPN, management portal, or jump host) and, where required, safe on-site access to supported systems.
- **Vendor platform subscriptions and entitlements** – the Buyer must hold the appropriate Extreme management platform subscriptions and device support entitlements required for the agreed features (for example cloud management, monitoring and access to GTAC).
- **Hardware and Software** – supported devices must be maintained under current Extreme Networks support, with valid GTAC entitlement, and run recommended firmware and patch levels. Where customers prefer, Panacea can supply or arrange the vendor-backed support on their behalf, with Panacea acting as the single point of contact and co-delivery partner for GTAC case management.
- **Data and Documentation** – customers should provide up-to-date network documentation, asset registers, and configuration baselines to support effective service delivery.
- **People and Time** – nominated contacts should be available to support onboarding, service reviews, and incident escalation. Customer staff should allocate time for joint activities such as knowledge transfer or change planning where applicable.
- **Facilities** – suitable workspace, connectivity, and health and safety measures must be provided for Panacea engineers during any on-site attendance.

Specific technical and client-side requirements are confirmed with the customer during the Call-Off process and documented in the Order Form.

Outcomes/Deliverables

By engaging Panacea's managed service, clients receive:

- **Defined service levels** – SLA-backed support hours and TTA/TTE incident targets aligned to operational needs.
- **Proactive stability measures** - such as monitoring, patching advice, and configuration backups, that reduce downtime risk.
- **Documentation and reporting** – service records, the baseline documentation required to deliver the Care service, and visibility of performance against SLA targets.
- **Direct access to expertise** – vendor-certified engineers who know the client's environment and provide accountable, immediate support.

- **Resilient operations** – assurance that critical networks remain available, secure, and compliant.
- **Transparent commercial model** - with predictable pricing based on the expected monthly support hours for each coverage tier, and quarterly (or ad-hoc) usage reviews to confirm the service still matches demand and to agree Bolt-On Hours or tier changes if usage consistently exceeds the baseline.

Development life cycle of the solution

This service does not involve software development. The "solution" offered under this G-Cloud listing is the configuration and operation of off-the-shelf Extreme Networks cloud platforms and associated tooling, delivered as a managed support service.

Panacea therefore does not apply a standalone software development methodology (such as a full Agile or waterfall SDLC) to this service. Instead, we follow a structured, change and configuration lifecycle for any changes we make to the cloud platforms and customer environments.

After-sales Account Management

Panacea builds long-term customer relationships by keeping account management close to the engineers who deliver the service. Rather than passing clients through layers of account teams, the same people who know the customer's environment remain directly engaged throughout the lifecycle of the contract.

We maintain relationships and satisfaction by:

- **Regular reviews** – scheduled service reviews to discuss performance against SLA, ticket trends, and future requirements.
- **Open communication** – direct access to Panacea engineers via phone, Teams, and email, with clear escalation paths.
- **Continuity of contacts** – customers deal with a consistent team who already understand their environment.
- **Feedback and improvement** – capturing lessons from incidents and service usage to refine delivery and prevent recurrence.
- **Strategic partnership** – identifying opportunities to improve resilience, efficiency, or value for the customer within the existing service framework.

This approach helps Panacea retain long-term relationships in healthcare, government, and defence, where continuity and trust are critical.

Termination Process

Termination of Panacea Care services is managed in accordance with the Buyer's Call-Off Agreement, including the Buyer's right to terminate for convenience.

