Security and Compliance Handbook

Introducing IntegrateCloud

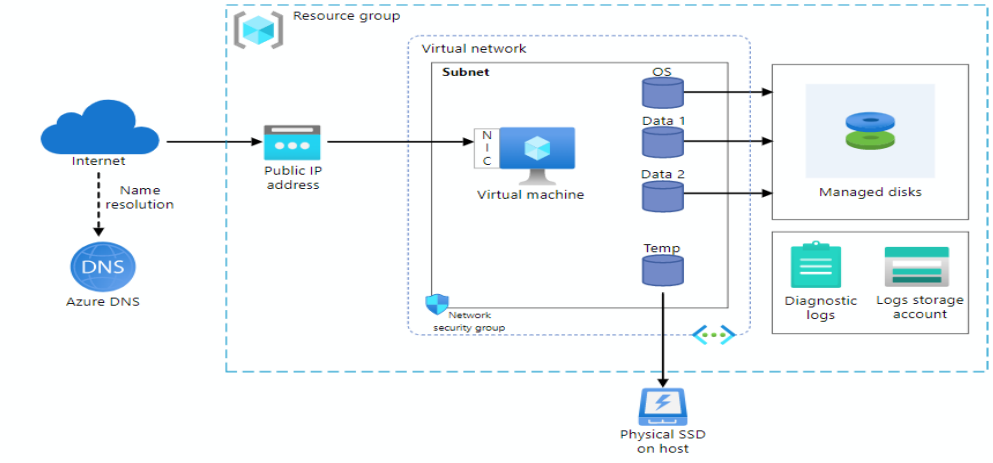
IntegrateCloud is a SaaS Integration tool that enables teams to streamline communication any cloud based and/or on-premise systems at scale. It turns into a flexible communication mechanism where organizations can easily connect their cloud based and/or on-premise systems to make the easily communication between customer support and engineer teams. Today, over 500 customers trust IntegrateCloud to seamlessly connect their cloud based and/or on-premise systems.

IntegrateCloud's Commitment to Security

As an organization, IntegrateCloud strives to build a secure application in accordance with security best practices to uphold the confidentiality, integrity, and availability of our customers' data. In the spirit of transparency, this document describes the systems and security practices we have in place to protect your sensitive data.

Enterprise Architecture

- Hosted on Microsoft Azure Cloud Services, designed to provide 99.99% availability, with services hosted regionally from the US and the EU.
- Content Server is hosted on Microsoft Azure Virtual Machine Cloud Services and Metadata Server is built on Microsoft Azure SQL Database.
- All systems and services are equipped with integrated failover and fault tolerance with multiple availability zones for redundancy.
- Built with a distributed architecture, where all services are contained within a protected VPC environment using individual security groups and Microsoft Azure Blob Storage.



Microsoft Azure

Security Controls

- All business systems follow the principle of least privilege.
- Sensitive administrative actions trigger notifications, which are reviewed in real time and are written to an immutable log.
- All production systems require VPN and multi-factor authentication.
- Application source code is stored in a secure environment and changes go through a peer review process.
- IntegrateCloud has dedicated staging environments for development and testing, separate from production.
- All company-owned assets are encrypted and have MDM technology installed, allowing IntegrateCloud IT admins to remotely wipe devices

Data Privacy

- All data in transit is secured with TLS 1.2 encryption and data at rest is secured through RDS and S3 services using AES 256-bit encryption.
- All API and client communication (desktop, web, and mobile) require HTTPS connections.
- All customer data is logically separated and tied to an enterprise ID that is used to validate requests during data retrieval processes.
- IntegrateCloud has security monitoring technology in place to detect system anomalies.
- Customers can dictate which geographic location (United States or European Economic Area) to host their data.
- IntegrateCloud has a Data Processing Addendum that is incorporated in our SaaS agreement

Compliance

- IntegrateCloud uses Microsoft Azure which have SOC 2 Type 2 compliant.
- IntegrateCloud adheres to the EU/US and EU/Switzerland Privacy Shield framework and is compliant with GDPR and CCPA.

Governance

- All employees go through background checks prior to employment.
- All employees undergo general security training and testing as part of IntegrateCloud's standard onboarding process.
- Engineers go through an annual security developer training.
- IntegrateCloud handles sensitive data through our mature information security management system to minimize risk and combat security breaches.
- IntegrateCloud has a defined information security response program to detect and respond to incidents, recover service, and maintain business continuity in the event of a disaster.

Enterprise Application Security

IntegrateCloud was designed to create a secure and collaborative experience for companies and their teams. To ensure IntegrateCloud can be deployed in compliance with the security needs of your organization, we've developed a suite of security features, some of which are highlighted below.

❖ Multi-Factor Authentication

Individuals and administrators can enable two-factor authentication, which adds an extra layer of security to their IntegrateCloud account. to their IntegrateCloud account. Authentication apps need to support "TOTP algorithm."

❖ Single Sign-On

IntegrateCloud's administrators can enable single sign-on (SSO) using any SAML-based identity provider (IdP) like Okta, Google, OneLogin, Microsoft Azure Active Directory.

❖ IP Restrictions

Company administrators can allow list the IP addresses from which their employees can access IntegrateCloud.

❖ Roles & Permissions

Administrators can define user roles with a customized set of permissions, like allowing certain users to create rules or restricting them from responding to messages.

❖ Delegated Inboxes

A IntegrateCloud user can delegate their individual workspace to another team mate, enabling them to manage their teammate's work queue without having to share login credentials.

❖ Admin Access Controls

IntegrateCloud's admin console provides administrators access to manage teammate settings like signatures and preferences, giving them heightened control over each user's workspace.

Frequently Asked Questions

Does IntegrateCloud retain a copy of my communication data?

No, IntegrateCloud just do the transmission of data between systems by using a Rest API’s.

Can I request IntegrateCloud to delete my data?

In compliance with GDPR, IntegrateCloud will delete any company’s data once an explicit request is submitted and the requester’s identification is properly validated. All deletion requests will be completed promptly, but metadata can take up to 10 days to be purged from backups

What types of personal data does IntegrateCloud store?

IntegrateCloud store only the respective ticket ids of both instances and Personal Access Tokens (PAT). Other than that, we just do the transmission of data between systems by using an API's