KnectIQ

WHITE PAPER

DoD Data Optimization:

Improving Operational Capabilities Through Secure Data Availability

KnectIQ Inc.
T: +1.651.447.4264

E: secure@knectiq.com
www. KnectIQ.com

1915 Highway 36 West
Roseville, MN 55113 USA

5 Rue de Bonnevoie
L-1260 Luxembourg

Objective/Problem Statement

Information Warfare and the cyber arena are the most challenging and important theater of global military and intelligence competition, both today and into the future. KnectIQ provides the data security, operational agility, and on-time information advantage necessary to dominate across the digital domain battlespace.

KnectIQ enables the full potential realization of multi-source data transmission, C4I and information advantage at reduced cost, full scalability, and any classification level.

Background on what problem KnectIQ technology solves

Modern networked infrastructure is dependent upon the integrity of its data communication. Data integrity requires knowing exactly where the data is coming from (identity) and preventing unauthorized access to reading or sending data (security). Currently deployed cybersecurity solutions have proven incapable of securing communication or ensuring identity due a security foundation dependent on the protection of static keys. This often requires a choice to "not use" the data rather than risk "losing it". This severely limits the mobility and delivery ability of critical data to optimal end-point users, blunting potential information and data superiority advantage.

Static Keys are a Single Point of Failure

Every lock needs a key. It is no different with software encryption where a secret key must be used to decrypt the data being sent from one endpoint to another. Existing solutions leave the key stored on endpoints well beyond their practical use. The infrastructure created to support key distribution and maintenance creates keys long before they are needed and, by default, adds to the attack surfaces adversaries can exploit. The organization is only one breach, misconfiguration, or leak away from losing the secrecy of their communications.

In fact, security based on the existing Certificate Authority model relies upon the integrity of the private key, one or more intermediate keys, and the root key to establish authenticity. Each one of those keys, if compromised, represents a single point of failure of the entire system. See Figure 1:

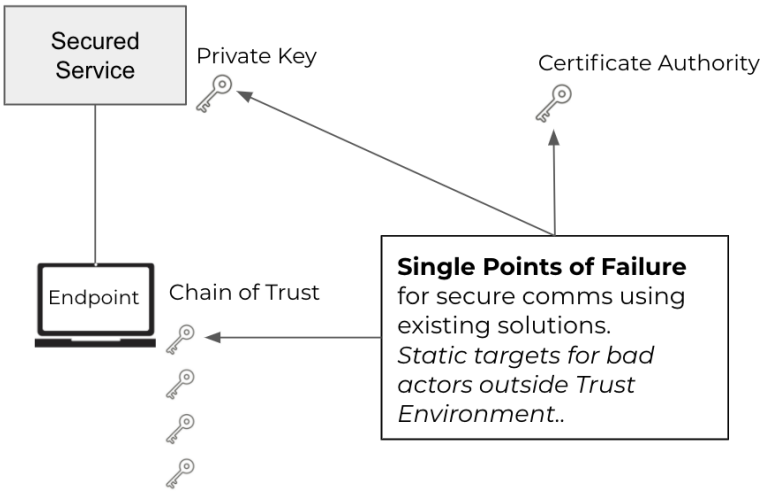


Figure 1. Single Points of Failure

Consequences of Static Keys

Inability to Detect Threats and Leaks: When a key is compromised, security is broken, and traffic is decoded in flight and visible to adversaries. Worse, unless the adversary uses the leaked data in a way that shows that the breach occurred, the compromise is undetected and can continue undetected for the remaining life of that key.

Impersonation: Here the identity of the sender of the data is not assured, so an adversary can impersonate a legitimate source. This can lead to installation of unauthorized software (e.g., Stuxnet, where Iranian nuclear facilities were brought offline), inserting bogus records, or otherwise spreading misinformation.

Inflexible and Slow: Because the consequences of losing these static keys are so great, care must be taken to protect the sending and receiving locations of sensitive data. This network centric security is too cumbersome for the digital battlefield and is why DISA has started moving away from it.

Current Zero Trust and Data Centric Solutions: Not a Solution

Zero Trust and Data Centric network solutions are being discussed, investigated, and adopted across a wide swath of the military, intelligence, and government communities. While this approach to network architecture provides a higher level of security (in that it more precisely matches the curated user/device to the data source to be accessed), these networks still rely on the flawed security architecture laid out above. Specifically, once the data starts moving, the static key method of securing the two ends of the encrypted data transfer continues to provide a rich target environment for adversaries to exploit and gain access to that communication and potentially even future communications between those or other endpoints. Without eliminating this threat surface, no change in network configuration or access policies could protect data in flight from these attacks.

