knectIQ

Building Trust Environments in a Zero-Trust World™

KnectIQ® Introduces KIQAssure®

Ultra High Security Solution for Data in Flight

We live in an increasingly connected world where digital communication and data movement is ubiquitous and critical, yet fundamentally untrustworthy. With existing solutions, not only is it difficult to secure data movement, it is impossible to know whether data movement has been compromised. Worse, a single fault can shatter system security.

KIQAssure® enables Trust Environments where communication and data movement occur without the threat surfaces associated with today's best practices.

Now imagine if the world could actually trust that their private communications are safe. The impact would be enormous.

KnectIQ enables Trust online. Without our solution, delivering trusted communication online is not just expensive - it is impossible to do consistently. Existing solutions cannot ensure the identity of the sender, receiver or even the security of the message. Worse, when security is broken, it is usually impossible to know that a breach has occurred.

The Problem

Breaches are common. Breached records are counted in the billions, and the cost of these breaches is measured in billions of dollars annually and deeply impacts customer trust.

While the means of compromising data in transit means some uncertainty about how often it is occurring, the chilling effects of lack of trust online are easy to see.

- Widespread consensus that public WIFI is dangerous, even with HTTPS.
- More than half of consumers have too little trust in online banking to utilize it.
- Medical research data cannot be shared online, limiting progress against disease.

KIQAssure®

1. **No need for Certificates of Authority.**
2. **No stored keys acting as Single Point of Failure.**
3. **Only known endpoints allowed to communicate.**
4. **Attempted breaches immediately detected.**

Finally, the world has real end-to-end encryption. Plus, KIQAssure is less expensive due to the elimination of costly key management programs.

Contact us today for a demonstration.

Contact Info:

secure@knectiq.com
651-447-4264

These problems exist because current solutions are built upon a flawed foundation. They bootstrap trust using three static elements: A Certificate Authority (CA), a preconfigured trust chain on one side, and a secret key on the other.

For this solution to work, dozens of keys across as many organizations must be kept secret, and users must correctly manage their computer's trust configuration. Any mistake is a Single Point of Failure (SPoF) for the system.

Commercial systems do not tolerate SPoF in their design. Yet existing security protocols are rife with SPoFs. Worse, the consequent breaches are undetectable.

Today, we begin with a flawed premise, we can't keep secrets, and breaches are undetectable.

This must change.

KnectIQ Difference

KnectIQ's system is not built upon a flawed foundation of static keys but leverages the relationship of the communicating parties. Specifically:

- **No Certificates** – CAs are often a proxy for identity. We remove this SPoF.
- **No Stored Keys** – The keys that secure our communication are used once then destroyed, removing this threat surface from the system.
- **Endpoint Provenance** – KnectIQ manages the identity of each endpoint and only enables communication between them.
- **Fully Auditable** – breaches are identified immediately, logged, and stored for further investigation.

KnectIQ enables organizations to secure online communication by employing these principles. Every communication is secured with a unique key that is immediately discarded, and only known endpoints are allowed to communicate.

Microsoft
P2P Member Company

WorkSpan
Ecosystem Cloud