A JITTERBIT WHITEPAPER

Security and Architecture

Table of Contents

Jitterbit

Introduction

Jitterbit delivers powerful integration tools and services through a multi-tenant cloud integration platform called Jitterbit Harmony.

While Jitterbit Harmony can drastically simplify and speed up most aspects of managing integration processes, the introduction of a multi-tenant cloud system can raise security questions for customers and users.

Jitterbit Harmony manages information security by applying an information security framework (hybrid model) based on NIST, CIS, CSA, and CERT recommendations. Jitterbit has also been certified to meet the requirements of:

- Health Insurance Portability and Accountability Act (HIPAA)
- SOC1 and SOC2 type 2 compliance
- ISO 27001:2013 with supplemental controls for 27017
- California Consumer Privacy Act (CCPA)
- European Union - General Data Protection Regulation (GDPR)

This document describes the following aspects of security provided by the Jitterbit Harmony platform:

- Logical Security and Architecture
- Physical Security
- Organizational Security

This document takes a broad view of security and covers things to consider from the perspective of availability and performance, in addition to data protection.

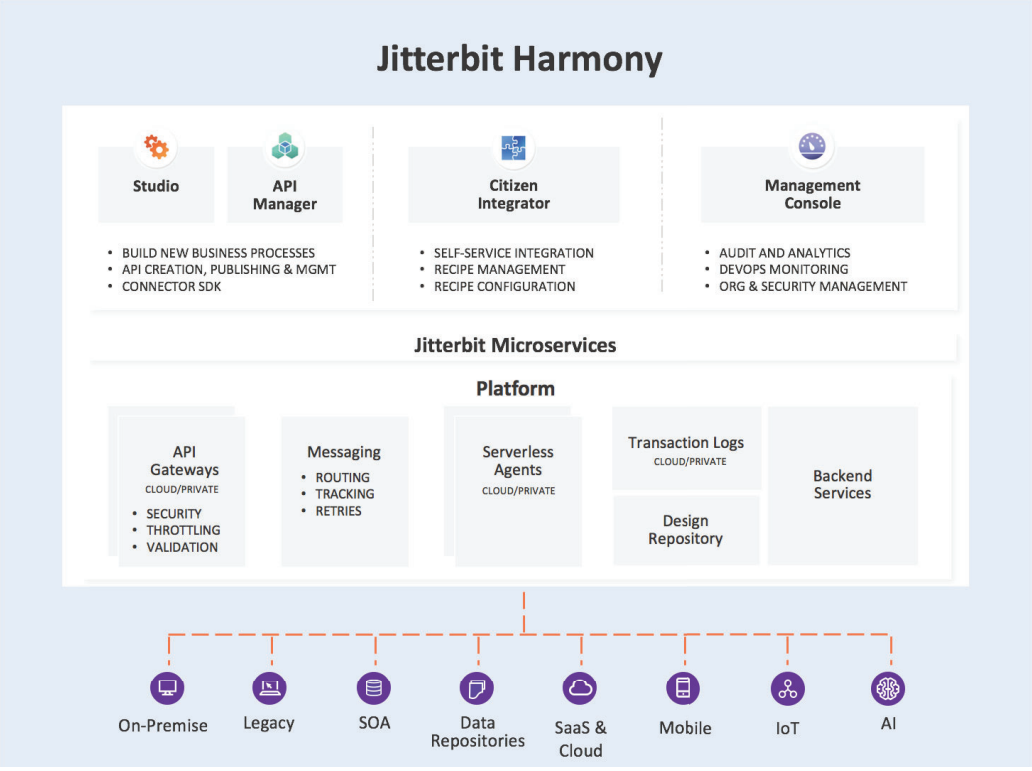
JITTERBIT CONFIDENTIAL | FOR INTERNAL USE ONLY | COPYRIGHT © 1998 - 2020 JITTERBIT, INC.

Logical Security and Architecture

Logical security is comprised of all the security measures taken within the Jitterbit Harmony software. This section describes the following:

- System Architecture
- Major Components
- Harmony Users, Organizations, and Roles
- Harmony Environments and Access Control
- Harmony Data Storage
- Harmony Security Topologies

System Architecture



JITTERBIT CONFIDENTIAL | FOR INTERNAL USE ONLY | COPYRIGHT © 1998 - 2020 JITTERBIT, INC.

Jitterbit enables users to design, test, deploy, run, and manage their Jitterbit integration projects. Using Jitterbit Harmony, customers can run their Jitterbit integration processes completely in the cloud without the need to procure or manage any software or the infrastructure required to operate it. Those who choose to deploy Jitterbit Harmony platform either on-premises or in a hybrid mode have the flexibility to run their integration processes by deploying private agents behind the firewall, thereby obtaining greater control on where their data flows.

Jitterbit recognizes that customers have a need for their integration processes to communicate with applications that operate behind corporate firewalls for various security and regulatory compliance reasons.

Jitterbit Harmony's system architecture caters to both scenarios: integration processes can run completely in the cloud or can run behind corporate firewalls to ensure that business data does not get exposed to the cloud. Users can also employ hybrid models where some integrations run in the cloud such as development and others for example in production can run behind corporate firewalls.

While the system simplifies the provisioning, deployment, and management of integration projects it also offers users the flexibility to run their integration operations using detachable Private Agent Groups. These are self-contained subsystems that can be installed behind corporate firewalls or on dedicated private clouds.

The separation of integration designs, which are stored on Jitterbit Harmony, from integration runtime that occurs on Agent Groups, enables customers to control access and flow of sensitive business data.

Major Components

The various major components of the Harmony system architecture, and how they address security requirements, are described below.

Harmony Cloud Platform

Jitterbit Harmony includes multi-tenant databases, files, services, and a service-messaging infrastructure that are used to deploy, manage, and run integration projects. Jitterbit Harmony runs on Amazon Web Services (AWS). AWS provides a best-in-class, secure hosting platform that excels at providing core services to Jitterbit, such as:

- Data center security
- Compliance

JITTERBIT CONFIDENTIAL | FOR INTERNAL USE ONLY | COPYRIGHT © 1998 - 2020 JITTERBIT, INC.

- Physical security
- Environmental security
- Network security
- Host hardening
- High availability
- Fault tolerance
- Disaster recovery

Jitterbit develops and improves its applications by using sound software-development lifecycle (SDLC) practices such as:

- **Identifying vulnerabilities** from outside sources to drive change and code improvement.
- **Applying hardware and software patches.** Jitterbit is responsible for code changes and Amazon Web Services (AWS) is responsible for providing hardware patches; our virtual environment allows us to apply changes without any downtime.
- **Providing secure authentication and logging capabilities.**
- **Removing development accounts, IDs, and passwords** from production environments.
- **Adhering to strict change management practices** for code updates as well as patches.
- **Separating test and development environments** from production.
- **Maintaining separation of** duties between development and support staff.
- **Ensuring that Personal Identifiable Information (PII) is not used** in test environments.
- **Removing test and development IDs** before migrating code to production.
- **Performing regular code review.**
- **Documenting code changes.**
- **Engaging senior developer input and approval** for all code changes.

