G-Cloud 15

Service Definition

Zscaler Zero Trust Exchange

NG-IT

Lot 2a Infrastructure Software as a Service (iSaaS)

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 Zscaler Zero Trust from Principle Networks as a key solution to deliver uninterrupted security and connectivity. Zscaler Zero Trust empowers organisations with code-to-cloud visibility and risk-based threat prioritization, letting users operate and expand more confidentially along their cloud journey.

The Solution

NG-IT have chosen to propose Zscaler Zero Trust from Principle Networks to address the challenges of delivering and maintaining adequate and effective security for users, workloads and devices.

Zscaler Zero Trust Exchange

Zscaler has built the Zero Trust Exchange for maximum resilience and robust SLAs, drawing on over 15 years of experience delivering the industry's largest security cloud. This deep expertise also underpins the Business Continuity Cloud (BCC). The BCC is an isolated, separate instance from the Zero Trust Exchange, ensuring seamless operations and business continuity via dedicated, isolated infrastructure — all part of a unified Zscaler solution.

The Zscaler platform allows organisations to minimise business risk through protection against cyberthreats and data loss, simplification of security controls brings about lower costs and reduced complexity by eliminating traditional point solutions and reducing overhead on IT staff. Increased business agility is delivered via zero trust networking for users, workloads and branches.

Service key benefits

Zero Trust Architecture

- **Minimize the attack surface**. Hide applications behind Zero Trust Exchange making them invisible to the internet.
- **Prevent compromise**. Inspect all network traffic and block threats in real-time.
- **Eliminate lateral movement**. Connect authorised user entities directly to apps not to the network.
- **Stop data loss**. Automatically identify and protect sensitive data in motion, at rest and in use.

- **High redundancy minimizes risk of downtime**: Business Continuity Cloud ensures uninterrupted operations for customers by providing an infrastructure with a private control plane and a private data plane that are in a read-only mode, completely isolated from the Zscaler primary cloud. This critical separation prevents major failures from affecting the datacenters providing Business Continuity Cloud service, allowing customer employees to maintain productivity and ensure critical processes run smoothly, thereby minimizing downtime and any potential loss of revenue.

- **Deliver consistent user experience**: With Zscaler Business Continuity Cloud, users avoid the re-login, downtime, and session interruptions common in multi-vendor environments. This seamless continuity minimizes the impact of critical failures on user productivity and experience.

- **Maintain security with zero trust**: The Zscaler Business Continuity Cloud offers a streamlined approach compared to multi-vendor solutions. It maintains your existing security policies and application connectivity, ensuring continuous protection during outages and disruptions. This is achieved without the need for separate security policies, multiple logins, or additional endpoint agents, unlike the complexities often associated with a multi-vendor strategy.

- **Cost Savings and Simplicity**: Eliminate complex, multi-vendor backup systems to reduce costs and streamline operations. This will improve end user experience, ensure consistent security policies, and remove the need for manual failovers.

- **Compliance Assurance**: Ensure continued adherence to regulatory requirements and SLA obligations like DORA, Australia CPS 230, and ISO 22301 even in the event of critical failures.

Resilient by Design

The Zscaler Zero Trust Exchange platform delivers uninterrupted security and connectivity—even when individual devices fail, networks slow, or entire regions go dark. Its globally distributed footprint, automated cloud operations, and built-in failure protections work together to maintain secure, low-latency access under any of these failure scenarios.

This approach to resiliency rests on three core pillars:

Resilient Global Cloud Infrastructure: Zscaler's cloud spans multiple autonomous system numbers (ASNs), automatically rerouting traffic around any regional or carrier outage. A true multitenant architecture shares capacity across its global footprint for instant scale, while extensive high-speed peering keeps users on the fastest, most available path and consistent security anywhere in the world.

