Security and resilience

Our architecture has been meticulously designed to ensure continuous contact centre operations for all our customers.

The fundamentals of our high-availability network is built on the following principles:

Security and Cyber Essentials

We have strong security controls to protect sensitive data, including encryption, multi-factor authentication, and compliance with relevant standards like GDPR and Cyber Essentials+ accreditation. Our network is eternally audited including full PEN testing.

Additionally, as an OFCOM regulated carrier providing services as part of the UK Critical National Infrastructure, we are required to comply with all OFCOM general conditions including Security and Resilience.

We hold the following third-party security accreditations:

- Cyber Essentials Plus with the National Cyber Security Centre
- ISO27001
- PCI-DSS Level 1

Features and Benefits

Reliability, resilience and data protection are our foundations.

Our UK-based platform is comprised of a multi-site network infrastructure which consists of three regional Tier 1 data centres and Microsoft Azure cloud. Real-time data replication takes place across all sites for resiliency and to prevent downtime.

Cxp provides a 99.999% and 99.9% uptime guarantee, for voice channels and digital channels respectively.

Security is reinforced with multi-layered encryption, and is assessed and certified as ISO 27001, Cyber Essentials Plus, and PCI-DSS Level 1 compliant.

The network overflows is built to manage traffic peaks due to days of the week and seasonal changes come as standard.

Regular auditing and penetration testing takes place to further ensure secure, continuous operations have built-in disaster recovery for business continuity capabilities.

Redundancy

Multiple instances of critical components are deployed across different geographical regions to avoid single points of failure.

Our voice platform spans across three Tier 1 Data Centres (DC) based within the UK (Birmingham, Manchester and London). All data remains within the UK.

Each site runs from a set of building blocks that plug together to create the overall services. All services are shared across all sites simultaneously and all data and user states are replicated between the sites in 0.1 seconds or less. The idea of redundancy and resilience continues as a theme through to how we use those building blocks and to create redundant solutions on many layers.

Each data centre houses multiple Session Border Controllers and multiple Call Control Telephony Servers. Each site also hosts a database, a bank of web servers and file servers and uses a dual LAN with Dual WAN Router configuration. TelXL have assured that there is replication across all sites via multiple backhaul service providers and makes sure that there are no single points of failure anywhere within our network.

We have provisioned multiple Carrier Interconnects at each site which provide voice connectivity for both inbound and outbound calls - these are currently, BT, Gamma, Vodafone and 6Degrees. Each Carrier provides the ability to load balance across the three sites for inbound calls and offers automatic multiple overflow call routing for extra resiliency. TelXL automatically overflow outbound calls between sites to these Carriers should faults occur and, if a Carrier should fail entirely, prebuilt routing options are set to overflow the calls to alternative Carriers.

Infrastructure maintenance

We seamlessly migrate customers around our network when we need to perform monthly maintenance tasks without risk to our customers.

If an unfortunate system outage does occur, the user can be reconnected on another server at the same or at another site with users refreshing their screen to continue.

TelXL ensures that there are at least three internet service providers per data centre site for diversity and to protect against any catastrophic internet outages, such as BGP major incidents.

w :telxl.com
t:+44 3300 220022
@: enquiries@telxl.com

a: Unit 2&3, Centech Park, Fringe Meadow Rd, Moons Moat North Industrial Estate, Redditch. B98 9NR

High availability

TelXL recognizes the importance of uptime for Emergency Contact Centres and offers all customers an SLA of 99.999% uptime.

We enable Reverse Proxy via NGINX at the edge of our network, used for accessing the internal web servers that provide the Call Control Portal. This provides resilience and load balancing, as there are multiple IPs connected to each Proxy and multiple Proxies at each Switch Site. TelXL use round robin DNS to reference each distinct ISP/Proxy combination. Call data is initially written to a site-based database server, then replicated to a master server and a back-up master in near real-time (seconds). This protects our customers from the impact of any hardware failure, outages, or accidental deletion. The Network is extensively monitored, every Web Blade, Telephony Server, ISP, Interconnect, Disk Capacity, Processing Capacity, WAN, Check Grafana etc.

Disaster recovery (DR) and business continuity management (BCM)

Our service includes in-built automated disaster recovery capability. This mechanism ensures that operations can continue even if a primary data centre fails.

The network overflows are built to manage traffic peaks due to days of the week and seasonal changes come as standard, but our service also provides the means to have many prebuilt versions of the service for various DR scenarios, which can be switched to live by the customer via the portal instantly or even via the use of a pin protected phone call should internet access not be available. Backup copies of services can also be stored providing further resiliency and DR coverage.

w :telxl.com
t:+44 3300 220022
@: enquiries@telxl.com

a: Unit 2&3, Centech Park, Fringe Meadow Rd, Moons Moat North Industrial Estate, Redditch. B98 9NR

Data protection and compliance

Ensuring the security, availability, and integrity of critical data is essential. Our data centres are configured to continuously back up and replicate data including call records and calls recordings. This guarantees that, even in the event of a hardware failure, data remains intact and accessible.

The confidentiality, integrity and availability of data is protected at rest and in transit through several security mechanisms and practices, including:

- Encryption of data both at rest and in transit
- TLS 1.2 for data in transit
- VPN access and MFA controls for all TelXL access to the platform, including secondary MFA for system administrator access

We also adhere to rigorous regulatory standards, including ISO 27001, CE+, and PCI DSS, ensuring that our data management processes meet the highest levels of security. Our operations are fully compliant with GDPR and other relevant regulations, and we conduct regular audits to maintain the highest standards of data protection.

Scalability

Be reassured that the you can scale up during peak times without compromising performance. We ensure significant headroom is always maintained, to allow for peaks and troughs in customer demand, but most importantly to enable all calls to continue in the unlikely event that a Data Centre entirely failed.

Having many servers distributed across our three data centres means we can handle an influx of unexpected traffic, for example caused by a disaster event, such as a power or environmental emergency.

w :telxl.com
t:+44 3300 220022
@: enquiries@telxl.com

a: Unit 2&3, Centech Park, Fringe Meadow Rd, Moons Moat North Industrial Estate, Redditch. B98 9NR