Security and Privacy Overview

Kiite is proud to provide enterprise-class security and data management services to businesses worldwide. Built on leading-edge infrastructure and technologies, Kiite is committed to keeping your confidential information as safe as possible.

Redundant Information Security

We handle sensitive information for organizations around the world. To do this, we employ multiple levels of data protection:

- We encrypt all data transmissions over 2048-bit SSL security
- Unique encryption keys are generated for each account and stored separate from customer data in an encrypted, secured secrets vault, making multiple account hacking almost impossible
- We use secondary in-database encryption for extra security

While it's common for Software-as-a-Service (SaaS) providers to provide SSL-security connections, the truth is that most compromises start after your data is in the hands of a service provider. We have taken a leadership role in protecting our customers' information, and as part of this commitment we separate all customer data. Everything Kiite learns about your company is encrypted uniquely and securely to your account, meaning that your company's critical business information is protected.

Proven Uptime and Disaster Prevention

We are committed to providing our customers with exceptional uptime and availability. You can trust that we are aligned with your availability expectations:

- 99.9% uptime service level commitment
- Fully redundant primary internet connections
- 24x7x365 Network Operations Centre (NOC)

Our Canadian-based enterprise-grade virtual private cloud has been constructed with true real-time redundancy. With live data synchronization, every application and database server has an active failover unit ready to take over in the event of a disaster.

Reinforcing this real-time failsafe, on a nightly basis, customer databases are backed up in full, ensuring backup processes do not disrupt access to customer data. Backups are shipped off-site to another secure Canadian location, ensuring that even in the event of a critical disaster, customer data is secure.

International Privacy & Security Standards

Privacy is part of our DNA. As part of our promise to you, we adhere to stringent international data management controls and policies to ensure 24x7 protection of your data.

European Union Data Protection Standards

Key for the transfer of personal data from European Union (EU) countries to third countries, is the adherence to privacy principles no less stringent than EU principles. As a Canadian company, we adhere to the Personal Information Protection and Electronic Documents Act (PIPEDA). Further to this participation, our service standards include authorized contractual clauses to govern the transfer of customer data.

Our Privacy Policy

Your privacy is important to us and to better protect your privacy we provide a public Privacy Policy1 explaining our online information practices and the choices you can make about the way your information is collected and used. To make this notice easy to find, we make it available on our homepage and at every point where personally identifiable information may be requested.

ISO 27001

Kiite is certified with ISO 27001, the world's leading standard for information security management. In addition to hosting information on AWS, Kiite has completed an independent third-party audit of its own management and data systems. This audit involves a rigorous review of our technology infrastructure and operational processes, and represents our commitment to customer security on an ongoing basis.

SOC 2

In accordance with the guidelines set by the American Institute of Certified Public Accounts(AICPA), the SOC 2 report provides Kiite users with confidence that our security, availability, and confidentiality controls to protect our customers' data has been audited by a qualified, third-party using an internationally recognized standard.

“We use only SOC 2 audited data centers to ensure our processes exceed industry best practices. ”

Operational Best Practices

Our customers enjoy security controls such as fully guarded premises and physical access management that are economically infeasible with typical in-house, on-premise deployments. Dedicated around-the-clock availability and security monitoring provide added layers of assurance.

- SOC 2 Audits
- Highly Restrictive Physical Access
- Audited Access Controls

We use only SOC 2 audited data centers to ensure our processes exceed industry best practices. The reports from these audits are available to our customers or auditors and are conducted in accordance with attestation standards established by the American Institute of Certified Public Accountants and International Standard on Assurance Engagements 3402.

To ensure application security trusted third-party scanners regularly audit and evaluate our services, verifying that we’re protected from malicious attacks.

Outside of core data operations, we designed our physical office to eliminate any central on-premises servers, ensuring employees and guests have no direct access to customer data. Our employees are unable to access customer data without explicit permission in the course of delivering support services. When requesting support, either at the time of request submission orduring the course of interaction with our team, customers have the opportunity to grant anynecessary access rights—all such grants are tracked.

Data Portability Commitment

Since its founding, Kiite has made data safety and portability a key principle. As a key part of this, our Data Portability Commitment is clear: you own your data, and you can take it with you at anytime. As much as we’d hate to lose you as a customer, we will never hold your data hostage. You can easily export your data in a common, SQL-compatible format, or make use of our various APIs to request data as needed.