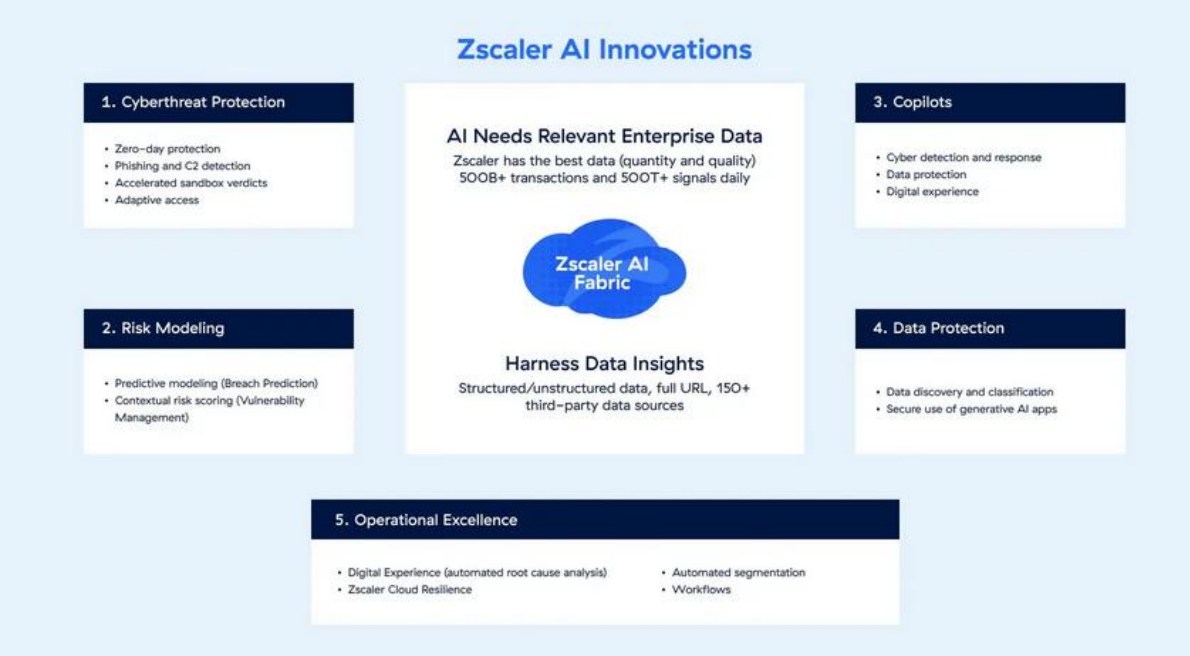
Resilient Cloud Operations: Staggered upgrades with zero downtime, AIOps-driven observability and robust incident handling enable nonstop feature delivery and security enhancements essential for 24x7 operations.

Built-In Failure Protection: Real-time policy and session replication absorbs any node failure. Redundant paths with adaptive routing shift traffic in milliseconds, while dynamic service edge

selection keeps every connection on the healthiest node to maintain availability and performance.

The Zero Trust Exchange delivers exceptional resilience, guaranteeing 99.999% uptime through its SLA. This commitment ensures uninterrupted security and connectivity, even when faced with individual device failures, network slowdowns, or regional outages. This is achieved through a combination of its distributed global infrastructure, automated cloud operations, and integrated failure protections, which collectively provide secure, low-latency access in common failure scenarios.

Leadership and competitive advantage in AI



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

Delivered by Principle Networks, the Zscaler proof of value (POV) is a time limited engagement designed to showcase the solution within a customers own environment. The POV is generally a time limited engagement working to a pre-defined and agreed scope that allows customer to experience and utilise the solution with a set of specific objectives, the POV can be fully featured to ensure a complete experience and is supported throughout by appropriately skilled technical resource to assist with the evaluation.

Please contact gcloud@ng-it.co.uk for more details about the proof of value.

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

Once the 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.

Getting Started

As a starting point, you will receive a Welcome Email from the Service Provider. This servers as a formal starting point and you will be introduced to the team that will work with you during any implementation and onboarding. You will receive assistance from Principle Networks to start using Zscaler through a mix of structured documentation, guided onboarding, and live support.

During this phase, 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 and describe the resources available that will be available during onboarding and the early phases of service adoption,

The Zscaler onboarding process ensures a smooth transition from the initial sale through to long-term service and support. Once a project is confirmed, we engage in structured onboarding that includes a full requirements review, stakeholder alignment, and handover from the sales team to project management. A dedicated project manager oversees delivery, coordinating timelines, dependencies, and customer expectations. Training is tailored to customer needs: we offer onsite training, online/remote sessions, and comprehensive user documentation to ensure all users can adopt the solution confidently. As part of onboarding, we provide access to knowledge bases, operational guides, and support contacts so customers know exactly how to get assistance. When a project moves into operations, we complete a formal service handover, including technical documentation, asset registers, support SLAs, and escalation paths. Support teams are fully briefed to ensure continuity.

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.

Off-boarding

Offboarding follows the same structured approach. If a service ends, we manage asset recovery, user deactivation, data management, and service closure tasks professionally and securely. Final documentation and confirmation ensure all contractual and operational obligations are completed.
The contract expires user accounts are disabled and removed. Customer Monitoring is removed as required.

