Secure connectivity.

Customer Boiler(s)
» Customer's specific on-site **physical and technical security** practices

C-B Monitoring Gateway
» Proprietary hardware design maintains **absolute control** over one-way flow of data from PLC
» No LAN/WAN, Wi-Fi or Bluetooth vulnerability
» Unique device identifier to **prevent unauthorized access**
» Only C-B monitoring gateways are permitted to connect to the **secure C-B Cloud**
» Gateway has a **non-published address** on cellular network
» **Security penetration testing** certified by a third-party auditor
» Defined **metadata management**

Cellular Network
» **Encrypted transmission** over a secure channel
» **Restricted** to C-B gateway devices only
» **Device patching** via secure tunnel between gateway and C-B Cloud
» **Certificate security** for added protection

C-B Cloud
» Virtual **private** cloud
» Web application **firewall**
» Data **encrypted** at rest
» Cloud-provided **security controls** mapped to leading standards
» **Virtual firewall** protects global infrastructure
» **Continuous security monitoring** and logging tools
» Administrative access via **multi-factor authentication**
» **Active security management** of user privileges based on role
» **Security penetration testing** certified by a third-party auditor
» ISO 27001 **certification** for information security management
» Replicated data centers

Users
» **Encrypted** browser-based connection
» **Active security management** of user privileges based on role
» Transport **layer security**

Call **1-800-296-4110** to find your local representative or visit **prometha.com** for more information.

© 2020 Cleaver-Brooks. Inc.

CleaverBrooks®

promētha™
Connected Boiler Solutions

SECURITY VALIDATION
CERTIFIED
PENETRATION TESTING