JITTERBIT CONFIDENTIAL | FOR INTERNAL USE ONLY | COPYRIGHT © 1998 - 2020 JITTERBIT, INC.

- **Completing functionality and regression testing** before release to production.
- **Maintaining backout procedures** to preserve high availability and integrity.
- **Following secure coding practices** according to an SDLC policy and addressing the security training needs for the development team.
- **Checking for security flaws as prescribed by the Open Web Application Security Project (OWASP)**, such as injection flaws, buffer overflows, cryptographic errors, error handling, etc.
- **Assessing for vulnerabilities on every release.**
- **Conducting annual penetration testing.**

Before a user can start their work, they must authenticate with Jitterbit Harmony using their Jitterbit Harmony user account credentials; password strength, complexity and attributes, such as two-factor authentication, are customizable so that customers can match the requirements of their security policy. When single sign-on (SSO) is enabled, these requirements are instead managed by the Identity Provider. All communication with Jitterbit Harmony occurs over HTTPS (greater than TLS1.2).

Once authenticated, Jitterbit Harmony identifies all the organizations and environments that this user has access to. Jitterbit Harmony provides the user with a list of the integration assets they can work on and allows the user to create a new project in any environment where they have sufficient privileges. Privileges are role-based and selectable/configurable per environment per organization. Common roles include Administrator, User, and Read Only.

Design Repository

Jitterbit Harmony stores all projects deployed in a multi-tenant design repository. Jitterbit backs up these projects and the system nightly. All backups are encrypted with a Federal Information Processing Standard (FIPS 140-2) algorithm. This project repository is built on a multi-tenant database architecture, which provides logical partitioning of projects by organization and, in most instances, by environment. Specifically, Harmony isolates and secures customer projects by:

- **Secure database architecture** — Includes separated database and separated schema architecture.

JITTERBIT CONFIDENTIAL | FOR INTERNAL USE ONLY | COPYRIGHT © 1998 - 2020 JITTERBIT, INC.

- **Secure connections or tables** — Uses trusted database connections.
- **Encryption** — Obscures critical data so that data remains inaccessible to unauthorized parties even if they come into possession of it.
- **Filtering** — Uses an intermediary layer between a tenant and a data source that acts like a sieve, making it appear to the tenant as though its data is the only data in the database.
- **Access control lists** — Determines who can access data in the application and what they can do with it.

Projects typically contain credentials such as username and password used to connect to various endpoints. This information is encrypted within the multi-tenant repository.

The repository is replicated across two regions. Each database is also backed up and can be restored, if needed, by the Jitterbit Operations team.

Customers do not have any direct access to this repository. The various Jitterbit Harmony platform components, such as the Studio and Cloud Agents, use APIs to access the repository. Once authenticated and access control is validated, all communication with the repository is done through various API layers. In addition to controlling edge API access via HTTPS and server-side sessions, APIs must validate user access control through environment-based and Role-Based Access Control (RBAC) lists. These lists ensure that users can only view, act upon, and change the system based on the permissions granted by their organization's administrator. In addition, audit trail granularity is configurable per customer.

The Jitterbit Harmony rotating activity database stores runtime status information as well as logs of running operations of all Jitterbit users.

The activity database is built on a multi-tenant architecture, and while activity data for all users resides in the same database, there is logical segmentation by organization and environment applied through a software access control layer and unique encryption keys to ensure that users can view only the activities that they have access to.

The activity database is replicated across AWS Regions and Availability Zones to ensure high availability and is backed up if there is a need for it to be restored.

Access to the activity database is provided by a set of APIs. The activity log uses similar APIs and access control list (ACL) infrastructure as the project repository.

JITTERBIT CONFIDENTIAL | FOR INTERNAL USE ONLY | COPYRIGHT © 1998 - 2020 JITTERBIT, INC.

File Services

Jitterbit Harmony includes a set of file services used to store files, such as schemas, and customizations. All files are stored in AWS S3 service and can be accessed only through Jitterbit Harmony's software and cannot be accessed directly.

Schema Repository

To support integrations from a variety of endpoints, Jitterbit Harmony stores various types of schemas, such as WSDL, XSD, JTR, and DTDs.

Customizations Repository

To support integrations from a variety of database endpoints, Jitterbit Harmony stores various JDBC and ODBC drivers. Jitterbit also provides a framework where customers can customize the Jitterbit operations using plugins.

Certified secure plugins are available on Cloud Agents. For customers that run Private Agents, customers can use customer-created plugins to achieve efficient, plug-and-play environments. In this private security model, customers are responsible for applying reasonable administrative and technical controls for the plugins they create for their private agent(s).

Harmony Studio

The Jitterbit Harmony Studio exposes the richest set of functionalities for creating, configuring, and testing Jitterbit integration projects. Jitterbit Harmony Studio is available in two versions:

- **Design Studio:** Design Studio is a standalone thick client that can be installed on a Windows or Mac workstation. It requires access to the Internet on the workstation or laptop that it runs on. Communication through corporate proxy servers is fully supported, as well as IP whitelisting to ensure corporate VPN adherence if or when required.
- **Cloud Studio:** Cloud Studio provides a platform- and location-independent browser-based design experience. Supporting the current versions of Chrome, Firefox, Safari. and Edge browsers, and using a modern technology stack, Cloud Studio integrates seamlessly with the Harmony platform for true cloud-based design, deployment, and monitoring of integrations.

JITTERBIT CONFIDENTIAL | FOR INTERNAL USE ONLY | COPYRIGHT © 1998 - 2020 JITTERBIT, INC.

Design Studio and Cloud Studio leverage Jitterbit Harmony security features including single sign-on (SSO) and user roles and permissions. Both products use the Harmony Cloud, running on the same platform with the capability to manage the same projects.

Cloud Agent Group

Harmony Cloud Agents are services, known as Backend as a Service (BaaS), designed to process and service client needs on an ad-hoc basis. They perform all of their work in an event-driven fashion, thereby eliminating the need for any setup, configuration, or management traditional with "always-on" server systems that sit behind applications.

Jitterbit provides its customers the option to run all their integrations in the cloud by providing a scalable, fault-tolerant, clustered Agent Group fully maintained and managed by Jitterbit.

To enhance security and protect privacy, Jitterbit Cloud Agents are coded to ensure that locally processed data is not persistent; it is used for the minimal time necessary to complete the intended process, then purged.

When the Jitterbit Cloud Agent Group performs an integration, it will directly connect with the application that requires data integration. It will then read and post data to these applications. Customers can also choose to persist their business data in temporary files for speed and efficiency especially when processing bulk data.

Data persisted in the Jitterbit Cloud Agent Group is stored in encrypted Amazon S3 buckets that are only accessible to the agent group. Each integration stores data in its environment's bucket.

