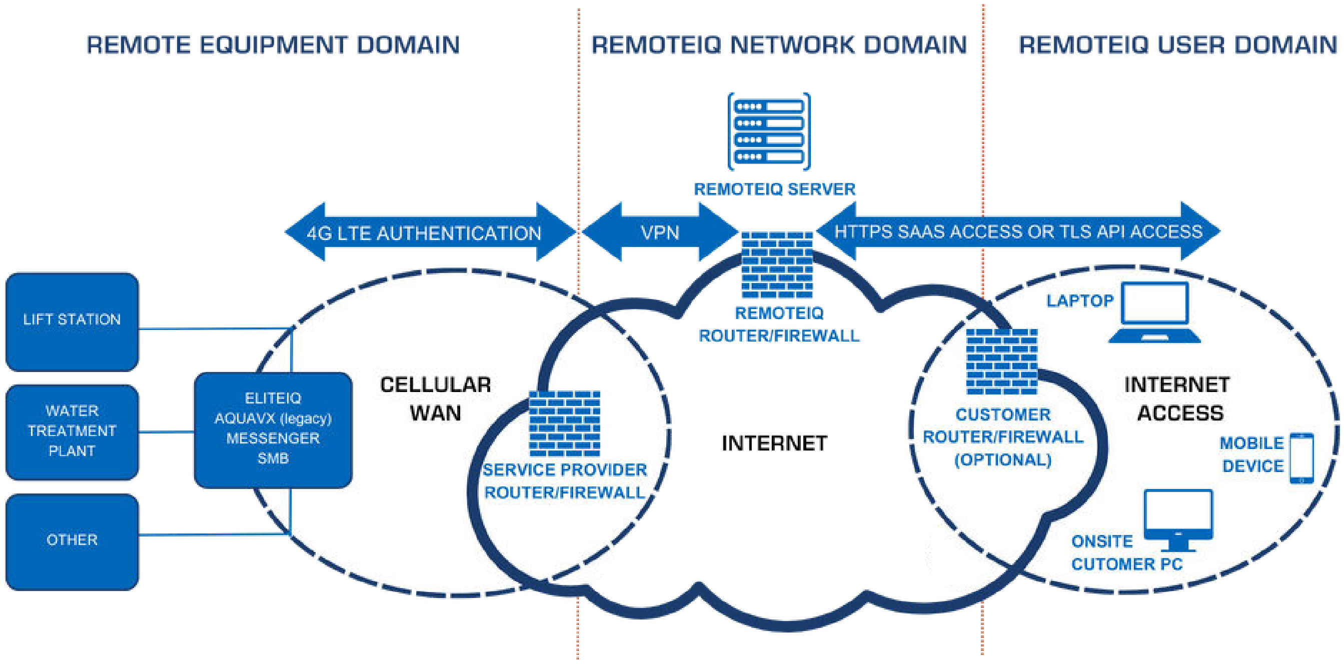
REMOTEIQ™ WATER SECURITY OVERVIEW

FOR ELITEIQ™, AQUAVX™ (LEGACY) AND MESSENGER SMB DEVICES

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



CONNECT. CONTROL. PROTECT.

SECURITY FOR WATER AND WASTEWATER APPLICATIONS

REMOTE EQUIPMENT DOMAIN

The Remote Equipment Domain refers to remote locations where a customer's equipment and Cattron control and monitoring solutions reside. 4G 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 or 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 is 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 a 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 implement additional security provisions on their respective IT networks and user devices.