KnectIQ

WHITE PAPER

Banking & Financial Services Data Loss Protection

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

Introduction: Cybercrime and the Banking Industry

Cyberattacks on the banking sector are up 238% in 2020 according to ZDnet.
Over 25 percent of all malware attacks in the world hit banks and other financial institutions, more than any other kind of industry, as recently reported by IntSights. According to the Boston Consulting Group, financial firms are 300 times more likely than other institutions to experience cyberattacks. Yet, in many cases the technologies used to protect these vital institutions and their ultra-sensitive data are based on 30-year-old security protocols that have known vulnerabilities.

Problem Summary

Cyberattacks on financial institutions come in many forms, but the common theme across all attacks is an unauthorized party gains access to the bank's network or data flows. From there, data theft, ransomware installation, etc. can be accomplished. Access to these networks and data can be accomplished through various means of exploiting the flaws in currently deployed cybersecurity solutions which have proven incapable of securing communication or ensuring identity due to a security foundation dependent on the protection of static cryptographic keys. Criminals can steal these keys and with them impersonate network users with valid access. Once past this exploitable gate, bad actors have unfettered access to the institution's most valuable data assets.

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 in the financial sector rests uncomfortably upon dozens of single points of failure. This problem is widely recognized by military, intelligence, government, and private industry. Current cybersecurity solutions merely move the problem around, still present a broad attack surface for cybercriminals, and introduce cost and complexity to data security without eliminating the base problem. Existing solutions for securing data in flight have fundamental flaws:

- **Security:** Existing systems are kept secure by carefully guarding the keys. But adversaries know where the keys are, and these keys represent a Single Point of Failure in the security of the protected data.
- **Verifiability:** Existing solutions are designed such that the security of data cannot be verified. Instead, agencies must trust or hope that their key protection efforts have been effective when they know that counter examples exist.
- **Fragility:** With existing solutions, a breached key enables data breaches that cannot be detected until the next key rotation. But existing systems to rotate keys are slow, cumbersome and themselves prone to breach, so the present reality is that breaches are persistent.

- **Inflexibility:** Because existing systems are so vulnerable to key breaches, classified data is restricted to well protected endpoints. This limits agency's ability to put that data to use as they would rather not use it than lose it.

Static or Stored Keys are a Single Point of Failure

Encryption has been utilized for decades to secure sensitive financial data moving between parties. Modern encryption algorithms are extremely solid when properly deployed. But encryption works like a lock, and every lock needs a key. With software encryption 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 leaves them on machines long after their use, by default, adding to the attack surfaces adversaries can exploit. The organization is only one breach, misconfiguration, or leak away from losing the secrecy of their communications and data transfers.

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 at right:

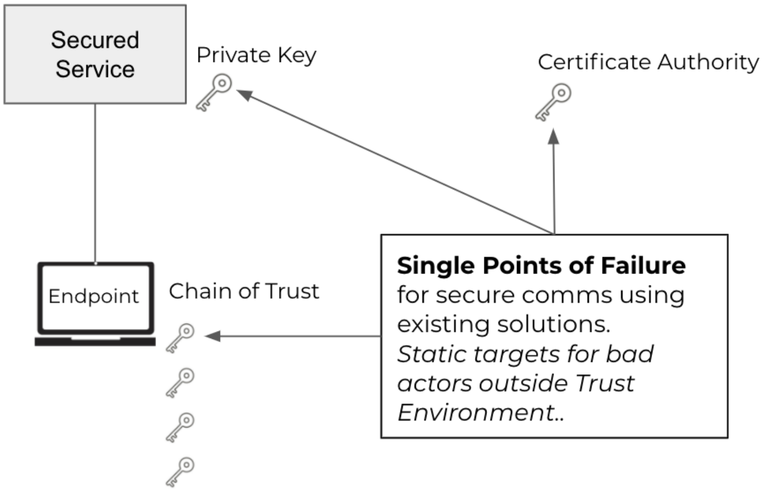


Figure 1. Single Points of Failure

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.

Credential Theft: If the existing security is to secure login to a site or application, the bad actor could observe the credentials being sent to the site and use these to their own benefit, resulting in financial and identity theft.

Current Zero Trust Solutions Do Not Solve the Problem

Zero Trust and Data Centric network solutions are being discussed, investigated, and slowly adopted across the financial sector. 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 same old method of securing the data in flight continues to provide a rich target environment for adversaries to exploit and gain access to that communication. Without eliminating this threat surface, no change in network configuration or access policies will protect data in flight from these attacks.

Solution Summary

The KnectIQ solution 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 a move to Zero Trust architectures with better than VPN security.

- **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.

- **Quantum Proof Cryptography:** This system has no public keys and no attack surface for quantum computing.

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 used 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 is possible, leading to real-time responses and minimal exposure when attacks occur. Finally, a crypto system built on identity can take Zero Trust architecture all the way to a cryptographic infrastructure that gives 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.

