PROTECTING WATER UTILITIES:

ATTACK RESPONSE & SECURE THIRD-PARTY ACCESS

BIFROST connect

REMOTE ACCESS AS IT SHOULD BE

Before the attack	**Hackers look for weak spots** • Scanning for open ports and outdated systems • Phishing emails to steal passwords • Insecure remote access left open	**BifrostConnect:** Replaces risky VPN and open ports with a secure hardware access path.
Attack detected + Immediate response	**Systems act strangely** • Alarms or unusual SCADA behavior • Equipment starts/stops unexpectedly • Operators lose access or see ransomware notes **Stop the damage** • Isolate affected networks and computers • Switch to manual control if possible • Notify security staff and authorities (e.g., national CERT)	**BifrostConnect:** enables safe, isolated troubleshooting and rapid expert support without opening the network, while logging all actions for later analysis.
Recover operations	**Bring systems back safely** • Identify and close the entry point • Restore from clean backups • Test before returning to normal operation	**BifrostConnect:** Gives BIOS/KVM-level access to restart and repair systems remotely without reconnecting to compromised networks.
Prevent future attacks	**Build stronger defenses** • Strong passwords + multifactor authentication • Close unused internet connections • Keep systems and software updated • Monitor for abnormal activity • Regular penetration tests and exercises • Clear, practiced incident response plan	**BifrostConnect secures 3rd party access by:** • removing permanent VPN exposure • granting only temporary, role-restricted access • physically isolating OT networks (air-gap) • logging all actions for traceability and compliance **Result:** suppliers can service safely without exposing the entire water system to hackers.