For customers that need applications to reside within their firewall, or for users that perform integrations under strict regulatory compliance that forbids data to either travel outside a given geographical boundary or reside in the cloud, Jitterbit recommends using a Private Agent Group.

Private Agents and Private Agent Group

Jitterbit provides the flexibility for customers to provision and manage their own Agent Groups and Private Agents (formerly known as Local Agents) within their corporate firewall or virtual private clouds. This allows customers to choose where their integration runtime environment operates and lets them control which

JITTERBIT CONFIDENTIAL | FOR INTERNAL USE ONLY | COPYRIGHT © 1998 - 2020 JITTERBIT, INC.

network their business data travels and resides in. By using Private Agent Groups for integrations, companies can ensure that their sensitive business data never flows through the Jitterbit Harmony platform.

Jitterbit Harmony Agents belonging to Private Agent Groups authenticate and communicate with Jitterbit Harmony over HTTPS. Private Agent Groups deployed behind corporate firewalls can be configured to communicate via a corporate proxy server. There are no additional networking requirements, such as opening ports within corporate firewalls.

Private Agent code is created with the same coding rigor as Harmony code.

While Private Agent Groups cater for stringent security requirements, the user or customer is responsible for installing and managing their Private Agents. In the Cloud Agent Group, Jitterbit Harmony provides out-of-the-box high availability and scalability on-par with what is expected from a serverless technology. However, in Private Agent Groups, the security and scalability for Private Agents is a customer responsibility (although high availability is still ensured by the Jitterbit platform whenever more than one agent is used within a Private Agent Group). Jitterbit provides some best practice advice for hosting Private Agent code in System Requirements for Private Agents.

Runtime Messaging Services

Communication among various Jitterbit components, such as the Jitterbit Harmony Studio, Serverless Agents, and Jitterbit Harmony, is achieved by using a set of secure runtime messaging services based on the Java Messaging Services (JMS) API included in the Java Platform. These APIs are internal to Jitterbit components, and customers do not have any access to these APIs.

The Jitterbit Serverless Agents include listeners to the JMS messaging service. All agents that listen for requests strongly authenticate and are provided an authorized session in the Jitterbit Harmony messaging network. They can only listen to requests for their particular Agent Groups or that are made to them directly via Jitterbit Harmony. Messages are never sent to agents; agents always pick them up over HTTPS. This enables agents to run behind corporate firewalls and to remain protected without the need for opening ports that would allow incoming traffic from the Internet.

JITTERBIT CONFIDENTIAL | FOR INTERNAL USE ONLY | COPYRIGHT © 1998 - 2020 JITTERBIT, INC.

Harmony Management Console

The Jitterbit Harmony Management Console communicates with Jitterbit Harmony through a well-defined set of management APIs. APIs are created using the same secure coding rigor as Harmony itself, as described above in the **Harmony Studio** section. All users of these APIs must be authenticated with Jitterbit Harmony and all communication is transmitted securely over HTTPS.

All the management functions provided via the Management Console are further controlled by an access control layer model defined for each environment. As a result, any user using the Management Console will be able to see only the data for which they have access permission. Access controls are applied to any and all functions, including searching for operations, running operations, viewing logs, etc.

Data Loader

Jitterbit Harmony Data Loader is a free product within the Salesforce AppExchange that provides useful integration features targeted toward Salesforce customers. Data Loader allows customers to move data in and out of Salesforce to flat files or databases. The Data Loader product is coded with the same coding rigor as Harmony.

The Data Loader installs a custom Private Agent on the same machine where the Data Loader client is installed. For every environment one Private Agent is installed. Data Loader is not meant for scalable, highly available projects; rather, it is intended for desktop/laptop users.

Data Loader has been deployed in a production version of Jitterbit Harmony since the summer of 2013. It has been adopted by thousands of users and has been used to test the security, scalability, and availability of Jitterbit Harmony.

Harmony Users, Organizations, and Roles

In order to access Jitterbit Harmony, a user must register their user account. Every Jitterbit Harmony user created within Jitterbit Harmony has their own personal, role-based account and login credentials where personal integration tools and projects are stored securely.

In addition, every organization has a role called Administrator that can access all assets belonging to that organization. Administrators can add new roles to the organizations and invite other Jitterbit Harmony users to join when they need to work in teams to design, build, test, and manage their integration projects.

For more information on authentication, see the **Harmony Studio** section.

JITTERBIT CONFIDENTIAL | FOR INTERNAL USE ONLY | COPYRIGHT © 1998 - 2020 JITTERBIT, INC.

Harmony Environments and Access Control

All projects deployed to Jitterbit Harmony are deployed to environments. Environments represent a given state of an integration project. Many projects exist in various stages within different environments (e.g., a common project lifecycle configuration might have three environments: development, test, and production.) A project can exist in different states within each environment.

Organization Administrators manage access to each environment using a role-based access strategy. For example, users in the developer role may have read, execute and write privileges in the development environment, but only read access to the test environment and no access to the production environment.

The access levels for an environment include:

- **View Logs** — Allows a user to view logs under a particular environment but provides no visibility nor control over projects under it. This can be used to allow users to fully support but not affect projects deployed to critical environments such as production.
- **Agent Install** — Allows a user to install agents but provides neither control nor visibility outside of this function. This can be used to allow Administrators within and outside the company to establish additional connectivity without any impact to the projects or even knowledge of the platform.
- **Read Access** — Allows a user to read a project from a given environment. This can be used to share project templates with various users or to allow them to view but not affect projects.
- **Execute Access** — Provides read access and allows users to run operations within a given environment. This is a common access control for test environments and is often granted to users who need to support an integration as they will need to both test and run/execute tasks ad-hoc.
- **Write Access** — Allows full control to a given environment. Users belonging to a role with write access can read, test, run, and change projects within that particular environment.

JITTERBIT CONFIDENTIAL | FOR INTERNAL USE ONLY | COPYRIGHT © 1998 - 2020 JITTERBIT, INC.

Harmony Data Storage

The following describes the type of information stored in Jitterbit Harmony:

User Data

When a user registers and subscribes to Jitterbit Harmony they must provide the following information, which is stored in the project repository: first name, last name, email, and phone number. Company, company address, and company website can be provided but are optional.

Project Data

In order to run and manage an integration project, a user must deploy the project to Jitterbit Harmony. The project stores design and implementation details to instruct Agent Groups what activities they need to perform. This includes the following:

- **Integration operations** that describe what a unit of integration will do. For example, synchronize all changes to customer data in the CRM system with customer data in the ERP system.
- **Transformations and scripts** that describe how that data is transposed from the source system to the target system. This includes any validation rules or data manipulation required to transfer the data successfully.
- **Interfaces** that describe the various source and target object structures. These interfaces can be simple text structures or complex XML, JSON, or EDI object representations.
- **Connections and endpoints** that are used as sources or targets. While these can be hard-coded values, including system addresses and credentials, they can also be referenced through variables that can be stored in internal databases for customers that implement their own credential vaults.
- **Schedules and notifications** that determine when batch operations need to run and what to do in the event of successful and failed outcomes.
- **API endpoints** that inform agents and Agent Groups how to expose APIs so that external system events can call and invoke Jitterbit integrations.