- **Notice period and Minimum Period** – The service is contracted for a Minimum Period and any Renewal Term(s) as set out in the Call-Off. Buyers must provide written notice of termination in line with the minimum notice period defined in the Call-Off.
- **Charges on termination** – On termination other than for Panacea's material breach, the Buyer remains liable for all charges up to the effective termination date, including any agreed minimum monthly service charge and notice-period charges. Panacea may also recover non-recurring setup charges and committed third-party costs as described in the Care Pricing Schedule
- **Exit planning** – Upon notice, Panacea will work with the Buyer to agree an exit plan, including timeframes, responsibilities, and the scope of any transition support. Standard handover of existing documentation and configuration backups is included. Extended exit activities (for example detailed transition run-books or parallel running) are available as chargeable services, using the rates set out in the Care Pricing document and Bolt-On rates schedule.
- **Exit assistance** - Standard exit support includes handover of the documentation and configuration backups held by Panacea as part of the service, plus reasonable cooperation to support an orderly transition. Exit migration activity, redesign, rebuild, or transfer to a new platform/provider is out of scope and is delivered as a separately scoped, chargeable engagement using Bolt-On rates.
- **Buyer responsibilities** – The Buyer must settle all outstanding charges up to the date of termination, provide reasonable cooperation to facilitate an orderly exit, and ensure appropriate access for any new provider.

5 Our experience

Case Studies

The following examples illustrate how Panacea's Extreme Networks support service has been used to stabilise and improve critical environments. They are included to help buyers understand how the service operates in practice rather than as separate bespoke offerings.

Case study 1 – NHS Trust

Problem: An NHS trust was experiencing persistent instability with a new clinical application. User sessions were terminating frequently, causing frustration for clinical staff and undermining confidence in the system. The issue had been investigated over several months by the incumbent partner without a clear resolution.

Action: Panacea was engaged to investigate using our Extreme Networks expertise and experience. Our engineers identified behaviour consistent with multicast-related issues and applied an appropriate edge policy to contain mDNS traffic. This immediately stabilised the environment. Further analysis confirmed that a condition on the network devices was causing multicast traffic to be reflected into the network and resulting in MAC flaps.

Outcome: This reduced pressure on IT teams, restored confidence for users, and demonstrated the value of having a specialist Extreme-focused support service in place.

Case study 2 – Campus Network

Problem: In another engagement, a customer reported severe performance issues that appeared to be caused by a Layer 2 loop within the LAN. Initial diagnostics suggested intermittent instability without a clear, fixed root cause.

Action: Using Extreme's management and monitoring tools, Panacea's engineers examined port and interface counters at the access layer and identified that wireless mesh functionality had been enabled on access points connected to the same VLAN. This created an unintended bridged loop using the wireless backhaul.

Outcome: By adjusting the wireless configuration and removing the unintended bridging path, we eliminated the loop condition and restored stable performance. The customer avoided a full network outage and gained a clearer configuration pattern to prevent similar issues in future, supported by ongoing monitoring through the cloud management platform.

Case Study 3 – National Security Environment

Problem: Persistent poor network performance was reported without any obvious indicators in logs or packet captures. The symptoms closely resembled a Layer 2 fault, but traditional loop detection and standard diagnostics produced no clear results, making the issue difficult to isolate and increasing operational risk.

Action: Panacea was engaged to perform a structured investigation. Using a disciplined divide-and-conquer approach, our engineers systematically isolated sections of the

network, correlating performance characteristics with changes in topology and utilisation. This methodical process ultimately traced the fault to a 40G-to-4×10G splitter cable issue that was introducing unexpected behaviour under load. Once the cable was replaced, network performance stabilised immediately.

Outcome: The complex issue was resolved without the need for a prolonged outage, safeguarding continuity of critical operations and restoring confidence in the stability and resilience of the infrastructure.

Clients

Panacea has a proven track record of delivering managed support and networking services across the UK public sector, particularly in healthcare and government. Our referenceable clients include:

Surrey and Sussex Healthcare NHS Trust

NHS Surrey and Sussex Healthcare NHS Trust

Royal Surrey NHS Foundation Trust

NHS Royal Surrey NHS Foundation Trust

Royal National Orthopaedic Hospital NHS Trust

NHS Royal National Orthopaedic Hospital NHS Trust

UK Health Security Agency (UKHSA)

UK Health Security Agency

CONTACT DETAILS

For G-Cloud enquiries, please contact

Martin Flammia, Director
Panacea Networking Limited

67–169 Great Portland Street,
5th Floor London, W1W 5PF

gcloud@panacea-networking.co.uk

0207 101 3111