KINDITE

Platform Whitepaper

Kindite provides a platform that eliminates all cloud-based data exposure risks by creating a zero-trust relationship with any cloud infrastructure. Our platform makes sure encryption keys never leave your domain while performing end-to-end encryption of data at rest, in transit and most importantly, in use. This document provides an overview of the platform's architecture, features and capabilities

Table of Contents

The Problem Kindite Aims to Solve

The bar of enterprise cloud maturity has been raised. Doubtful organizations now understand they have no choice and are rapidly increasing the use of cloud infrastructure. While the benefits of migrating enterprise workloads to cloud environments are well-known - elasticity, capacity, scale, and cost - it's also clear that this decision introduces some new heavyweight dilemmas.

Within the average organization endless entities (departments, users, devices) interact with multiple data points on a daily basis, every second. Following these interactions, data flows throughout the infrastructure - from the endpoint to the app logic, from app logic to database and from there to the disk level. When this happens within the organization trusted domain designated protection walls can be built around these interactions. But when data is outsourced to third-parties - such as cloud services - that need to perform computation on this data, there is a loss of control - and no walls can be built.

Cloud providers are nowadays investing great efforts in order to incorporate data protection solutions within their stack. However, as organizations engage with them, they have to take in mind the shared responsibility model. The model provides a security framework that dictates the obligations of the service provider and its users to ensure accountability. While looking into it one can observe that it doesn't matter which service model organizations choose (SaaS, PaaS or IaaS) data is always under the customer's responsibility and liability. This means that one can trust the infrastructure with factors such as functionality or availability - however protecting the data is always in the clients' hands.

Given the advances on data privacy regulations and the fast-paced accumulation of competitive and sensitive organizational information, the protection of workloads containing this type of information has become a key factor within the question of whether or not to expand the organization's cloud presence. Existing solutions offered for the cloud ecosystem include:

- **Protection of data at rest** - aims to secure static data when being stored in a database or other storage. Popular solutions within this category include disk or filesystem-level encryption, database encryption tools and cloud storage encryption services.
- **Protection of data in transit** - aims to secure data while being transported between two endpoints. Popular solutions within this category include Transport Layer Security (TLS).
- **Protection of encryption keys** - aims to secure the keys used for data encryption. Popular solutions within this category include Hardware Security Modules (HSM) and Cloud-based Key Management Systems.

These solutions do not cover all types of data within the full flow cycle, as data is not just static or in transit. Protecting data while it's being processed in real-time is a challenge that hasn't been fully resolved yet. Current technical limitations force encryption keys and plain-text data to be continuously accessed by the cloud infrastructure. In this case, organizations potentially expose themselves to the following threats:

1. Internal threats:
    - Internal attackers
    - Human error vulnerabilities
2. External threats:
    - External attackers
    - Third party access
    - Governmental interference

Creating a Zero trust cloud application environment

As we already based, organizations have no option but to give away some trust while they base their presence in the cloud. However trusting with sensitive data has the potential to enable the existence of alarming vulnerabilities and points of failure. Zero-trust is a term coined by Forrester that has been gaining ground along the concept of "*never trust, always verify*", as a way to gain control and increase security levels. A Zero-Trust security model enforces the idea that data flows need to be authenticated, verified and secured. Current Zero-trust offerings focus on the user and application levels, but in order to have a true zero-trust architecture one must follow and encrypt by the data level.

Kindite aims to fill this gap. In order to significantly reduce the attack surface it assembled a unique set of confidential computation technologies into a single data-protection platform, which makes sure data remains encrypted end-to-end at all times, even while being processed. Furthermore, Kindite's platform makes sure encryption keys are never available to the cloud, creating a true zero-trust relationship with any infrastructure.

While providing a pure client-side encryption, Kindite's platform maintains full business continuity, allowing the application logic to continue working while being fully transparent to end users. Kindite's "Collaborative encryption" utilizes a set of cryptographic algorithms allowing the regular search, update and data-level manipulations to be performed over the cipher without the need to decrypt it. Kindite's solution is seamlessly integrated with the target application without making any code changes to neither the application nor to its database.
The benefits of Kindite as a Zero-Trust Encryption solution are:

- **Full control of data:** Built on the basis of end-to-end encryption. Customers have control over private data even within cloud-based platforms. Data is only encrypted and decrypted at the end-point device.
- **Data protection, no matter where data resides:** Continuous encryption across the data lifecycle to flow safely. Even if data is intercepted, it will remain encrypted, therefore inaccessible.

- **Decoupling the data from the infrastructure:** The encrypted data can only be decrypted at the end-point device. This means the infrastructure is blind to the data while still being able to process eliminating all potential cross tenancy issues.

How it works

Two subsystems make up Kindite's unique architecture: the encryption subsystem and the key orchestration subsystem. The encryption subsystem is responsible for encrypting, decrypting and working with encrypted data. The key management subsystem is responsible for making keys ready-to-use for the encryption subsystem, in a secure and controlled fashion.

