Q-Net Security Protects Smart City from Coordinated Attack

Cyberattacks on Critical National Infrastructure are increasing

During the week of May 19, 2020, a US DoD Command set up a three-day exercise to protect a Smart City (comprised of municipal infrastructure, utilities, and manufacturing facilities) from cyberattack by a team of elite hackers. This was conducted in a "Red Team/Blue Team" format, where Q-Net Security (QNS) was one of several Blue Team network cybersecurity solutions tasked to identify intrusions and protect the networks as the Red Team worked to break through. QNS focusses on cybersecurity through intrusion prevention (stopping breaches and compromises before they happen); other solutions take a complementary approach of intrusion detection (once the network has been compromised, find, observe, and ameliorate the exploit). US Defense and Intelligence agencies observed the exercise.

QNS was the only solution to prevent breaches

Throughout the entire exercise, the Red Team attackers were unable to penetrate QNS defenses. At no point were any QNS-protected endpoint devices compromised, demonstrating network intrusion prevention at its best. In fact, QNS was the only solution to remain unbroken over the three-day exercise! One DoD Command observed ***"… the Q-Box [lived] up to its description, as neither it, or the endpoint behind it, responded to any scans".***

An unclassified report regarding QNS will be distributed within the DoD that is expected to highlight QNS very positively. It will likely include details affirming key QNS technical claims, such as our ability to drop seamlessly into existing networks and deliver quantum compute-resistant encryption.

QNS solutions are cost-effective, drop-in easy, and low maintenance

QNS has developed easy-to-use, drop-in hardware devices that robustly secure endpoints against known and future hacks and disruption attacks. By creating a constellation of peer-to-peer devices, each of which autonomously rotates truly random encryption keys thousands to millions of times a second, QNS has created the strongest commercially available security solution.

QNS solutions require no changes or modifications to existing infrastructure, and no software agents are installed on the existing endpoints, so no regression testing is required to protect legacy networks. The QNS solution uniquely incorporates a combination of network security features including sessionless VPNs, distributed firewalls, and whitelisting to create a microsegmented and completely secure network. This strong security does not translate to management burden — QNS technology is highly cost effective and easy to implement and manage. Endpoints are secured by QNS without configuring any ports, drastically reducing configuration and management time for new and legacy networks.

Solve your most severe cybersecurity needs with the Q-Net Security "easy button"

QNS provides the strongest cybersecurity network solution for the protection of endpoints, networks, and the data that flow over them. These hardware-based systems deliver quantum compute-resistant encryption, are decentralized for robustness, render network nodes invisible to attackers, and are "drop-in ready" for existing networks. Our system anticipates decades of continuous use without patches or modification. The QNS solution will secure data in transit, prevent unauthorized network access, and ameliorate network compromises, including DDoS and man-in-the-middle attacks.

Q-Net Security