Securing Shipping from Cyberattacks

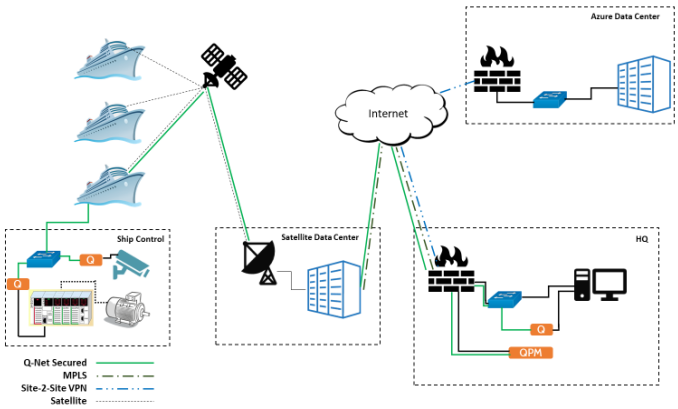
As the recent headlines have shockingly highlighted, utilities, manufacturing, and transportation are challenged more than ever by the possibility of offensive cyberattacks. These critical infrastructures, whether in the US or abroad, are often remote and may need to be managed by collecting and processing telemetry from the devices and delivering control to the devices (see example in the illustration below). Given the distributed locations, an attacker will likely compromise a network using a cyber assault so that physical travel to each location is not required. And being remote, leveraging public network infrastructure can be a cost-effective approach to monitoring and control but too insecure to use responsibly.

As with other industrial control systems and SCADA networks that control our nation's infrastructure, managers of shipboard critical networks need a solution that can resist the best efforts of a rogue state and yet is both simple to install and easy to maintain. Q-Net Security (QNS) provides such a solution enabling OT or IT personnel to achieve system cybersecurity at the most secure level commercially available. This solution does not require any new security software be installed in endpoints nor any network changes to the existing infrastructure. And being of such exceptional strength, it enables operators to securely use the economies of an insecure public network (such as LTE, Wi-Fi, and the Internet).

The QNS solution secures data in transit, protects precious and personal data, prevents all unauthorized network access, and ameliorates Distributed Denial of Service (DDoS), Man-In-The-Middle (MITM), and other nefarious network activities. QNS solutions are particularly well suited for utility applications as being remote challenges conventional security and frustrates maintenance. Furthermore, many components may be aging if barely supportable, and the components may be integrated from a variety of disparate manufacturers. QNS is a drop-in security overlay that protects utilities from compromise, keeps authorized data secured, prevents unauthorized activity from disrupting or weaponizing the control operations, and keeps critical internal information safe from access by either man or machine.

Designed to protect utilities anyplace on the globe, even those lacking sophisticated training and facing severely constrained budgets, QNS delivers security by design and achieves superior protection through a hardware security barrier (HardSec). Drop-in and forget: we provide secure communications anywhere yet are fast and easy to deploy; our systems are also maintenance-free since they never need patching, ever. QNS solutions work seamlessly with existing networks – we don't replace it, complicate it, or degrade its performance. Instead, we simply lay QNS on top of a current network to create an impenetrable barrier that provides ultimate protection and confidence today and tomorrow.

Plug-and-play. Maintenance-free. Future-proof.



Example Shipping Network Implementation Schematic