Serious About Security

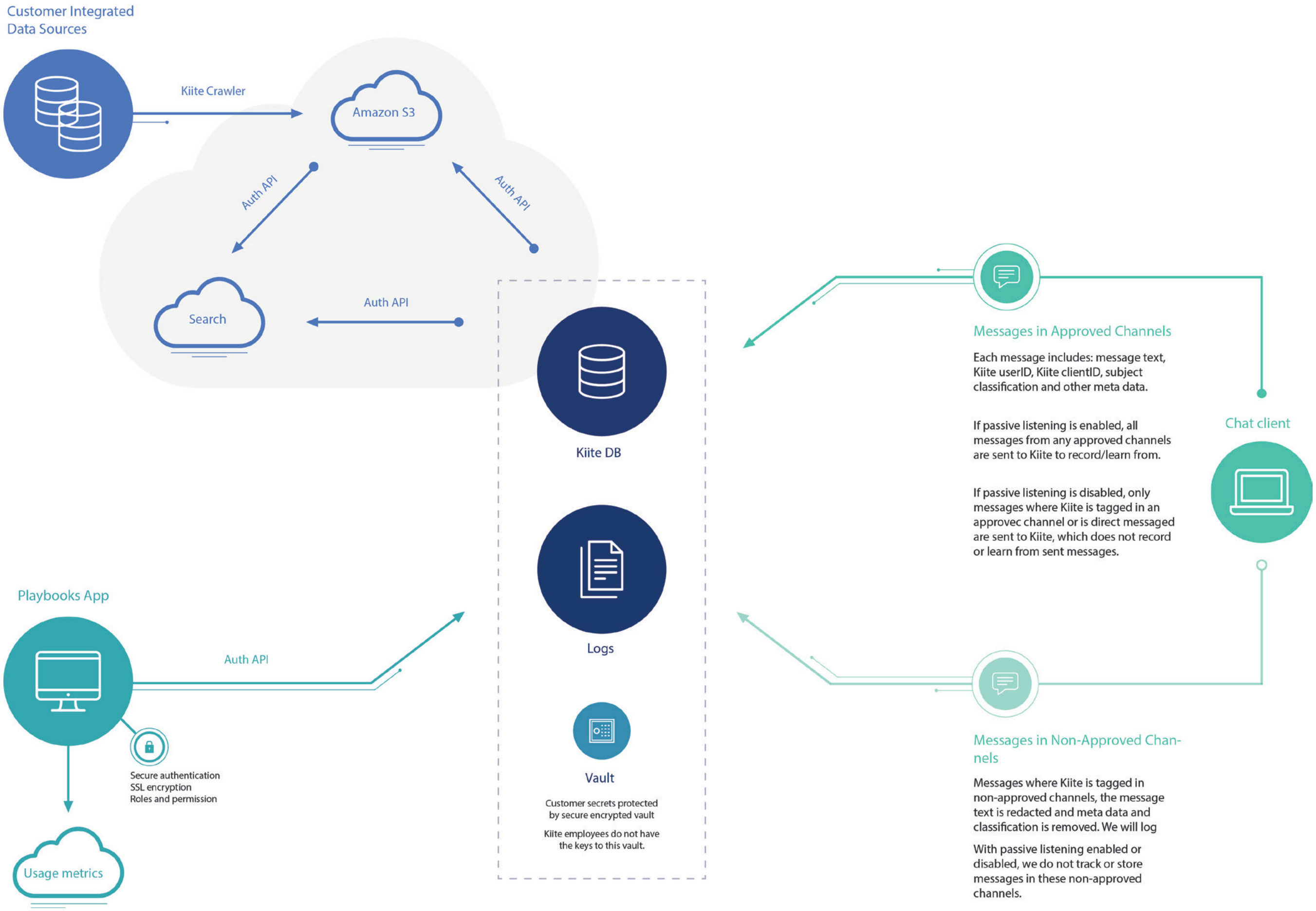
Our data centers are locked and guarded, and can only be accessed by authorized personnel. Monitored closed circuit television systems and onsite security teams vigilantly protect our datacenters around the clock, while military-grade pass card access and biometric finger scan units provide even further security. Enhancements include:

- Regulated Climate Control
- Redundant Power—Just in Case
- Fire Suppression
- 24x7 Support

Unlike some providers, we don't rely solely onnthe local power grid to guarantee around- the-clock power. Our onsite diesel-powered generators and uninterruptible power systems (UPS) deliver redundant power if a critical incident occurs, so that all operations are uninterrupted and your dedicated servers remain online. We regularly test our infrastructure to make sure it performs as designed in the event of an emergency. And we back it all up with our 99.9% Uptime SLA.

Security-First Architecture

We believe that the best defense is a defense-in-depth approach, and as such bake security best practices into our service at multiple levels. From at-rest and in-transit encryption, to secure vaults for secrets and authenticated APIs at each layer, we pride ourselves on ensuring the protection of all customer data.



Secure authentication
SSL encryption
Roles and permission

Customer secrets protected by secure encrypted vault

Kiite employees do not have the keys to this vault.

Messages in Approved Channels

Each message includes: message text, Kiite userID, Kiite clientID, subject classification and other meta data.

If passive listening is enabled, all messages from any approved channels are sent to Kiite to record/learn from.

If passive listening is disabled, only messages where Kiite is tagged in an approvec channel or is direct messaged are sent to Kiite, which does not record or learn from sent messages.

Messages in Non-Approved Channels

Messages where Kiite is tagged in non-approved channels, the message text is redacted and meta data and classification is removed. We will log

With passive listening enabled or disabled, we do not track or store messages in these non-approved channels.