Q-Net Security

The Strongest Commercial Cybersecurity Solution

Q-Net Security is delivering National Intelligence-grade solutions to enterprises for securing all data in flight, especially machine-to-machine (including IoT applications). Q-Net uses a patented hardware barrier that leverages strong, quantum-resistant encryption and True Random Number Generated symmetric keys that can change every packet or transaction to move and authenticate data securely and is drop-in ready to implement in public networks. By operating at line rates Q-Net can also protect endpoints from such nefarious activities as DDoS attacks.

HIGHLIGHTS

1. Secure Communication Utilizing the Public Internet
2. Hardware-Based (Silicon) Approach to Cybersecurity
3. Simplify Security on Legacy Systems
4. Utilizes Quantum Resistant Symmetric Keys
5. Next Generation Encryption: AES-256
6. Encryption Keys Changed Every Transaction
7. Superior Information Authentication
8. Achieve and Maintain International Compliance

A new approach to cybersecurity which has significant advantages over current solutions. The crucial difference is that a physical hardware barrier is provided to thwart cyber attacks.

PATENTED TECHNOLOGY

"Secure Network Communications using Hardware Security Barriers"

About Us

Q-Net Security, Inc. (Q-Net), is an innovative cybersecurity company based in St. Louis, Missouri. Founded in 2015 by a team of highly acclaimed technologists, engineers and security experts, Q-Net is driven to provide clean communication channels which leverage the public internet. Through the power, performance and the inalterable nature of silicon, Q-Net's hardware-barrier is a truly groundbreaking approach to cybersecurity.

For more information, please contact us:
info@qnetsecurity.com

National Intelligence-Grade Cybersecurity

qnetsecurity.com

Q-Net Security

A Different Cybersecurity Approach

Contemporary cybersecurity methods are software based, such as monitoring the status of the network, monitoring the operating system, or implementing patches and updates. Q-Net's approach is focused below the operating system. Q-Net enforces cybersecurity at the hardware, or silicon, level.

Silicon-Based Approach to Cybersecurity

A benefit of hardware security (in silicon) is that it cannot be hacked. Silicon, by definition, is "immutable" and cannot be modified in any way by an attacker. In addition, since there are no changes that can occur to the security, there is no need to provide additional tools to observe suspicious network activity. The Q-Net Policy Manager (QPM) records statistics on unauthorized packets.

Simplify Security on Legacy Systems

Existing networked computers with point-to-point communications can be Q-Net enabled simply by inserting a Q-Net device (Q-Box) between each endpoint and the network. The Q-Box operates independently of the endpoint and thus has no impact on existing configuration or performance.

Next Generation Encryption

Q-Net utilizes the US Top-Secret standard, AES-256 encryption, utilizing symmetric keys for which decryption is computationally intractable. In addition, Q-Net changes keys after every packet or transaction, further reducing the risk of exposure beyond that required for national security. The entropy needed for these many keys comes from a separate True Random Number Generator (TRNG) located in each endpoint.

A Hardware Barrier Separates Endpoint from Network

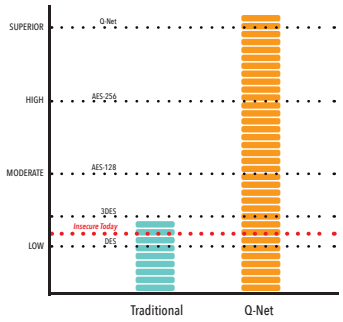
Q-Net's hardware barrier security completely isolates the protected node (computer) from the unprotected and untrusted network. This barrier not only provides encryption, but also authentication and detection of violations of packet integrity. The barrier is completely independent of the protected node, cannot be compromised and utilizes no resources in any protected node.

Superior Information Authentication

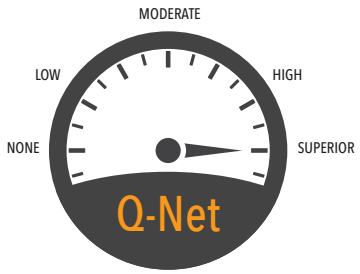
Q-Net technology ensures that all packets forwarded to a Q-Net endpoint are generated by an authorized source and have not been covertly or accidentally altered. Q-Net uses Galois Counter Mode (GCM) technology to achieve non-repudiation and message authentication.

International Compliance

With Q-Net, regulatory compliance is a snap. Organizations facing Sarbanes-Oxley, HIPAA, GDPR-EU, and other governmental regulations need to demonstrate active implementation of industry best practices that comply with these rules to avoid breaches and potentially substantial fines. Q-Net goes beyond industry best practice and raises the bar for compliance with confidentiality of sensitive information. For those criminals who try to gain inappropriate access to these precious data, the bar becomes unreachable.



TOP SECRET ENCRYPTION



SUPERIOR AUTHENTICATION

QUANTUM RESISTANT

INTERNATIONAL COMPLIANCE