Service Management

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

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

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

Service Constraints

Maintenance: Weekly updates occur during off-peak hours; typically transparent. Customisation: Multi-tenant SaaS; customisation limited to configuration, not code. Connectivity: Requires active internet and outbound port 443 access. Device Support: Legacy OS versions may not support current Client Connector. Bandwidth: Usage is subject to fair use policies. Data Residency: Traffic processing is global; log storage is region-specific. Deprecation: Features retired with advance notice

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

The service provider delivers 24×7×365 email and ticketing support, with response times governed by strict SLAs. For critical (P1) and high-impact (P2) issues, response is within 30 minutes. Medium-impact (P3) tickets receive a response within 2 hours, and standard requests (P4) within 4 hours. All tickets raised via email, phone, or the customer portal enter our ITSM system immediately, where they are prioritised and actioned by the service desk. Our monitoring systems also auto-generate tickets to ensure rapid response without user intervention.

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

Zscaler maintains transparency regarding service availability primarily through the Zscaler Trust Portal (trust.zscaler.com). This public dashboard provides granular, real-time visibility into the health of the entire global infrastructure. Here is how outage reporting is handled: Public Dashboard: The Trust Portal displays the live status of all clouds (ZIA, ZPA, ZDX) and individual data centres. You can filter views by region to see specific service degradation or maintenance events. Email Alerts: You can subscribe to the Trust Portal to receive proactive email notifications for incidents, scheduled maintenance, and security advisories relevant to your specific cloud instance. API & Feeds: The Trust Portal provides JSON and RSS feeds for incidents. These allow you to programmatically ingest status updates into your internal monitoring tools (like ServiceNow or Splunk) rather than manually checking the website. Additionally, for internal troubleshooting, Zscaler Digital Experience (ZDX) can alert your IT team if users face connectivity issues, helping distinguish between a local network fault and a Zscaler service anomaly.

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.

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 Principle Networks 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 guarantee high availability across our managed services through 24×7×365 monitoring, proactive alerting, and resilient architecture. Our services operate under IS 20000-1-aligned service management, with strict SLAs governing response and resolution. For incident availability, we commit to a 30-minute response for P1 and P2 incidents, with target fix times of 2–5 hours for critical issues, depending on whether the solution is resilient, hardware-based, or dependent on third-party circuits. Lower-priority issues follow defined SLA timelines to maintain consistent service quality. Where contractual availability SLAs are in place, we provide service credits if availability falls below the agreed threshold. Credits are calculated using a transparent formula based on the number of hours outside SLA multiplied by the proportional hourly service cost. This ensures customers receive fair compensation for any material downtime. Our approach combines continuous monitoring, resilient design, rapid engineering response, and clear escalation paths to maintain service uptime and minimise disruption.

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

4. Provision of the service

Customer Responsibilities

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

- Providing the most accurate information during all phases of the Service Delivery
- Promptly notifying us of any significant business and technical changes that may affect the Service performance
- Providing timey responses to the Service Provider queries, incident responses and approval requests
- Adhering to agreed change-management, approvals, lead times and risk assessments

- Submitting requests using approved channels
- Participating in Services Reviews if applicable
- Honouring contractual payment terms

The customer is responsible and liable for all uses of the Services and Documentation resulting from any access whatsoever provided to Principle Networks by Customer, directly or indirectly. Without limiting the generality of the foregoing, Customer is responsible for all acts and omissions of Authorized Users, and any act or omission by an Authorized User that would constitute a breach of the Service Agreement if taken by Customer will be deemed a breach of the service Agreement by Customer. Customer shall make all Authorized Users aware of this Agreement's provisions that are applicable to such Authorized User's use of the Services and shall cause Authorized Users to comply with such provisions. Customer shall use reasonable efforts to secure its passwords and credentials and will promptly notify Principle Networks of unauthorized account use of which it becomes aware.

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 within the deployment of Zscaler Zero Trust Exchange. 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.

After-sales Account Management

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

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

Termination Process

The term of this agreement begins on the Effective Date and, unless terminated earlier pursuant to the service agreement's express provisions, will continue in effect for the period set forth on the

applicable order form. Principle Networks may terminate the agreement, effective on written notice to Customer. Upon expiration or earlier termination of the agreement, Customer shall immediately discontinue use of the Zscaler Inc. IP and, without limiting Customer's obligations set under the Service Agreement, Customer shall delete, destroy, or return all copies of Zscaler Inc. IP and certify in writing that the Service Provider IP has been deleted or destroyed. No expiration or termination will affect Customer's obligation to pay all Fees that may have become due before such expiration or termination. Notwithstanding any termination of the Agreement, those provisions which by their nature are intended to survive termination, including but not limited to provisions regarding intellectual property rights, confidentiality, indemnification, limitation of liability, disclaimers of warranties, dispute resolution, and governing law, shall continue to remain in full force and effect after such termination.