JITTERBIT CONFIDENTIAL | FOR INTERNAL USE ONLY | COPYRIGHT © 1998 - 2020 JITTERBIT, INC.

Persistent data is secured at rest with:

- Authentication
- Access control lists
- FIPS 140-2 encryption and unique per customer encryption keys

Persistent cloud data is secured in transit with:

- Authentication
- TLS (Transport Layer Security) encryption

Integration Activity Log

When an Agent Group runs an integration operation, it synchronizes its logs to the Jitterbit Harmony multi-tenant rotating activity log. This includes the following information:

- **Status** — The state of an operation (e.g., pending, running, successful, failed).
- **Agent** — Which agent in the Agent Group ran the operation.
- **Timing** — When the operation run was submitted, started, and completed.
- **Submitted By** — Who submitted the request to run the operation.
- **Records Processed** — The number of records processed from the source system and how many records were posted to the target.
- **Message** — Any additional information that is relevant for troubleshooting a failed outcome, or summary information that a user explicitly tells Jitterbit to write to the log using the internal function `WriteToOperationLog()`.

The activity log data is stored in the cloud on a rotating daily partitioned system. The activities for each day are captured in that day's partition and each partition is dropped after 31 days. Activity log data older than 31 days is permanently removed.

JITTERBIT CONFIDENTIAL | FOR INTERNAL USE ONLY | COPYRIGHT © 1998 - 2020 JITTERBIT, INC.

Agent Logs

Each agent can generate additional data that can either be accessed via Jitterbit Harmony or can be stored on local file storage devices, such as file shares and SFTP, and accessed from within a firewall. These are detailed logs, which include:

- Debug logs
- Files of successful records processed
- Files of failed records processed

The Agent Groups and agents do not automatically synchronize these with Jitterbit Harmony, as they typically include confidential business data. By using their own storage devices, customers can secure their data within their firewall or on their own private cloud infrastructures.

These logs are useful for detailed troubleshooting and auditing purposes. By default, an Agent Group will store this for one to 14 days. The Agent Group can be configured to clean up this data at other intervals.

Test Data That Flows Through Jitterbit Harmony

In addition to data stored in Jitterbit Harmony, business data can flow through the cloud platform during integration design. This non-persistent test data flows when performing functions such as:

- **Load source data** — Brings sample data into a transformation tree to assist a user in identifying elements in an interface and testing transformations.
- **Test transformation** — Shows the transformed target result for a given set of data that is loaded.
- **Test transformation function or script** — Allows a user to test functions and scripts that could include a database select statement or view variable values returned from a web service API.
- **Test web service call and test operation** — Allows the user to run an integration and view all results on the screen.

The Jitterbit design services enforce a limit of 100 KB on all test data, thereby limiting this in-the-cloud data type to a very small subset.

JITTERBIT CONFIDENTIAL | FOR INTERNAL USE ONLY | COPYRIGHT © 1998 - 2020 JITTERBIT, INC.

Harmony Security Topologies

Any integration project or service, including APIs, can be deployed with the security topologies described below. Depending on the immediate and/or specific environmental needs, you should employ the topology that meets your organization's data requirements and governance policies. These deployment architectures, with associated security topologies, are summarized as follows and detailed in this section:

- **Cloud (Serverless):** On the Jitterbit Harmony cloud, where the system and scale are completely managed by Jitterbit.
- **Private (On-Premises, Local):** On an on-premises server or private cloud, where the system is self-hosted and managed locally.
- **Hybrid:** In a hybrid mode, where particular portions of the system are self-hosted and the rest is managed by Jitterbit.

Furthermore, Jitterbit allows any number of combinations and locations for its components, as well as allows swapping the deployment options ad hoc in different situations. This flexibility leads to these benefits:

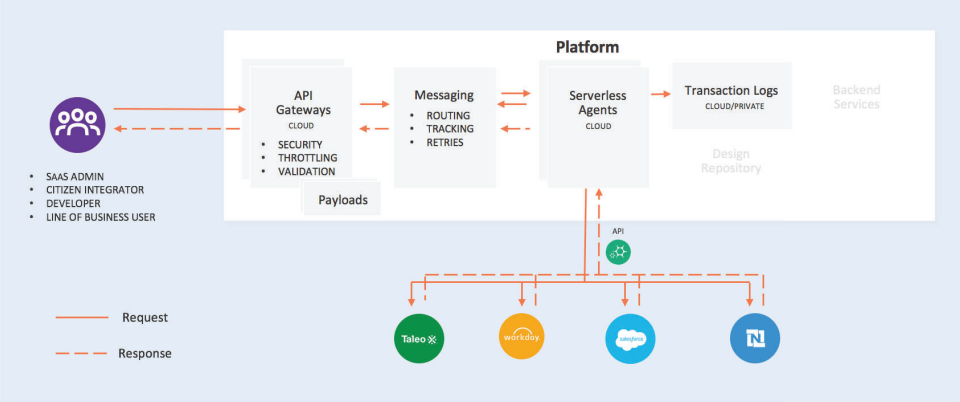
- **Greatest processing performance.** Performance can be enhanced by using edge processing, where agents are located next to where the data resides.
- **Ease of management.** Remote management is available even for private/local deployments.
- **Security and privacy.** All processing is performed by the agents directly without exposure to outside parties beyond the immediate source and target connections.

JITTERBIT CONFIDENTIAL | FOR INTERNAL USE ONLY | COPYRIGHT © 1998 - 2020 JITTERBIT, INC.

Full Cloud Deployment Security Topology

Customers who need to perform integrations where all their data sources are accessible via the cloud can deploy their projects to Jitterbit Harmony environments and run their projects on the Jitterbit Harmony Cloud Agent Group.

Real-time APIs: Full Cloud Deployment



Here, the Jitterbit-operated multi-tenant public Cloud Agent Group will access customer business data directly over the internet using HTTPS. Jitterbit Agents within this Agent Group will process business data and post it to any required target system. The data will flow within the Jitterbit network using HTTPS.

NOTE: All data mentioned above will persist in Jitterbit Harmony's secure operating environment for a brief period of time.

