Workato Security

White Paper

Feb 2017

Introduction

Anytime data is moved into the cloud or through cloud-based applications or services, there are legitimate concerns around security, reliability, and privacy. Cloud-based systems are outside the direct control of IT departments, and under the management of a vendor's hosted environment. It is essential to ensure that cloud systems are at least as strongly secured as would be an application in a well-managed private cloud or internal IT environment.

Integration platforms may have extra challenges in this area. Not only is there the security of the platform to consider--the integration application itself--but also the data that passes through the integration system, which is typically sourced from many different applications.

Workato is committed to providing a highly secure and reliable integration service using proven, tested, best-in-class technologies, practices and procedures.

Requirements in this area include:

- Access control: restricting, monitoring and controlling access to the system, so that only legitimate users have access and and have privileges that accord with their business role.
- Network security: data should be protected in transit, including data flowing through the integration environment itself as well as from there to any business applications it accesses.
- Data protection and privacy: data should be protected at rest. Any data stored within the system should be protected (using encryption).
- Isolation: In a multi-tenant environment, it is essential to guard against any leakage of data from one user or organization to another. Each user's data should be private and visible only to that user or to another authorized party such as an administrator.
- Monitoring and management of the overall system. Visibility into usage of the system and the ability to adjust user permissions, monitor activity, and assess performance.
- Physical security of the hosting environment.
- Commitment of the vendor to auditing, testing and certification to industry standards.

Security also encompasses high availability and resilience to software or system failures, and assurance that the software system and underlying business operations are prepared for disaster recovery.

The following sections detail Workato's comprehensive approach to these concerns.

Security and Privacy

Authentication

Workato uses an industry standard strong hashing mechanism for passwords. Hashing enables login without the application ever having to store any user's in-clear password. Password guessing attempts are foiled because the hashing process deliberately takes some time, so that no one can rapidly try a large number of passwords. In addition Workato enforces a password policy that prevents overly short or simple passwords.

Besides password login based on Workato credentials, Workato also supports Single Sign-On with popular applications including Google, Salesforce, Slack, Intuit and InfusionSoft. SAML support is planned.

User privileges

Users within the Workato system do not have any privileged access to applications, but must supply their application credentials in order to connect.

Finer grained control over a user's access to features of the Workato system is available through the administration console.

Auditing and logging

All user activity within the system and all application interactions are logged.

Network Security

Workato services are accessible only over HTTPS or SSH (for administration). Traffic over these protocols is encrypted and is protected from interception by unauthorized third parties. Workato uses industry best practices for network security and only permits interactions using strong encryption algorithms, with a key length of at least 128 bits.

All access to applications from the Workato platform is only over secure protocols (typically HTTPS).

Access to on-premise applications is managed through a secure gateway hosted by Workato and an on-premise agent installed at the application site. The application initiates connection to the integration server and this is done through a TLS encrypted link. Client certificate authentication is used to establish the link.

Access to databases used in the Workato service is over an encrypted link (TLS).

All network access, both within the datacenter and between the datacenter and outside services, is restricted by firewall and routing rules. Network access is logged and logs are retained for a minimum of 30 days.

Data Protection

Data “at rest” in the Workato databases is encrypted. This is done as part of a “defense in depth” strategy. Securing network links and restricting access to authenticated users should prevent any unauthorized access to stored data. Nevertheless, encryption adds an extra layer of protection against unauthorized access.

When Workato recipes connect to remote systems using user-supplied credentials, where possible this is done using OAuth, and in those cases, no credentials need to be stored in the Workato system. However, if a remote system requires credentials to be stored, they are encrypted using a standard strong encryption method (aes-256-cbc).

Data Isolation and Privacy

Workato servers run in Linux virtual machines which are isolated from one another and from the underlying hardware layer. Server processes are restricted to a particular directory and do not have access to the local filesystem.

While users of the Workato platform share some common infrastructure, a strong layer of privacy is enforced across users. One user cannot see another user’s application data. And when recipes are shared, any sensitive data, including login details, is stripped out before another user is given access to a shared recipe.

Workato has a privacy policy, which further details the steps we take to protect clients’ information.

Hosting and Physical Security

Workato provided services including deployed recipes are hosted in physically secure data centers managed by Amazon. These provide 24/7 access control and monitoring. Amazon’s hosting environment and software services have met numerous US and international certification requirements related to privacy and security.

Workato’s hosting environment regularly updates its underlying software to protect against vulnerabilities.

Auditing, Testing and Certification

Workato has achieved SOC 2 Level 1 compliance for its cloud-based services. This involves a comprehensive examination of security and privacy practices, as well as the reliability and availability of the service. The Workato cloud application has also undergone other external security audits, for example as part of Salesforce and Intuit app certifications. And there is internal testing and vulnerability analysis by the development team, on an ongoing basis, as well as periodic penetration tests performed by a qualified 3rd party firm.

Workato is also planning to adopt the Standard Contractual Clauses (also referred to as “Model Clauses” or “Model Contracts”) approved by the European Commission to secure European users’ legal privacy rights.

Governance and Policy Management

When multiple users within an organization are accessing the Workato platform for integration, it is important for IT and management to have an overall view of the activity. Workato supports a management console (Workato Aegis) to provide this view. It is possible to monitor the applications that are being accessed through Workato across multiple users, inspect the data, and see a history of activity including any errors or exceptions.

Workato Aegis is designed to be flexible, so that business users can perform self-service functions while still allowing IT to have visibility into their operations. Or business integrations can be delegated to IT to manage.

In addition the console provides control over the permissions granted to individual users, which can be finely controlled through Access Control Lists (ACLs)..

High Availability and Disaster Recovery

Part of security is maintaining uninterrupted availability of the service. Workato has an architecture which is designed to maintain high throughput while eliminating single points of failure.

Database

Workato databases are hosted and managed by Heroku (the same infrastructure that runs Salesforce) in a high availability configuration with continuously synchronized hot standby instances, distributed across hosting regions. If for any reason one database instance should become unavailable, there is automatic failover to a standby. The maximum data loss for the database is 160MB of data, or 10 minutes, whichever is less (this is a worst case). Recovery time is typically 10 minutes or less.

Storage

Workato also relies on Google Cloud Storage, a highly scalable, reliable and redundant storage service.

Application Services

The Workato runtime does not impose any design limit on total data volume or number of transactions. Workato can handle very large data volumes as well as million of trigger events per day.

As events are received from business systems, they are processed in a distributed event queuing system. This ensures that all events are eventually delivered and none will be processed twice. Because the queue can temporarily store more data than is being processed, this system also provides the ability to handle bursts of traffic.

To process application data, the Workato runtime system uses a pool of workers. Events are generated in the system either by polling or by asynchronous event triggers (webhooks). Polling is done by a variable size but always redundant pool of worker processes. Should one or more individual workers become unavailable, there is no interruption of service: processing continues using the remaining workers.

The Workato system is continuously monitored. A public webpage status.workato.com shows current status.

Disaster Recovery

Workato as part of SOC 2 certification has implemented a Business Continuity and Disaster Recovery Program. This encompasses not just the IT assets which host the Workato integration service, but all other aspects of Workato's business operations. The plan is subject to at least annual review and update.