Encryption Subsystem

Kindite's solution is provided as a service, and supports target applications running on AWS, Azure or GCP. Two modules are involved as part of a Kindite deployment:

1. **Local Encryption Extension (LEX).** LEX is deployed on each endpoint which needs to store encrypted data or requires access to decrypted data. An endpoint can be an end-user on-premises machine or an application instance.
   - The LEX is responsible for:
     - Local encryption/decryption
     - Local (secure) Key Management and Key Storage
   - The LEX also provides an API for easier application-level integration.

2. **Database Module.** The database module is automatically deployed by Kindite between the application and its database. This module acts as an ODBC/JDBC bridge, intercepting all DB queries from the application while allowing standard operations to be performed over the encrypted data. Since this module is automatically deployed as a "bridge" between the application and the DB, it requires no code changes to the application server nor to the DB itself.

- Supports all data sources with an ODBC / JDBC / ADO.NET interface (between the application and DB)

- Requires configuration changes only:
  - Change the application's DB connection string to target the DB module instead of the original DB location

Features

- **Endpoint encryption-decryption** - our local module captures requests to and from the application server and encrypts and decrypts as required preventing from plain text data to leave the endpoint and from encryption keys to reside anywhere else.
- **No code changes** – Kindite's service does not require any application code changes.
- **Auto deploy of the Database module** - Automatically deployed by Kindite between the application and its DB, acting as an ODBC/JDBC bridge intercepting requests to the original cloud based DB.
- **Deploy once** - The LEX is deployed once on each endpoint regardless of the number of target applications.
- **Fully agnostic** – Kindite solution can be deployed on any cloud (focusing on Azure and AWS), and is able to protect any application and any type of database, provided the connection between the application and its database is ODBC, JDBC or ADO.NET.

Cryptographic Library and Algorithms

Kindite's patent-pending algorithms are based on widely-accepted published academic research and have been mathematically proven to pass the strictest cryptographic tests, including NIST standard test.

Under the hood, Kindite uses only modern, well known and widely spread industry-standard cryptographic libraries, compliant with NIST's FIPS 140-2 and PKCS#11, tested with NIST's standard tests and audited by world-renowned cryptographic experts.
Kindite utilizes only industry standards and government-approved set of cryptographic tools and algorithms, thus providing the highest grade of encryption available.

Key Orchestration Subsystem

Kindite offers a secure, straightforward, easy to use Key orchestration. Our subsystem allows a full Key life-cycle and reduces maintenance and administration overhead in basic day to day key management operations.

Key management and provisioning

Each user is provisioned with two sets of encryption keys:

1. Asymmetric Public Key Pair - This Key pair is generated for each managed device and is meant to securely identify the user against Kindite service as well as protect the per-application keys. This means
    a. This Key pair is generated automatically once the LEX is installed on the endpoint.
2. Unique Device Key - This set is comprised of two types of Keys:
    a. Read Key - used to decrypt data by the LEX. Decryption utilizes a unique cryptographic process which allows a unique identification process against Kindite's service, which allows easy key revocation and re-generation.
    b. Write Key - used to encrypt data by the LEX.

This means the secret never leaves the device, there are app-specific keys (protected by the secret) that are sent to the device and that are tied to the identity after the identity of the user is established.
All read keys can decrypt all data encrypted with all write keys, achieving true and secure collaboration over encrypted data.
On top of these Keys, each application has its own key, which is used to securely derive the Read/Write Keys for each user and managed device.
There are no manual processes involved in Key generation or provisioning, as all keys are encrypted using the user specific public key, and all communication channels are secure.

Features

- **Blind KMS** – The Key Orchestration subsystem stores only strongly-encrypted copies of data keys and has zero knowledge of how to decrypt them. The KO allows flexibility at scale while assuring key secrecy can't be accessed by cloud infrastructure, service providers and government or state officials, unless specific access is given by the organization
- **Automatic Key orchestration** – Keys are generated and transferred automatically.
- **Single click revocation** – With a click of a button you can revoke data-keys immediately eliminating the user's ability to read data without affecting other users.
- **Granular user-device-data access management** – Manage each user's access at different levels of data sensitivity on each application. Manage access to sensitive data from both managed and unmanaged devices.
- **Central management of key lifecycle** – Users and keys are managed through a dedicated admin console. Where users have full control over KO processes .
- **Key Rotation and Data Re-Encryption** – New data is encrypted and decrypted using the data encryption key derived from the previous active secret. Key rotation involves no additional record keeping of historic keys, as all read keys can decrypt all data encrypted with all write keys.

Securing data with Kindite's platform

Kindite's platform is based on a combination of strong, verifiable cryptography and multiple technological approaches in a way that enables contemporary end-to-end encryption. With our platform you can establish full control over your data and pave your way into a full zero trust architecture.

For more details visit:
www.kindite.com

Or contact us at:
info@kindite.com

KINDITE

Real Encryption. In use.

www.kindite.com | info@kindite.com | +1-(650)-727-9178