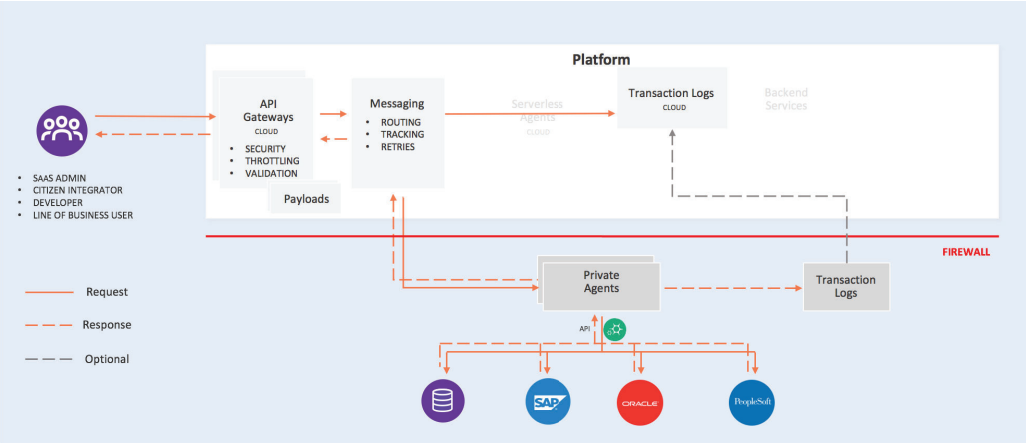
Customers that have policies that don't allow for cloud utilization or require excessive liability and indemnification guarantees should validate that the Jitterbit Master Subscription Agreement and Privacy Policy comply with needs pertaining to their industry regulations, customer provisions, customer indemnification, and customer liabilities terms.

JITTERBIT CONFIDENTIAL | FOR INTERNAL USE ONLY | COPYRIGHT © 1998 - 2020 JITTERBIT, INC.

Hybrid Deployment Security Topology

In a hybrid deployment scenario, particular portions of the system are self-hosted, and the rest is managed by Jitterbit. For example, you may not want to expose databases and apps to any cloud systems, including Jitterbit, if your organization's requirements do not allow for data to reside in the cloud (outside the firewall) due to privacy and regulatory concerns.

Real-time APIs: Hybrid Deployment



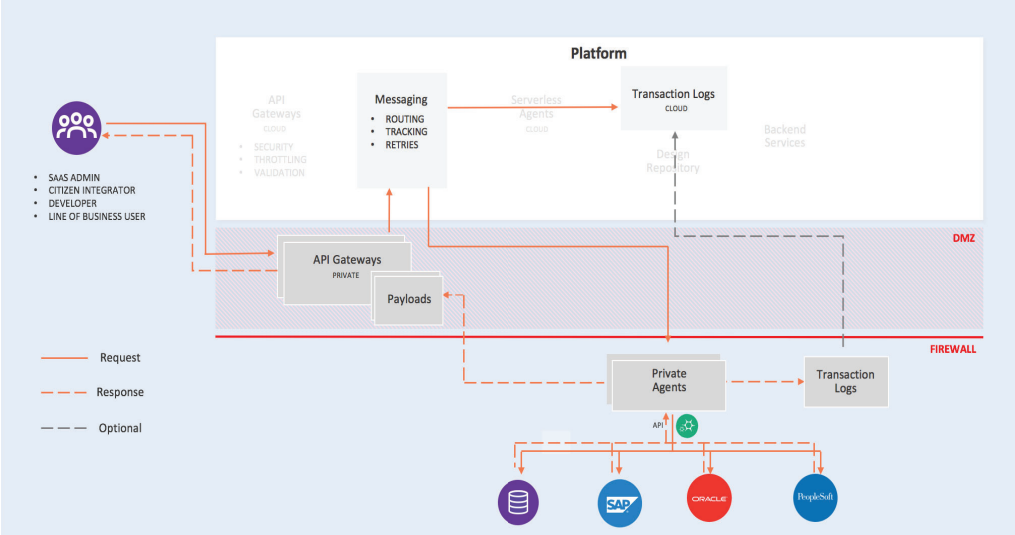
In this case, the Jitterbit Private Agents reside behind the firewall, while the API Gateway is in the Jitterbit Harmony cloud. The Agent requests the information through the messaging layer and puts the payload from the apps and data sources back to the gateway via payload. Customers can limit what gets stored in the logs to prevent this data from reaching the Jitterbit Harmony cloud.

JITTERBIT CONFIDENTIAL | FOR INTERNAL USE ONLY | COPYRIGHT © 1998 - 2020 JITTERBIT, INC.

Private Deployment Security Topology

In most enterprise integration scenarios, the Agent Group has to access internal as well as cloud applications. Here, users would deploy their projects to Jitterbit environments, install their own Private Agent Groups within their networks that have access to their applications, and then manage those Agent Groups provisioned via the Jitterbit Harmony platform.

Real-time APIs: On-Premise Deployment



This topology enables users to provision and manage their Agent Groups using Jitterbit Harmony, but the Agent Group and any sensitive business data that is processed or persists resides within their network. In this topology, the Private Agent Group can run on Windows or Linux physical or virtual server environments (see Private Agent System Requirements for further information).

JITTERBIT CONFIDENTIAL | FOR INTERNAL USE ONLY | COPYRIGHT © 1998 - 2020 JITTERBIT, INC.

Physical Security

Jitterbit Harmony is hosted on AWS cloud infrastructure. Jitterbit chose AWS as it provides a platform that addresses Jitterbit Harmony's scalability and availability, and many of its security requirements.

Infrastructure Compliance

The IT infrastructure that AWS provides is designed, managed, and third-party audited in alignment with security best practices and a variety of IT security standards. See Amazon Web Services: Overview of Security Processes for a description of core AWS security services.

In addition, integration projects deployed on Jitterbit Harmony can be configured to meet several industry-specific regulations and standards, including:

- HIPAA
- GDPR
- Cloud Security Alliance (CSA)
- SOC1 type 2
- SOC2 type 2
- ISO 27017, 27001

Physical and Environmental Security

Jitterbit Harmony is deployed across AWS managed data centers. More information on AWS physical security can be found at AWS Data Centers – Our Controls.

Business Continuity Management

Jitterbit Harmony leverages AWS's infrastructure to provide very high levels of availability. AWS has designed its systems to tolerate system or hardware failures with minimal impact.

JITTERBIT CONFIDENTIAL | FOR INTERNAL USE ONLY | COPYRIGHT © 1998 - 2020 JITTERBIT, INC.

High Availability and Fault Tolerance

Data centers are built in clusters in various global regions. In case of failure, built-in processes reroute customer data traffic away from the affected area to avoid downtime affecting your data. Core applications are deployed in an N+1 configuration, so if a data center failure occurs, there is sufficient capacity to enable traffic to be load-balanced to the remaining sites.

Jitterbit Harmony is deployed across three independent and geographically-distinct clouds (each with a primary and secondary region): NA East and NA West; EMEA East and EMEA West; APAC East and APAC West, with three data centers (availability zones) in each region.

Each availability zone is designed as an independent failure zone. This means that availability zones are physically separated within a typical metropolitan region and are located in lower risk floodplains; specific flood zone categorization varies by region. In addition to discrete UPS and onsite back-up generation facilities, they are each fed via different grids from independent utilities to further reduce single points of failure. Availability zones are all redundantly connected to multiple Tier-1 transit providers.

This provides high levels of resiliency for Jitterbit Harmony, as it can tolerate most failure modes, including natural disasters or system failures without shutdown.