Problem Summary

No critical infrastructure tolerates single points of failure in the delivery of their service. Web servers, databases, power supplies, network connections, and even geographies are redundant in most applications. However, the security of data in transit rests uncomfortably upon dozens of single points of failure. This problem is widely recognized by military, intelligence, and government leaders. As a result, solutions that inhibit the free flow of data have been implemented to try and improve the security of data transmissions. These solutions merely move the problem around, still allow a broad attack surface for adversaries, and introduce cost and complexity to data security that cripples digital battlefield dominance.

Technical Overview

The KnectIQ solution succeeds because it uniquely addresses the root of the problem. By focusing on the root cause, the system leverages the proven strength of existing cryptographic tools along with the technology of “no static keys”, simultaneously protecting against, detecting, and containing any breach.

KnectIQ is enabled by an identity-based approach to security. Where existing systems use static keys to establish security before establishing the identity of those communicating, this solution reverses the script:

KEY-BASED	IDENTITY-BASED
Security first	Identity first
Then identity	Then security

The security protocols of today were created in the 1990s when much communication was between parties where identity was not already established. This does not meet today’s military, intelligence, and government requirements for success in an information-centric competition space. The KnectIQ solution uses the power of identity to fully realize the desired security and agility of traditional and Data Centric information systems. Data in this architecture is no longer location limited but end-user optimized. Furthermore, due to the nature of the system design, each data packet can be tracked and verifiably decrypted by the intended receiver. As a result, real-time threat detection and security compromise is possible, reducing burdens on the Security Operations Center. Finally, a cryptographic infrastructure built on identity can take Zero Trust architecture to a place of great advantage.

Zero Trust

Zero Trust only allows identified users to access controlled data or services. But existing cryptographic systems do not identify the endpoint from which the user is connecting, and they also accept connections from untrusted endpoints. It is only when Zero Trust is built on top of a cryptographic system that ensures the identity of the endpoints that all its benefits are realized. By positively identifying every endpoint, a KnectIQ enabled Zero Trust endpoint delivers two significant benefits:

1. **Enhanced Security** that avoids the vulnerabilities inherent in legacy systems. MITM, interception and other attacks on data in flight are defeated.
2. **Reduced vulnerability to compromised credentials**. A bad actor attempting to use valid credentials to penetrate the network would be rejected because they would be coming from an external, untrusted endpoint. Almost all attacks originate from untrusted endpoints, and attacks as identified in the Solar Winds breach would be defeated by locking out bad actors even from compromised node.

By protecting communications between trusted endpoints and making the endpoints reject connections from untrusted endpoints, the benefits of Zero Trust can be fully and verifiably achieved.

KnectIQ Zero Trust Architecture

KnectIQ securely manages the identity of every endpoint - centrally. It accomplishes this through the creation, management and use of a Trust Environment. Simply put, a Trust Environment is a set of endpoints that are allowed to communicate securely with each other. Communication can only occur when a sender and a receiver are both provisioned within the trust environment and then bound together, enabling communication. The Trust Environment is broken into two parts: Broker and Device.