Termination for Unpaid Overages. If Principle Networks determines, through its monitoring or audit rights under the service agreement, that Customer has exceeded the scope of the licensed use (including without limitation, the quantity of purchased licenses), Service Provider will notify Customer in writing of such excess use and the corresponding fees due at then-current list prices. If Customer fails to remit full payment of such fees within fourteen (14) days of receiving such notice, Service Provider may, in its sole discretion, (a) immediately suspend Customer’s and its Authorized Users’ access to the Services, and/or (b) terminate the service agreement upon written notice. Customer acknowledges that any such use beyond the licensed scope constitutes a material breach of this Agreement.

Detailed Service Terms and Conditions, including the Termination, will be addressed in the Service Agreement.

5. Our experience

Case Study

Zero Trust Network and Security Infrastructure Upgrade for a Major UK Law Firm

Overview

A major UK law firm providing trusted advisory services to organisations and individuals across multiple sectors worldwide required network and security infrastructure upgrades. Operating across multiple UK offices with an international presence, the firm identified opportunities to expand its footprint and recognised the need to strengthen its network security and infrastructure through strategic investment to enhance resilience and agility, simplify complexities, and lay foundations for future growth.

Challenges

- **Limited agility under fully managed services**: The firm found itself constrained and less able to react quickly enough to critical changes such as opening or relocating sites or implementing network adjustments to support new client requirements, creating barriers to meeting growth targets.
- **Mobility and secure connectivity requirements**: With a large, globally distributed workforce frequently travelling to remote and sometimes less digitally secure locations around the world, the firm needed seamless, secure and reliable connectivity with assurance that endpoints were connecting safely and securely to the network without compromising performance or data integrity.
- **Resilience demands**: High-profile client events and conferences could see up to 100 additional users on the network on top of regular staff, placing significant demand on infrastructure. Network disruption during these events could directly impact the firm's reputation and client relationships.
- **Legacy infrastructure and security constraints**: Existing systems created complexity that increased operational burdens and reduced the firm's ability to scale and adapt rapidly, holding back innovation and business evolution. The firm required a strengthened security posture to protect sensitive client data and maintain regulatory compliance.
- **Growth and expansion support**: The firm needed a technology environment that would remove barriers rather than create them, allowing teams to scale rapidly and support the opening of new sites and integration of acquisitions without being slowed down by internal technical limitations.

Solution

The firm partnered with a specialist cybersecurity and network infrastructure provider, experts in designing and implementing scalable, secure and future-proofed cloud-based networks for mid-large enterprises, to undertake a comprehensive digital transformation project:

- **Zero trust security framework**: Legacy systems were replaced by an internet-based Software-Defined Wide Area Network (SD-WAN) integrated with a Secure Service Edge (SSE) zero trust security framework, ensuring that all connections were verified and secured regardless of location.

- **Cloud-based, scalable architecture**: The solution harnessed cloud technology, leveraging the internet for scalability and resilience, delivering an efficient, cost-effective and scalable network capable of onboarding new acquisitions seamlessly.
- **Co-managed service model**: The provider delivered a co-managed service offering 24-hour support services across the new SD-WAN and SSE infrastructure and the firm's Local Area Network (LAN) and Wi-Fi estate, providing flexibility and responsiveness to support rapid growth while allowing the firm's internal IT team to retain control where needed.
- **Unified security architecture**: The solution consolidated systems and adopted consistent security frameworks with fewer moving parts, minimising vulnerabilities and significantly improving the ability to monitor, detect and respond to threats across all business units, including new acquisitions.
- **Future-ready foundation**: The infrastructure was designed with growth in mind, enabling secure adoption of emerging technologies such as generative AI to fuel further growth and innovation.

Conclusion

- **Improved agility and flexibility**: Transitioning to a co-managed approach provided the flexibility and responsiveness required to support rapid growth and continuous evolution, with the IT team able to focus on innovation and business enablement rather than managing fragmented infrastructure.
- **Enhanced user experience with security**: Performance improvements were immediately noticeable, with users enjoying reliable, secure access with minimal friction whether in the office or working remotely, without compromising on security controls.
- **Strengthened cyber security posture**: A unified and streamlined security architecture with integrated zero trust controls significantly improved the firm's ability to monitor, detect and respond to threats across all business units, including new acquisitions, while minimising the attack surface.
- **Faster expansion capability**: Improvements in meeting regulatory and compliance requirements, combined with the ability to scale infrastructure quickly and consistently, enabled the firm to identify, negotiate and open new sites or integrate acquisitions faster.
- **Strategic partnership value**: The proactive and consultative approach from the cybersecurity and network provider helped the firm make better decisions, driving operational efficiencies and significantly improving security posture, with the provider acting as a true partner rather than just a vendor.
- **Foundation for innovation**: The streamlined infrastructure laid solid foundations allowing the firm to grow, innovate and stay ahead of the curve in an increasingly competitive legal market, removing friction and building resilience into every layer of infrastructure.

Clients

Contact Details

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