In the United States, in case of a widespread catastrophic outage, Jitterbit can also route all traffic destined for the affected data center to a data center on the opposite coast.

Physical access is strictly controlled both at the perimeter and at building ingress points by professional security staff utilizing video surveillance, intrusion detection systems, and other electronic means. Authorized staff must pass two-factor authentication a minimum of two times to access data center floors. All visitors and contractors are required to present identification and are signed in and continually escorted by authorized staff.

AWS only provides data center access and information to employees and contractors who have a legitimate business need for such privileges. When an employee no longer has a business need for these privileges, his or her access is immediately revoked, even if they continue to be an AWS employee. All physical access to data centers by AWS employees is logged and audited routinely.

JITTERBIT CONFIDENTIAL | FOR INTERNAL USE ONLY | COPYRIGHT © 1998 - 2020 JITTERBIT, INC.

Incident Response

Jitterbit's Operations and Customer Support teams work to identify any issues that may impact Jitterbit Harmony users. They monitor Jitterbit Harmony's API usage, databases, services, messaging infrastructure, and Jitterbit Cloud Agent Groups. The Jitterbit Support and Operations teams provide global coverage to detect any critical issues and manage the impact and resolution of those incidents.

Jitterbit Harmony's infrastructure is supported by the Amazon Incident Management team, which employs industry-standard diagnostic procedures to drive resolution during business-impacting events. Staff operators provide 24/7/365 coverage to detect incidents and to manage the impact and resolution.

Communication

Jitterbit implements various methods of internal communication at a global level to coordinate all critical communication across Jitterbit's Operations, Customer Support, Engineering, QA, and Service teams. These teams have a presence across the US, Asia, and Europe. Our employees understand their individual roles and responsibilities and know when to communicate significant events in a timely manner.

Jitterbit has standard daily meetings among the various teams, which include team managers and company officers, to highlight any known issues and ensure that there are no bottlenecks within the organization preventing fast resolution.

Network Security

Jitterbit Harmony resides within the AWS network, which has been architected to provide the level of security and resiliency required for Jitterbit Harmony to support high trust and service levels.

Jitterbit Harmony is geographically dispersed, with a fault-tolerant architecture supported in all core services. Jitterbit Harmony relies on AWS world-class network infrastructure that is carefully monitored and managed. This includes:

Secure Network Architecture

Network devices, including firewall and other boundary devices, are in place to monitor and control communications at the external boundary of the network and at key internal boundaries within the network. These boundary devices employ rule sets, access control lists (ACL), and configurations to enforce the flow of information to specific information system services.

JITTERBIT CONFIDENTIAL | FOR INTERNAL USE ONLY | COPYRIGHT © 1998 - 2020 JITTERBIT, INC.

Specifically, AWS provides the following services to Jitterbit and Harmony:

Specifically, AWS provides the following services to Jitterbit and Harmony:

- **Secure Architecture**
  Jitterbit Harmony infrastructure components run in separate AWS Virtual Private Clouds. Each stack is an isolated network. Most services run in a private subnet. Only TLS endpoints and a bastion host (for Jitterbit management) are exposed to the Internet. Backend users connect to the stack through the bastion host, which restricts access to stack components and logs activity for security review.
- **Firewalls**
  All stack hosts run mandatory inbound firewalls configured in deny-all mode. HTTP, HTTPS, and SSH ports are opened only as necessary.
- **Distributed Denial of Service (DDoS) Protection and Mitigation**
  - Jitterbit Harmony's Virtual Private Cluster (VPC)-based approach means that no backend infrastructure is directly accessible from the Internet. As such, Harmony components cannot be targeted directly for a DDoS attack. AWS perimeter controls are in place (and tested) and are designed to prevent and detect DDoS attacks. Response teams and supporting processes are in place on behalf of all AWS clients.
  - Jitterbit Harmony TLS endpoints include an AWS Elastic Load Balancer, which only supports valid TCP requests, meaning DDoS attacks such as UDP and SYN floods do not reach the Harmony application layer.
  - We acknowledge that no control set is perfect. Should Jitterbit need extra capacity to deal with a potential DDoS attack, we can instantly scale our technology stack.
- **Port Scanning**
  AWS tools and teams monitor and block unauthorized port scanning. Because Harmony's cloud infrastructure is private and all hosts are protected by robust firewalls, port scanning is generally ineffective.
- **Spoofing and Sniffing**
  AWS configures their network and hosts to prohibit sending traffic with a source

JITTERBIT CONFIDENTIAL | FOR INTERNAL USE ONLY | COPYRIGHT © 1998 - 2020 JITTERBIT, INC.

IP or MAC address other than its own. The AWS hypervisor is configured to disallow the delivery of any traffic to a host the traffic is not addressed to. This means that any host trying to run in promiscuous mode will not be able to sniff traffic intended for other hosts.

- **Man in the Middle (MITM) Attacks**
  All of the Jitterbit Harmony APIs are available via TLS protected endpoints, which provide server authentication.
- **Intrusion Detection and Prevention**
  AWS regularly penetration tests their infrastructure. Annually, Jitterbit also engages a third-party security service firm to do a penetration test of the Harmony infrastructure. For both AWS and Jitterbit, any penetration test findings are remediated immediately.
- **Network and Host Vulnerability Scanning**
  AWS scans the internet-facing network and Jitterbit scans Harmony's private network systems regularly. AWS and Jitterbit are jointly responsible for host security. AWS and/or Jitterbit remediates adverse findings without customer intervention or downtime.
- **Penetration Testing**
  AWS regularly penetration tests their infrastructure. Annually, Jitterbit engages a nationally recognized third-party security services firm to penetration test the Harmony infrastructure. For both AWS and Jitterbit, any penetration test findings are remediated immediately.
- **Secure Harmony Hosts**
  AWS provides Jitterbit with secure hardware (server/hosts) and operating systems. AWS uses the Center for Internet Security (CIS) Configuration Benchmark for the operating systems and versions.

Host Hardening

For all operating systems:

- Automated configuration management tools install bare operating systems from "gold" images.
- Password logins for hosts are disabled. SSH root keys are not permitted.
- No unauthorized user SSH keys are permitted on hosts by default. Jitterbit internal workforce user access is configured only on a per-user basis, and only

JITTERBIT CONFIDENTIAL | FOR INTERNAL USE ONLY | COPYRIGHT © 1998 - 2020 JITTERBIT, INC.

when necessary to provide developer or customer support.

- Non-default SSH ports are used.
- Host security updates are automated.
- All host ports are opened only via whitelist.

Transmission Protection

The only external communication possible with Jitterbit Harmony is via HTTPS using Transport Layer Security (TLS), a cryptographic protocol designed to protect against eavesdropping, tampering, and message forgery.

