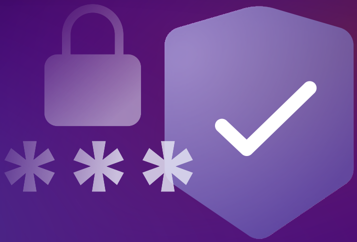
SECURITY AT SCALE



The security of your connected devices and the trust of your customers can make or break your business. You can't afford to gamble.

Xyte is built with security at its core. Our platform follows modern SaaS security standards and enterprise IT requirements, making it easier to complete security reviews and vendor assessments with confidence.

Compliance & Governance

SOC 2 Type II Certified

Xyte maintains SOC 2 Type II certification, covering security, availability, and confidentiality controls, which have been validated by independent auditors.

GDPR, CCPA & DPA

Xyte supports its customers in achieving compliance with the General Data Protection Regulation (GDPR) and the California Consumer Privacy Act Regulations (CCPA).

Privacy and Data Protection

Xyte maintains a published Privacy Policy and Data Processing terms. Data handling practices align with industry standards for SaaS providers.

Subprocessors

We maintain transparency regarding subprocessors used for infrastructure and service delivery. See the current list of Xyte's authorized providers in our documentation portal.

Identity & Access Management

Single Sign-On (SSO)

Xyte supports SAML-based SSO integration with enterprise identity providers.

Two-Factor Authentication (2FA)

Multi-factor authentication is supported and can be enforced at the organization level.

Role-Based Access Control (RBAC)

Administrators can define user roles and permissions to ensure appropriate access control.

Principle of Least Privilege

Internal access to production systems is restricted based on role and necessity.

Data Security

Encryption in Transit

All data transmitted between devices, Edge components, and Xyte cloud services is encrypted using TLS 1.2+.

Encryption at Rest

Customer data stored within Xyte infrastructure is encrypted at rest using industry-standard encryption mechanisms provided by AWS.

Data Segregation

Customer environments are logically isolated to ensure strict separation of data.

Secure APIs

All API communications require authentication and are protected via encrypted transport.

Network Architecture & Connectivity

Outbound-Only Architecture

Xyte is designed so that all data traffic with client organizations is outbound only. No inbound firewall ports need to be opened. No incoming connections are initiated from the Xyte cloud into customer networks.

No VPN Required

Xyte does not require VPN tunnels or inbound routing rules to operate.

Hosting & Infrastructure

Amazon Web Services (AWS)

Xyte is hosted on AWS.

EU Hosting

European customer data is hosted in AWS Ireland regions.

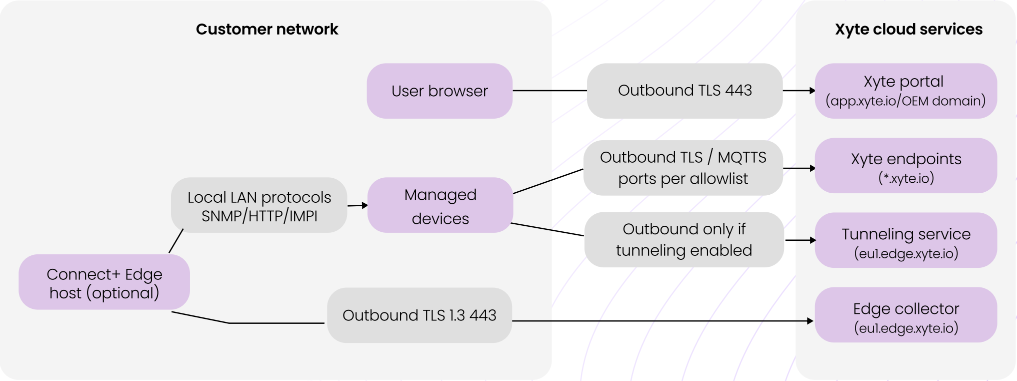
High Availability Architecture

Infrastructure is designed for redundancy and reliability.

Continuous Monitoring

Systems are monitored for uptime, performance, and security anomalies.

Xyte Secure Outbound Architecture


Customer network
Xyte cloud services
User browser
Outbound TLS 443
Xyte portal (app.xyte.io/OEM domain)
Outbound TLS / MQTTS ports per allowlist
Xyte endpoints (*.xyte.io)
Local LAN protocols SNMP/HTTP/IMPI
Managed devices
Outbound only if tunneling enabled
Tunneling service (eu1.edge.xyte.io)
Connect+ Edge host (optional)
Outbound TLS 1.3 443
Edge collector (eu1.edge.xyte.io)

Device communications occur via outbound TLS connections to Xyte cloud services. No inbound ports are required.

Edge Security

Outbound Communication Only

Edge devices initiate outbound connections to Xyte cloud services. No inbound connections are required.

Hardened Device Configuration

Edge components are designed with minimal exposed services and hardened operating system configurations.

Secure Device Claiming & Provisioning

Devices must be securely claimed and authenticated before being associated with an organization.

Encrypted Communications

All traffic between Edge components and Xyte cloud is encrypted.

Operational Security Practices

Access Controls

Production access is restricted and logged.

Audit Logging

System events and administrative actions are logged for traceability.

Vulnerability Management

Security updates and patches are applied according to defined internal policies.

Secure Development Practices

Xyte follows secure coding practices and performs internal review and testing prior to releases.

Documentation & Transparency

Customers can access detailed technical documentation including internet access requirements, Edge security documentation, data subprocessors, and security and privacy FAQs. Additional documentation is available upon request to support formal security reviews.

For additional info or to support a security questionnaire, contact your Xyte rep. or email support@xyte.ai.