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 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

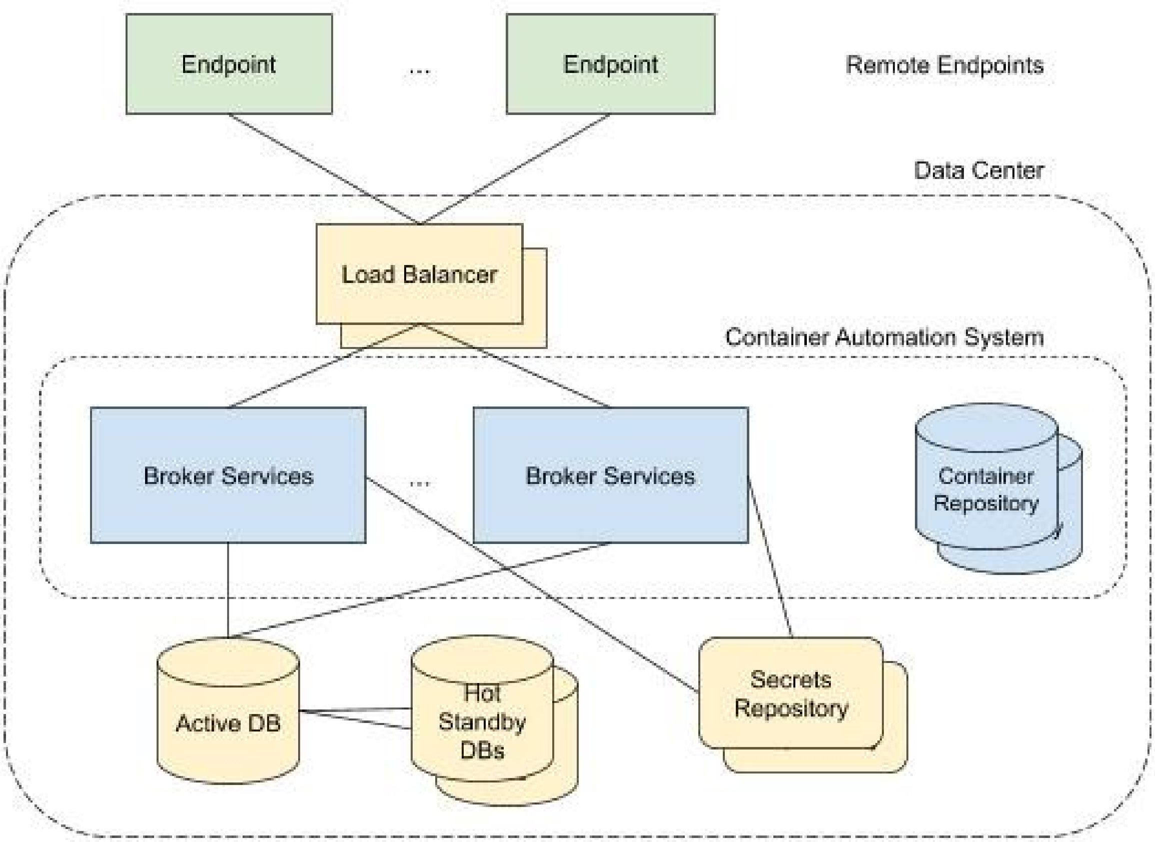
The broker manages the Trust Environment. Deployed on premises or in a private or government cloud, the broker enables configuration and operation of the Trust Environment. It does this by enabling the following operations:

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 level 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.

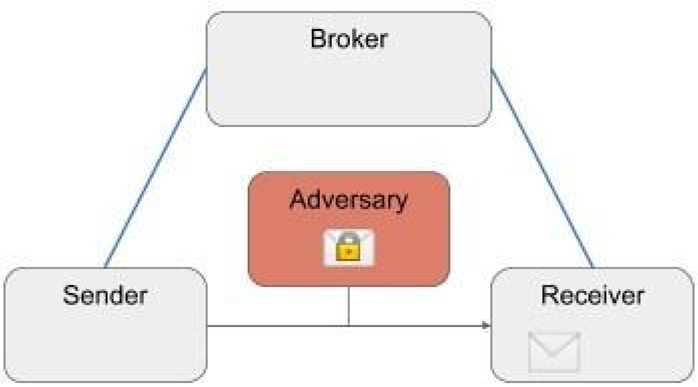
Device

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, but 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.

5. **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.

6. **Production:** The solution is deployed as an additional layer of security, leaving current solution in place. Once verified, obsolete means of protecting data in flight can be removed and cost savings realized.

SOLUTION APPLICATIONS

The system provides cutting edge data security solutions across the breadth of banking data flow sources and relationships.

Mobile apps (banking, payment, other):

Customer access through banking apps provides a rich environment for criminals to exploit. Many mobile applications in banking today attempt to prevent compromise of data in flight by employing certificate pinning where the Financial Institution effectively serves as its own Certificate Authority. While more secure than TLS or other off-the-shelf cyber security solutions, it does not play nice with DLP or other SSL Intercept solutions but more importantly still leaves one or more static keys as single points of failure in the solution.

Web portals (banking, payment, other):

No need to warn customers not to use public Wifi to access their accounts and information. KnectIQ can create ultra-secure pathways for customers by adding their devices to the Trust Environment and allowing safe access from anywhere.

APIs:

The security of banking partners connecting into a platform is only as secure as the weakest partner's security choices. KnectIQ can help banks give partners secure access to parts of their Trust Networks and in so doing enhance the protection and enable the monitoring of secure data transmissions.

Inter-branch/Interbank communications and data transfers:

Data moving between branches, branch to data center, or branch to corporate can be better protected with the elimination of static keys throughout the security systems deployed. The costs associated with monitoring and rotating the static keys can also be recovered.

Remote employee access:

To successfully navigate the work practices forced upon the industry by COVID or simply to allow the most flexible work options for its employees, banks can use KnectIQ to help secure communications and access from home for their employees with a higher level of security than VPNs and existing solutions provide.

Intellectual Property Details

KnectIQ's process is both patented and patent pending.

Patent Granted

Patent 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

Patent Pending

File Date: 28 Jan 2019
Application # 62/797,439

SYSTEM AND METHOD FOR SECURE ELECTRONIC DATA TRANSFER