Network Monitoring and Protection

Jitterbit Harmony leverages AWS utilization of a wide variety of automated monitoring systems to provide a high level of service performance and availability. AWS monitoring tools are designed to detect unusual or unauthorized activities and conditions at ingress and egress communication points. These tools monitor server and network usage, port scanning activities, application usage, and unauthorized intrusion attempts. The tools have the ability to set custom performance metrics thresholds for unusual activity.

Systems within AWS are extensively instrumented to monitor key operational metrics. Alarms automatically notify operations and management personnel when early warning thresholds are crossed on key operational metrics. An on-call schedule is used so personnel are always available to respond to operational issues. This includes a pager system, so alarms are quickly and reliably communicated to operations personnel.

Jitterbit Operations and Support teams work with Engineering to handle any incidents or issues related to Jitterbit-developed software or infrastructure. All critical issues are identified and discussed during daily calls among the teams. Postmortems are documented after any significant operational issue, regardless of external impact, and root cause analysis (RCA) reports are drafted so the root cause is captured, and corrective and preventative actions are put in place.

Jitterbit leverages AWS security-monitoring tools to help identify and resolve DDoS attacks, including distributed, flooding, and software/logic attacks. In addition to this, Jitterbit employs its own tools, monitoring and detection system with the

JITTERBIT CONFIDENTIAL | FOR INTERNAL USE ONLY | COPYRIGHT © 1998 - 2020 JITTERBIT, INC.

ability to reroute to another region if needed.

Jitterbit Harmony gains the benefits of the AWS network, which provides significant protection against traditional network security issues as described in the **Secure Network Architecture** section.

Secure Design Principles

Jitterbit Harmony's development process follows secure software development best practices. Formal design reviews, code scans, and vulnerability scans validate that Jitterbit software is designed and developed to prevent error messages from transmitting sensitive information and ensure that software services reject unauthorized access and misuse.

Change Management

Routine, emergency, and configuration changes to existing Jitterbit Harmony infrastructure are authorized, logged, tested, approved, and documented in accordance with industry norms for similar systems. Updates to Jitterbit Harmony's infrastructure are done to minimize any impact on the customer and their use of the services. The Jitterbit Harmony Trust site provides a public-facing dashboard that lists any outages and periods of system performance degradation, as well as scheduled maintenance and software releases.

Software

Jitterbit Engineering applies a systematic approach to managing change so that changes to customer-impacting services are thoroughly reviewed, tested, approved, and well-communicated. The change management process is designed to avoid unintended service disruptions and to maintain the integrity of service to the customer. Changes deployed into production environments are:

- **Reviewed**: Peer reviews of the technical aspects of a change are required.
- **Tested**: Changes being applied are tested by a separate QA team to ensure they will behave as expected and not adversely impact performance.
- **Approved**: All changes must be authorized in order to be rolled out by Engineering, QA, and Customer Support.

JITTERBIT CONFIDENTIAL | FOR INTERNAL USE ONLY | COPYRIGHT © 1998 - 2020 JITTERBIT, INC.

When possible, changes are scheduled during regular change windows. Emergency changes to production systems that require deviations from standard change management procedures are associated with an incident and are logged and approved as appropriate.

Infrastructure

Jitterbit Harmony runs inside a Virtual Private Cluster (VPC) and includes the following services within each region:

1. **Elastic Load Balancer (ELB)** that ensures requests to Jitterbit Harmony services and APIs scale and are highly available together with the Apache Tomcat Cluster where Jitterbit Harmony services run. The number of nodes per cluster scales dynamically as request volumes scale up and down.
2. **Caching Server Cluster** for managing user sessions. This cluster is designed with built-in redundancy to ensure that a user's session is not affected, switching to another node when needed.
3. **MQ Broker Network** that manages requests for agents. This ensures that there is a highly available redundant network among Jitterbit Harmony and all agents.
4. **Relational Database Server** with near real-time asynchronous replication across regions. This ensures that all project designs and activity data is available across regions in the event that an entire region becomes unavailable.

AWS services are architected to work efficiently and securely with all AWS networks and platforms. Each service provides extensive security features to protect sensitive data and applications.

Amazon Elastic Compute Cloud (Amazon EC2) Security

Jitterbit Harmony makes extensive use of AWS Elastic Compute Cloud (EC2), which provides resizable computing capacity using server instances in AWS's data centers.

Multiple Levels of Security

Jitterbit Harmony leverages the security within Amazon EC2 provided via the virtual instance OS firewall. External API access is only available on the Jitterbit Harmony HTTPS servers. All other services are protected behind the firewall.

JITTERBIT CONFIDENTIAL | FOR INTERNAL USE ONLY | COPYRIGHT © 1998 - 2020 JITTERBIT, INC.

The Hypervisor

Jitterbit Harmony Amazon EC2 currently utilizes a highly customized version of the Xen hypervisor, taking advantage of paravirtualization (in the case of Linux guests). Because paravirtualized guests rely on the hypervisor to provide support for operations that normally require privileged access, the guest OS has no elevated access to the CPU. The CPU provides four separate privilege modes: 0 through 3, called rings. Ring 0 is the most privileged and 3 is the least. The host OS executes in Ring 0. However, rather than executing in Ring 0 as most operating systems do, the guest OS runs in a lesser-privileged Ring 1 and applications in the least-privileged Ring 3. This explicit virtualization of the physical resources leads to a clear separation between guest and hypervisor, resulting in additional security separation between the two.

Each Jitterbit Harmony Virtual EC2 instance is controlled by the Jitterbit Operations team. All Jitterbit Harmony instances are hardened and utilize certificate based SSHv2 to access the virtual instance. All key pairs are generated by Jitterbit Operations in order to guarantee that they are unique, and not shared outside Jitterbit Operations.

Load Balancing Security

Amazon Elastic Load Balancing (ELB) is used to manage traffic on a fleet of Amazon EC2 instances. ELB has all the advantages of an on-premise load balancer, plus several security benefits:

- Takes over the encryption and decryption work from the Amazon EC2 instances and manages it centrally on the load balancer.
- Provides a single point of contact, and also serves as the first line of defense against attacks on your network.
- Supports end-to-end traffic encryption using TLS (Transport Layer Security, previously SSL) on those networks that use Secure HTTP (HTTPS) connections. When TLS is used, the TLS server certificate used to terminate client connections can be managed centrally on the load balancer, rather than on every individual instance.
- Supports creation and management of security groups associated with your Elastic Load Balancing, when used in an Amazon VPC, to provide additional networking and security options.

JITTERBIT CONFIDENTIAL | FOR INTERNAL USE ONLY | COPYRIGHT © 1998 - 2020 JITTERBIT, INC.

Data Storage

Jitterbit Harmony uses Amazon S3 for file data storage. This data includes transformation schemas, database drivers, plugins and in certain cases, temporary and log files.

Jitterbit Harmony uses the Amazon S3 Encryption Client to encrypt data before uploading to Amazon S3. Amazon S3 uses one of the strongest block ciphers available: 256-bit Advanced Encryption Standard (AES-256). With Amazon S3, every protected object is encrypted with a unique encryption key. This object key itself is then encrypted with a regularly rotated master key. Amazon S3 provides additional security by storing the encrypted data and encryption keys in different hosts.