Broker

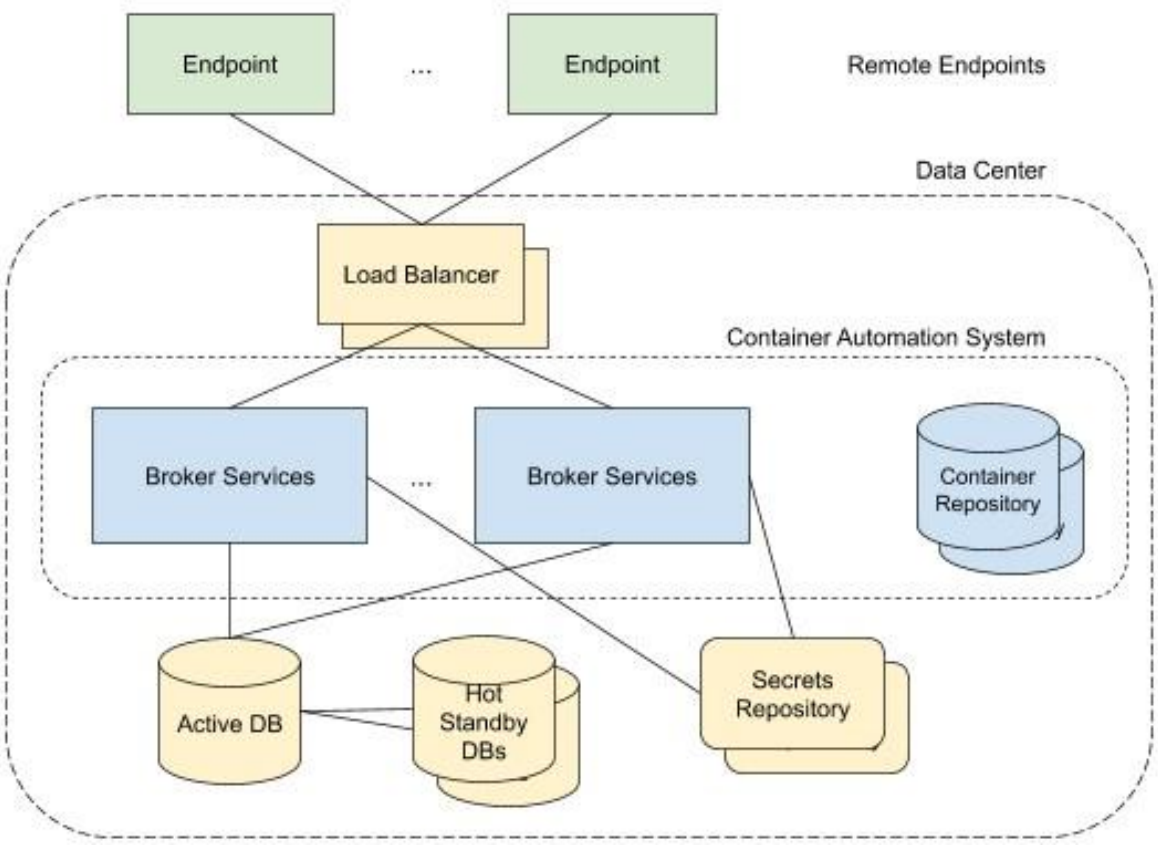
The broker manages the Trust Environment. Deployed on premises or in a private or government cloud, the broker enables configuration and operation of the Trust Environment. It does this by enabling the following operations:

Provisioning: Endpoints can be added or removed from a Trust Environment.

Binding: Endpoints can be bound so that they can communicate with each other.

Operating: Once provisioned and bound, endpoints can communicate with the endpoints with which they are bound.

Although only a single Broker is shown in the system diagram below, it is built for redundancy and scalability, with many processes handling the load.



Key Design Points

- All components can be deployed with redundancy.
- While this drawing shows an Enterprise deployment, the system can be scaled down to run on small devices.
- Although only one Active DB is shown, this can be scaled horizontally for large applications as well as down for smaller.
- The details of the services are not shown. Instead, Broker Services represent the various services responsible for delivering the configuration and operational functionality.
- No component of the system is tied to a specific operating or container automation system, but the broker is usually delivered as a containerized solution, for example in Kubernetes.

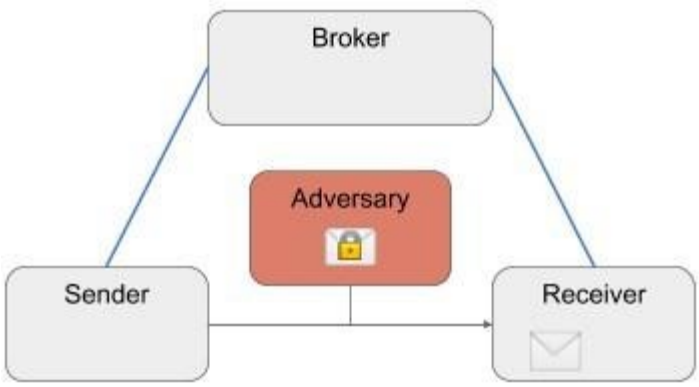
Device

Devices are the endpoints in a Trust Environment. They can be physical or software devices. As a software device, they can be integrated into any application or system that is on the network with the Broker.

Once provisioned and bound to other Devices, they can communicate with (and only with) the devices with which they are bound.

System Operation

Putting it all together, secure communication between sending and receiving devices can be diagrammed as follows:



- Every communication has a new key - only at the moment it's needed - not before or after.
- Communication is secure and auditable.
- Attempted breaches are flagged.
- No expensive, slow, human-reliant key management systems
- Allows increased speed-of-data delivery with easily configured provisioning of endpoints in any network.

Note that the data communication path remains unchanged. Communication continues to flow over existing networks, but with new security.

METHODOLOGY

Implementing this solution can be broken into the following steps:

1. **Identify Communication Networks:** During this phase, the communication networks to be protected are identified. These may be existing networks in need of better security or new networks that have required better security before deploying. This phase may identify multiple independent or interconnected networks. Depending on this discovery the remaining steps may be carried out independently, in concert, or sequentially for the identified communication networks.

