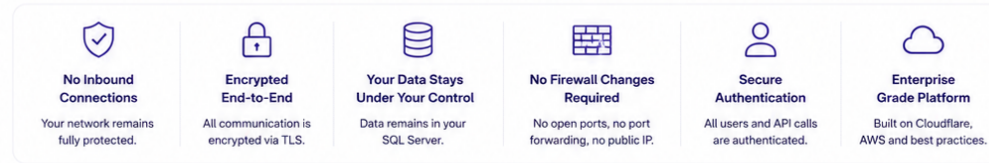


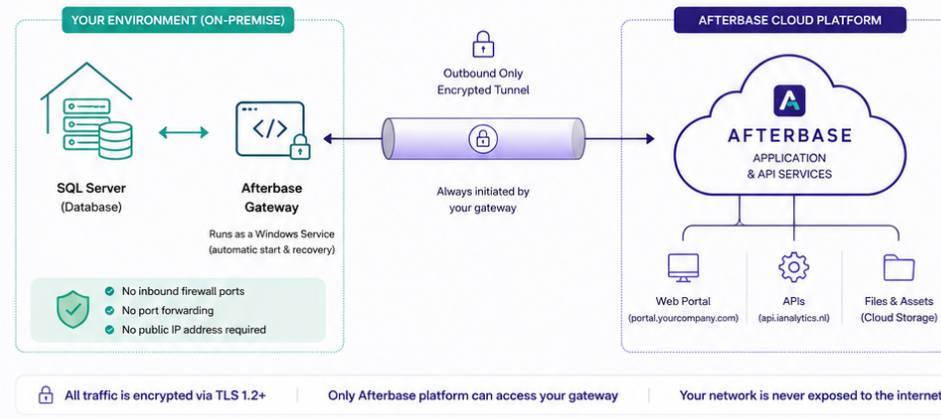
Afterbase Security

Your data. Your control. Built for enterprise security.

Afterbase is designed with security by default. Your data stays in your environment, connected to our platform through a secure, outbound-only tunnel.



How it works



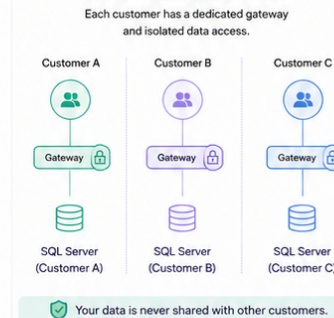
SECURE BY DESIGN

- ✓ **No inbound connections to your network**
The gateway initiates the connection.
- ✓ **No firewall changes required**
No open ports, no port forwarding.
- ✓ **No public IP address required**
The gateway works behind any firewall.
- ✓ **End-to-end encrypted**
All communication is secured with TLS.
- ✓ **IP restrictions at the edge**
Only Afterbase backend systems can connect to your gateway.
- ✓ **Strong authentication**
JWT-based auth for users and APIs.

RELIABLE & RESILIENT

- ✓ **Automatic reconnection**
The gateway maintains the tunnel and reconnects automatically.
- ✓ **High availability**
If the connection is interrupted, the platform remains available.
- ✓ **Monitored & healthy**
Continuous monitoring ensures optimal performance.
- ✓ **Windows Service**
Automatic startup on reboot and auto-restart on failure.

MULTI-TENANT ISOLATION



Security is our priority. Always.

Afterbase follows industry best practices for security, privacy and compliance.

- Data Privacy By Design
- Regular Security Updates
- Role-Based Access Control
- Audit Logging & Monitoring

In short:

- ✓ Your network stays protected
- ✓ Your data stays in your control
- ✓ Communication is secure and encrypted
- ✓ No complex firewall configuration
- ✓ Built for enterprise environments