Data Durability and Reliability

Amazon S3 is designed to provide 99.999999999% durability and 99.99% availability of objects over a given year. Objects are redundantly stored on multiple devices across multiple facilities in an Amazon S3 region. To help provide durability, Amazon S3 PUT and COPY operations synchronously store customer data across multiple facilities before returning SUCCESS. Once stored, Amazon S3 helps maintain the durability of the objects by quickly detecting and repairing any lost redundancy. Amazon S3 also regularly verifies the integrity of data stored using checksums. If corruption is detected, it is repaired using redundant data. In addition, Amazon S3 calculates checksums on all network traffic to detect corruption of data packets when storing or retrieving data.

JITTERBIT CONFIDENTIAL | FOR INTERNAL USE ONLY | COPYRIGHT © 1998 - 2020 JITTERBIT, INC.

Organizational Security

Jitterbit strives to apply the operational best practices of leading cloud-computing providers around the world. This includes the following:

Confidentiality

Jitterbit Harmony's confidentiality measures work to protect sensitive customer data from unauthorized access. In addition to the physical and logical security layers provided by our software and physical infrastructure, our internal policies dictate:

- **Separation of Duties:** Access to Jitterbit Harmony's production system is available only to the Jitterbit Operations team. Any changes to the production environment must be applied by the Jitterbit Operations team.
- **Minimum Necessary and Least Privilege:** Within the Jitterbit Operations team, access is restricted to the various Jitterbit services on an as-needed basis. The team knows which employee has access to which Jitterbit Harmony production resource at any point in time and can revoke that access as needed.

Personnel Policy

Jitterbit's personnel policy is designed to maintain a high level of employee trustworthiness and to keep employees aware of key aspects of information security and privacy. Employees must comply with a code of conduct that emphasizes confidentiality, ethics, and professionalism in all interactions with Jitterbit's users, partners, and competitors. All employees sign a confidentiality agreement that protects Jitterbit's customer data. All Jitterbit employees receive regular security training and testing.

Jitterbit Operations

The Jitterbit Operations team is responsible for defining and executing procedures for application release management, hardware and operating system upgrades, system health monitoring, and other activities required for the maintenance of Jitterbit Harmony.

JITTERBIT CONFIDENTIAL | FOR INTERNAL USE ONLY | COPYRIGHT © 1998 - 2020 JITTERBIT, INC.

The team's responsibilities include:

- Reviewing the security of cloud infrastructure design and implementation.
- Implementing procedures that follow security standards, such as Cloud Security Alliance (CSA) and Cloud Internet Security (CIS).
- Defining and implementing identity and access management policy, and procedures for assigning unique and trackable identities to each authorized Jitterbit team member.
- Defining data confidentiality classifications that require employees who access Jitterbit Harmony customer information to do so in a prescribed manner that limits the possibility of unauthorized access.
- Identifying and implementing technologies that secure customer information, including FIPS 140-2 level encryption technologies for data in transit and data at rest.
- Conducting technical and non-technical information security assessments (evaluations) that are based on penetration tests, vulnerability scans, and audits against core regulations and standard codes of practice.
- Monitoring the Jitterbit Harmony applications and infrastructure for possible security issues.
- Remediating findings and issues quickly.

Jitterbit Engineering

The Jitterbit Engineering team is responsible for designing, implementing, and testing the software services provided by Jitterbit Harmony. The Engineering team works closely with the Operations team to identify security concerns, develop monitoring procedures, and implement protective technology. The security responsibilities of the Engineering team include:

- Defining and implementing secure design and coding practices.
- Conducting design reviews to identify possible security concerns prior to coding.

JITTERBIT CONFIDENTIAL | FOR INTERNAL USE ONLY | COPYRIGHT © 1998 - 2020 JITTERBIT, INC.

- Conducting code reviews to identify code that could be exploited to grant unauthorized access to customer data.
- Conducting code reviews to identify code that could negatively impact availability.
- Performing load tests in pre-production environments to verify that availability requirements have been met.

Jitterbit QA

The Jitterbit QA team is responsible for carrying out new and existing regression tests on all software released by Engineering to ensure no security or functional issues are introduced with changes in the software. The Jitterbit QA team performs its function in a separate environment that closely resembles production configurations. The Jitterbit QA team must approve any software release before the Jitterbit Operations team can deploy that software to the Jitterbit Harmony production environment.

Jitterbit Harmony Trust Site

Jitterbit Harmony availability and security statuses are monitored 24 hours a day, seven days a week by the Jitterbit Operations Team. The data pertaining to such monitoring is published on the Jitterbit Harmony Trust site giving users and the general public transparent visibility into our operations.

Identity and Access Management

Access Control and Least Privilege

Identity and access management policy requires that all Jitterbit personnel that have access to Jitterbit Harmony production environments be provisioned with unique and trackable identities in the form of a user ID. Identity and access management policy enforces the principle of least privilege, which restricts personnel to the minimum level of access required to complete their assigned tasks.

JITTERBIT CONFIDENTIAL | FOR INTERNAL USE ONLY | COPYRIGHT © 1998 - 2020 JITTERBIT, INC.

Periodic Access Review

Virtual instances, firewalls, database servers, and other infrastructure software and hardware are protected by user identities that have been granted a limited set of permissions. Permission grants are regularly reviewed by the Operations team and revoked when an employee leaves the company. The Operations team enforces a password policy throughout Jitterbit Harmony production environments that require strong passwords, regular password expiration, and restrictions on password reuse.

Incident Management

The goal of the Jitterbit incident management policy is not only to quickly and effectively close incidents, but also to collect and distribute incident information so that processes are continuously improved and future responses are driven by accumulated knowledge.

Incident management includes initial diagnosis, classification, prioritization, escalation, and closure. All incidents that do not affect users of Jitterbit Harmony are recorded in the engineering issue tracking system. Any issues that affect users are recorded in the Customer Support system so that any effects on SLAs are tracked.

Patch Management and High Availability

Jitterbit is continually strengthening its products as new threats to security emerge. In addition, the software infrastructure we use is also being strengthened.

In order to keep software current, the Operations team works with the Engineering and QA team following a detailed patch management policy that covers the discovery, testing, and deployment of security patches. The AWS and Harmony's virtual infrastructure strategy allows Harmony to remain available, even during upgrades.

The Operations team actively monitors vendor security advisories and subscribes to new patch release notifications.

Capacity Management

Jitterbit Harmony currently supports thousands of active users who perform various integration processes. The Jitterbit Harmony platform has been developed to scale dynamically. The core services that expose APIs to our tools and users run on Apache Tomcat. Our systems track current usage rate and automatically provision and stop EC2 instances as required.

JITTERBIT CONFIDENTIAL | FOR INTERNAL USE ONLY | COPYRIGHT © 1998 - 2020 JITTERBIT, INC.