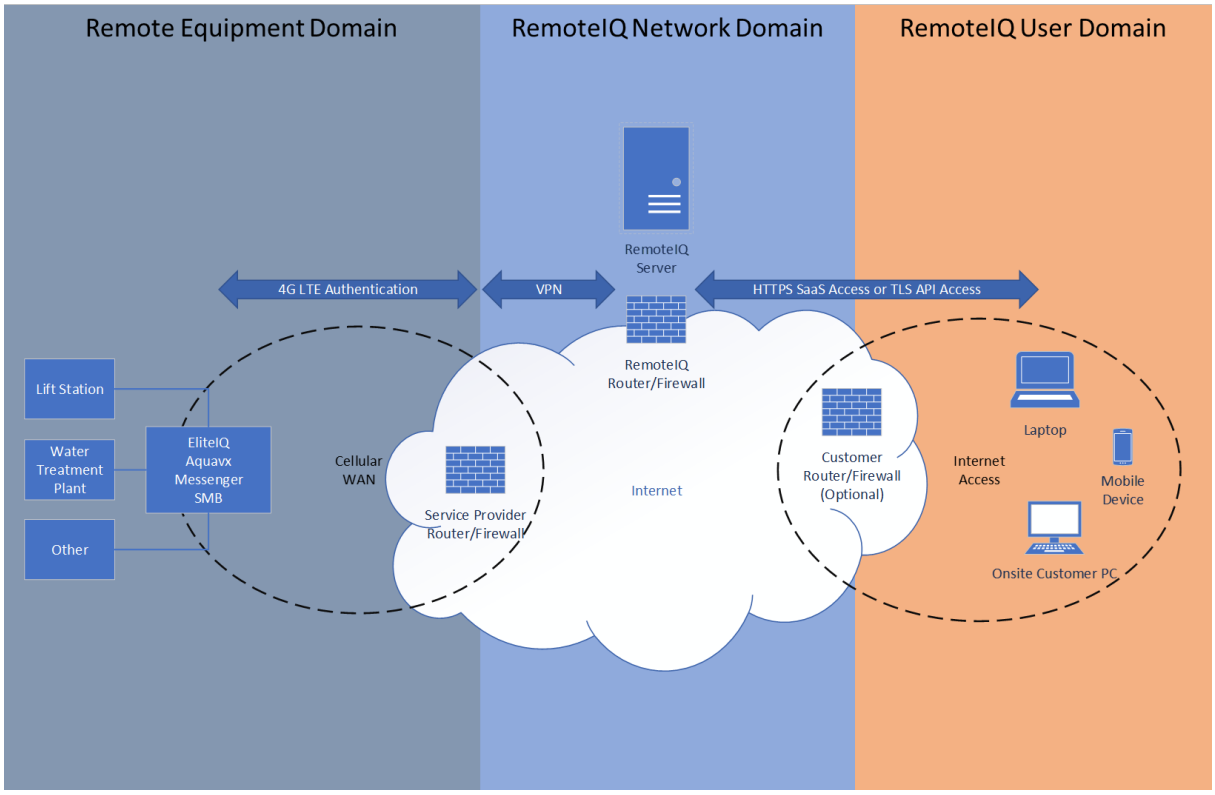
CATTRON™

RemoteIQ™ Security Overview

Water & Wastewater Applications

RemoteIQ™ provides security provisioning in three domains for water and wastewater municipal customers. This is, in part, to emphasize that Cattron IoT devices are never on a customer's network or SCADA platform. Due to this separation of domains, malware or viruses cannot pass to/from Cattron devices by tunneling into them from a customer's network or vice versa.



Remote Equipment Domain

The Remote Equipment Domain refers to remote locations where a customer's equipment and Cattron control/monitoring solutions reside. 4 G LTE cellular data networks provide wireless access to Cattron instrumentation in the field.

The cellular modem is authenticated by the cellular service provider utilizing a unique SIM card for each device and a dedicated, non-public access point name (APN) to which the device communicates over the air. This allows the service provider to manage device connectivity and monitor the cellular connection for suspicious behavior.

RemoteIQ Network Domain

The RemoteIQ Network Domain communicates securely over the Internet to provide connectivity from the RemoteIQ Server to remote equipment in the Remote Equipment Domain and the PCs/laptops/mobile devices in the RemoteIQ User Domain. The end devices in the RemoteIQ User Domain are used to access the web application with a browser.

A Virtual Private Network (VPN) is set up using IPsec to create a secure tunnel between the Cellular Data Provider Router/Firewall and the RemoteIQ Router/Firewall. Each firewall is maintained by the respective organization's network administrator and monitored for suspicious network activity and security breaches.

RemoteIQ User Domain

The RemoteIQ User Domain provides any supported computing device access to the RemoteIQ Server. A supported computing device refers to any stationary or mobile device with internet connectivity running a supported web browser. It should be noted that the end user's PC/laptop/mobile device should have the latest software updates and security patches applied to protect against vulnerabilities completely.

The RemoteIQ web-based application is accessed via web browser utilizing HTTPS, an authenticated and secure connection (via TLS). The RemoteIQ web-based application uses a secure login to provide accessibility from any supported computing device and login credentials are required to access the server.

Customers may choose to implement additional security provisions on their respective IT networks and user devices as necessary.

Contact your Cattron representative or learn more at Cattron.com

North America: +1.234.806.0018 | Sales.US@Cattron.com

Europe: +49.2151.4795.0 | Sales.EU@Cattron.com

UK: +44.1932.238121 | Sales.UK@Cattron.com

South America: +55.19.3518.7030 | Sales.BR@Cattron.com

Asia: Sales.CN@Cattron.com

Oceania: Sales.AU@Cattron.com

Created June 2021.