Protected business
Advanced Secure Remote Access

Liquid Telecom offers an Advanced Secure Remote Access Service that ensures your organisation can avoid the risks of unauthorised access to your organisation's systems and sensitive data where employees are working from home.

What are the threats whilst working from home?

Your teams are key in your defense against cyberattacks during this extended period of working from home. Your teams should be alerted to increased social engineering attacks and phishing attempts, especially during this time of both dramatic change and urgency. The COVID-19 pandemic opens your organisation up to a new avenue for malicious actors using phishing emails or "social engineering" to gain access or steal sensitive information your organisation.

What security controls are typically already in place in your organisation?

To protect key systems and sensitive information organisations would typically adopt these security controls:

- Employees' machines have approved anti-virus software, with the latest anti-virus and patching updates.
- Machines have configured built-in personal firewall.
- Information on machines and servers are backed up once a week at least (online and offline).
- Hard drives on users' machines are encrypted for security reasons in the event of machine theft.
- When sharing sensitive organisation information, your teams use only approved repositories, for example, SharePoint, One Drive, Email, or Teams Chat.
- Use of advanced email protection, especially if you are concerned about the risks from sophisticated business email compromises, attempts by threat actors to gain unauthorised access to emails, unwanted disruption from email malware, phishing attacks, email malware, mail virus infection and mail-borne spam.
- Employees would change the default administrator password of their home Wi-Fi router to be a complex password as an attacker can easily discover the default password.

We offer an Advanced Secure Remote Access Service based on Netskope for Web, and Netskope Private Access (NPA) with these Service characteristics:

- The enterprise is given a shared call service number, such as 0860–ABC-xxx
- Strong end-to-end encryption to protect your critical systems and sensitive information from traffic interception.
- Concurrent traffic performance management.
- Service performance and availability management.
- Detect and prevent potential exploits and compromises by attackers.
- Real-time, full file inspection to detect and block malware.
- Zero-day protection using advanced heuristic analysis and dynamic sandbox analysis.
- Up-to-date patching and malware protection.
- Security incident response process in the event of attacks on the Service.
- Threat protection against malicious web sites.
- Quickly implement cloud-delivered data loss prevention policies using dozens of predefined policy templates to identify sensitive data in accordance with common regulations.
- Next-Generation Secure Web Gateway that enables you to govern web usage and provide a safe experience for your users with comprehensive web classification and content filtering.
- By steering web traffic, we ensure you can distill web activity into user sites, page visits, and other web activities in order to analyse usage and protect your enterprise.
- Netskope NG SWG is built to meet the demanding needs of today's organisations, providing a low latency service with full SSL inspection of traffic.
- NPA (which is based on Zero-trust network access) connects your remote users directly to applications hosted in public cloud and private data centers using Netskope's NewEdge - a high-performance, scalable global network infrastructure.
- NPA gives employees access to applications, not the network. This protects private applications and other network assets from malicious insiders or compromised accounts.

Advanced Secure Remote Access

Benefits

- Zero Trust Network Access for private applications
- Provide authorized users with access to their applications – not the whole network – and protect private applications and other network assets from malicious insiders or compromised accounts.
- Connect directly to public cloud applications
- Connect remote workers directly to applications hosted in public cloud and private data centers using Netskope's globally hosted network of PoPs. This provides an architecturally elegant and low-latency end user experience for accessing private applications.
- Phase out legacy VPN remote access
- Retire legacy VPN hardware and enable a move towards a cloud-first security architecture. Phase out the capital investment, refresh cycles, and ongoing management costs of VPN appliances.
- Protect private applications and resources
- Ensure that private applications hosted in public and private cloud are never exposed to the Internet. Avoid brand damage, fines, and remediation costs associated with a breach of a private application hosted in the cloud.
- Seamless and transparent user experience
- Use a unified, lightweight client, to provide users with simultaneous access to all their applications deployed across public cloud and data centers without the hassle of connecting and reconnecting to various VPN gateways.
- Begin your transformation to a SASE
- Use a single administrative console for simplified policy management, analytics and incident investigation for employee use of web, cloud and private applications. Move towards the cloud-based future of network security – Secure Access Service Edge (SASE).

Features

- **Secure Access –** Connectivity between remote users' devices and private applications is secured by an end-to-end TLS encrypted tunnel and optimally routed through the Netskope NewEdge network.
  - A low latency, high-capacity, scalable global network infrastructure.
  - Built on the principles of zero trust, NPA policies ensure that remote users are directly connected only to the applications they are authorized to use and do not have broad network-level access to environments.
- **Application Support –** Support for browser-based access to web applications (e.g. HTTP or HTTPS applications) and for non-web / thick applications (e.g. SSH, RDP, Microsoft Windows Active Directory). Support for both TCP and UDP protocols on almost all associated ports.
- **User Authentication –** Following the principles of Zero Trust, Secure Remote Access ensures that only authenticated and authorized users can gain access to applications. Netskope is able to integrate with Microsoft Active Directory and Single Sign-On (SSO) providers to understand users, groups and organizational units.
- **Device Security Posture –** Ensure that only corporate devices meeting a specific security posture can access private applications. A corporate device can be identified by monitoring the encryption status, registry setting, running process, presence of a file or certificate, or Active Directory Domain membership.
- **Securing remote Workers –** In addition to connecting remote workers to their private applications using ZTNA, Netskope also provides a globally available, cloud-based security platform for securing remote workers' access to websites and cloud applications. Netskope has the unique ability to decode cloud application and website traffic to understand remote workers' activities, inspect data movement, and detect threats hidden in SSL/TLS traffic. Netskope uses the same, lightweight client installed on a device to manage web and cloud traffic, and tunnel private application traffic.
- **Client Deployment –** Secure Remote Access utilizes a lightweight Netskope Client installed on a Microsoft Windows or Apple macOS device. The Client steers Private Access application traffic to the Netskope Security Cloud using either DNS or the IP address.
  - **Note:** The same Netskope Client is used to steer website and cloud application traffic when subscribed to the Next Gen Secure Web Gateway solution (for data loss prevention and threat protection).
- **Inline Policies –** Granular policies for blocking or allowing access to private applications can be built on criteria including User, Group or Organizational Unit (OU); Device Classification; or Operating System.
- **Events and Alerts for Private Applications –** Events enable visibility of private application traffic and relevant details, such as who has accessed what, from where, and for how long.
  - Alerts highlight where private app policy violations occur (i.e. when an attempt to access a private app is explicitly denied by a policy).
  - Both Events and Alerts are retained for analysis within the Netskope platform for 90 days (optionally up to 1 year).