2. **Identify Management:** Parties responsible for identifying and allowing access to communication and data are identified. This enables better provisioning of endpoints later. If desired, the people responsible for responding to threat alerts and notifications are also identified.

3. **Identify Endpoints**: The hardware or devices and software that are sending and receiving data are identified.

4. **Software Integration Plan:** Having identified the communication, management, and endpoints, a plan is created to enable the deployment to every type of node. This plan will include:

    a. Planning software modification or additions

    b. Identifying where the Broker will be hosted and managed while ensuring availability as required by the application.

    c. Identifying how endpoints are provisioned into the Trust Environment and creating necessary identification for provisioning.

    d. Creating an alert management plan

        I. Threat Detection: Who receives any alerts for threat detection.

        II. Review: Who is responsible for reviewing security logs

        III. Automated Threat Response: Define automated response when threats are detected.

        IV. Proof of Concept: A version of the system is implemented and tested to verify the design and architectural decisions. The logs of system communication are reviewed, and penetration tests and other evaluations are run. Any needed changes or iterations of the initial plan are handled in this phase.

5. Limited Rate Initial Production (LRIP) and Multi-System, All Domain Full Rate Production (FRP).

SOLUTION APPLICATIONS

The system provides cutting edge data security solutions across the breadth of military, intelligence and government network and information sharing requirements. Enhanced security and information agility can be delivered in numerous critical components of the digital competition space.

Network Security:

Secure data in flight across the entirety of military, intelligence, and government computer systems, regardless of classification level. Enable controlled information and collaboration engagements on existing networks or commercial infrastructure.

Command, Control, Communication, Computing, Intelligence, Surveillance, Reconnaissance, and Targeting (C4ISR&T):

Ultra-secure data and communication transmission and sharing across a wider collection and distribution spectrum in real time.

Advanced Data Collaboration and Distribution Systems:

Increase the incoming information stream and outbound delivery endpoint security for increased operational collaboration and coordination when used in advanced battle management and collaboration systems. Tailorable in real time to information security level/endpoint receiver.

Critical Infrastructure Protection:

Energy command and control system security, early warning system data security.

Unmanned System Command, Control, and Data Management:

Ultra-secure command and control of unmanned systems in any domain, thwarting attempts of seized control or counter commands by adversaries. Secure transmission of video/data collection products from collection source to endpoint.

Satellite/Space Network Communication Security:

Secure data transmission and distribution across all pathways and data types throughout the satellite constellation. Provides a non-hardware intensive, updatable security capability throughout a rapidly configurable, interconnected constellation system for enhanced reliability and flexibility of communication and data transmission needs, secure from network data intercept/decryption, corruption, and pathway disruption risks not associated with physical satellite attack.

Quantum Proof Cryptography:

This system has no public keys and no attack surface for quantum computing.

SOLUTIONS SUMMARY

The KnectIQ provides the following capabilities:

Security: Because every communication has its own key, it is not vulnerable. The threat surface associated with static keys has been completely removed.

Verifiability: Every communication generates audit logs that enable the system to monitor exactly where each communication was encrypted and decrypted. Every endpoint in the system is also tracked ensuring the identity of the sender and receiver for every communication.

Threat Isolation: Attempts to steal a key are blocked and flagged. Even a compromised endpoint would only be able to leak key material for a single message.

Automated Threat Detection: Any attempt to breach this system leaves a trace that is automatically flagged, allowing the system to defeat the attempt and investigate the causes.

Flexibility: Because the attack surface associated with static keys has been removed, this system enables agencies to provision secure endpoints outside the traditional network centric model. Thereby allowing the secure use of classified data in situations where it was previously not possible.

Scalability: This system can run in small environments or secure vast amounts of data across millions of endpoints.

High Availability: Every component of the system can be deployed with redundancy and resiliency, enabling carrier class reliability.

Intellectual Property Details

Patents Granted

Issue Date: 11 June 2019
US Patent No. 10,320,785

METHOD OF PROTECTING THE IDENTIFYING INFORMATION OF PERSONS AND COMPUTING DEVICES, SPECIFICALLY THOSE DEVICES WHICH ARE CAPABLE OF SENSING, CAPTURING, RECEIVING, TRANSMITTING, PROCESSING, AND STORING DIGITAL INFORMATION

Issue Date: 02 Nov 2021
US Patent No. 11,165,568

SYSTEM AND METHOD FOR SECURE ELECTRONIC DATA TRANSFER