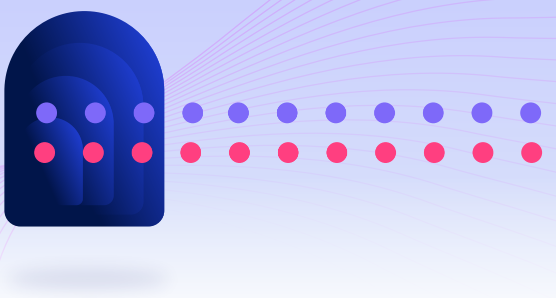
XYTE

Xyte Data Sheet

Secure Tunneling



Secure tunneling enables encrypted connection between remote workstations to support secure access to on-premise interfaces, helping achieve secure transmission of data between local and remote devices. Secure tunneling ensures **confidentiality, integrity, and protection against unauthorized access and data manipulation during transfer**.

With Xyte's secure tunneling feature, end-customers and managed service providers can connect to on-premises devices through the cloud in a secure fashion. A number of Xyte customers use secure tunneling to monitor, configure, troubleshoot, and update their devices remotely, including making configuration and programming changes as if they are on site.

Enabling Safe, Efficient Support for Remote Monitoring and Management

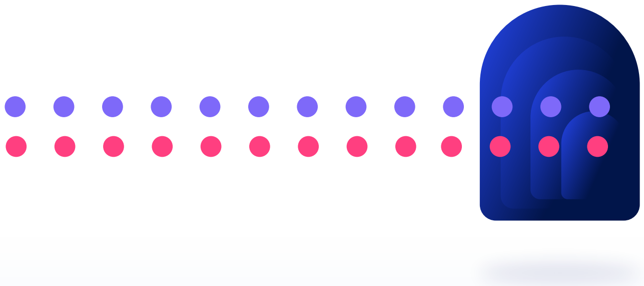
Secure tunneling allows operators to conduct remote support securely and efficiently, without worrying about the safety of their data or systems. Secure tunneling offers:

Protected Communication
Data is encrypted during remote sessions, ensuring that sensitive information remains safe from hackers or eavesdroppers.

Seamless Connectivity
Secure tunneling allows you to access devices and systems even if they are behind firewalls or network address translators (NATs), allowing for smooth remote support without compromising security.

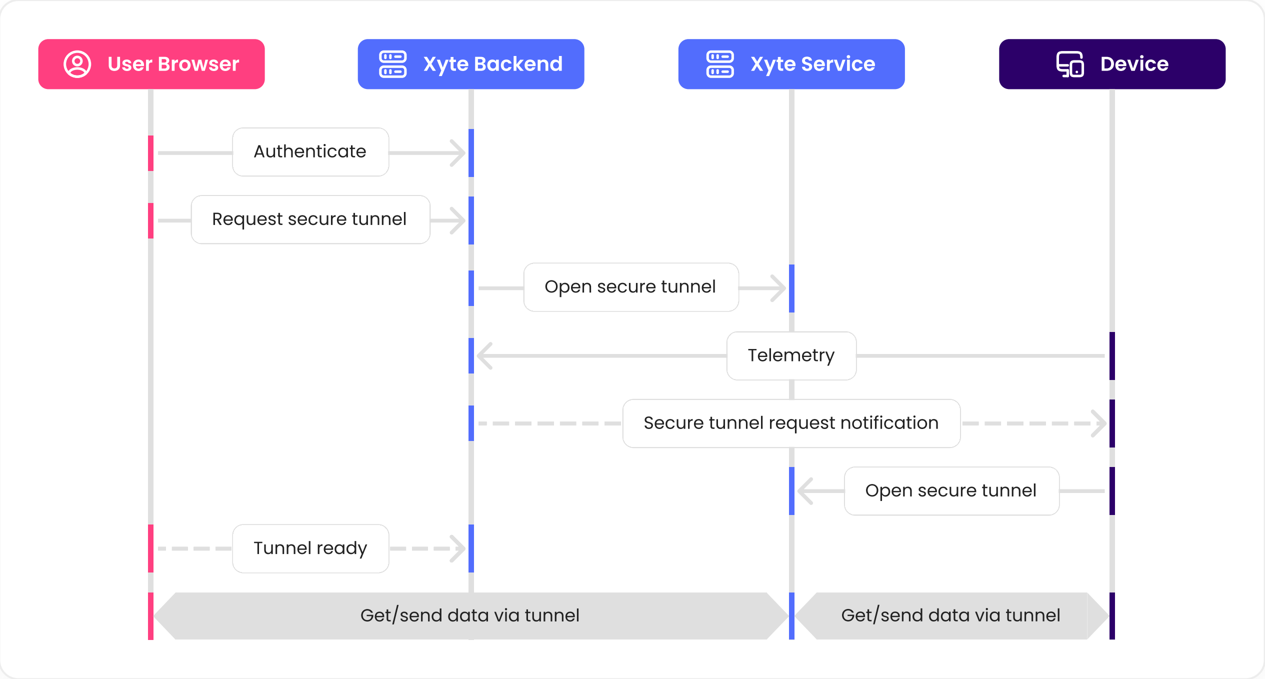
Enhanced Security
Only authorized individuals can access your AV systems, minimizing the risk of unauthorized access or malicious interference.

Reliable Data Handling
With secure tunneling, data integrity is maintained, ensuring that no tampering or data loss occurs during remote interactions, crucial for sensitive operations or troubleshooting.



How does Xyte's Secure Tunneling work?

1. Xyte uses a reverse SSH Tunnel architecture, which securely initiates the connection from the device to the server, mitigating the need for opening incoming ports into organizations.
2. Xyte does not require agents installed on any device, simplifying deployment and reducing potential vulnerabilities.
3. Two steps are required to successfully implement secure tunneling:
   - Outgoing ports required: 49152 - 65534.
   - Domains for tunneling are dependent on your region (for example): **eu1.hub.tunnel.xyte.io**



Penetration Tests and Architectural Security Review

Xyte retains third party security firms to run penetration tests on a regular basis and architectural security reviews.

Additionally, Xyte takes several measures to ensure the highest levels of security and privacy, including:

Data hosting in a highly resilient infrastructure

Xyte's security model and controls are based on international standards and best practices. Our systems are hosted on Amazon Web Services (AWS), ensuring that your data is available whenever you need it. AWS employs leading physical and environmental security measures for a highly resilient infrastructure.

Secure, frictionless authentication for all user journeys and tenant management

Xyte enables multiple, frictionless authentication methods for your users to avoid needless redirects and detect and stop bot attacks, adhering to session management best practices.

SOC 2 TYPE 2 GDPR CCPA MFA SSO