BETTERCLOUD, INC.

INDEPENDENT SERVICE AUDITOR'S SOC 3 REPORT

FOR THE

BETTERCLOUD APPLICATION SYSTEM

FOR THE PERIOD OF JANUARY 1, 2018, TO SEPTEMBER 30, 2018

Attestation and Compliance Services

INDEPENDENT SERVICE AUDITOR'S REPORT

To BetterCloud, Inc.:

Scope

We have examined BetterCloud, Inc.'s ("BetterCloud") accompanying assertion titled "Assertion of BetterCloud, Inc. Service Organization Management" ("assertion") that the controls within BetterCloud's BetterCloud Application system ("system") were effective throughout the period January 1, 2018, to September 30, 2018, to provide reasonable assurance that BetterCloud's service commitments and system requirements were achieved based on the trust services criteria relevant to security and confidentiality (applicable trust services criteria) set forth in the 2016 TSP section 100A, *Trust Services Principles and Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy (AICPA, Trust Services Principles and Criteria)*.

BetterCloud uses a subservice organization for data center hosting services. The description of the boundaries of the system indicates that complimentary subservice organization controls that are suitably designed and operating effectively are necessary, along with controls at BetterCloud, to achieve BetterCloud's service commitments and system requirements based on the applicable trust services criteria. The description of the boundaries of the system does not disclose the actual controls at the subservice organization. Our examination did not include the services provided by the subservice organization, and we have not evaluated the suitability of the design or operating effectiveness of such complimentary subservice organization controls.

Service Organization's Responsibilities

BetterCloud is responsible for its service commitments and system requirements and for designing, implementing, and operating effective controls within the system to provide reasonable assurance that BetterCloud's service commitments and system requirements were achieved. BetterCloud has also provided the accompanying assertion about the effectiveness of controls within the system. When preparing its assertion, BetterCloud is responsible for selecting, and identifying in its assertion, the applicable trust services criteria and for having a reasonable basis for its assertion by performing an assessment of the effectiveness of the controls within the system.

Service Auditor's Responsibilities

Our responsibility is to express an opinion, based on our examination, on whether management's assertion that controls within the system were effective throughout the period to provide reasonable assurance that the service organization's service commitments and systems requirements were achieved based on the applicable trust services criteria. Our examination was conducted in accordance with attestation standards established by the American Institute of Certified Public Accountants. Those standards require that we plan and perform our examination to obtain reasonable assurance about whether management's assertion is fairly stated, in all material respects. We believe that the evidence we obtained is sufficient and appropriate to provide a reasonable basis for our opinion.

Our examination included:

- Obtaining an understanding of the system and the service organization's service commitments and system requirements;
- Assessing the risks that controls were not effective to achieve BetterCloud's service commitments and system requirements based on the applicable trust services criteria; and
- Performing procedures to obtain evidence about whether controls within the system were effective to achieve BetterCloud's service commitments and system requirements based on the applicable trust services criteria.

Our examination also included performing such other procedures as we considered necessary in the circumstances.

Inherent Limitations

There are inherent limitations in the effectiveness of any system of internal control, including the possibility of human error and the circumvention of controls.

Because of their nature, controls may not always operate effectively to provide reasonable assurance that BetterCloud's service commitments and system requirements were achieved based on the applicable trust services criteria. Also, the projection to the future of any conclusions about the effectiveness of controls is subject to the risk that controls may become inadequate because of changes in conditions or that the degree of compliance with the policies or procedures may deteriorate.

Opinion

In our opinion, management's assertion that the controls within BetterCloud's BetterCloud Application system were effective throughout the period January 1, 2018, through September 30, 2018, to provide reasonable assurance that BetterCloud's service commitments and system requirements were achieved based on the applicable trust services criteria is fairly stated, in all material respects

Schellman & Company, LLC

Tampa, Florida
November 5, 2018

ASSERTION OF BETTERCLOUD, INC. SERVICE ORGANIZATION MANAGEMENT

We are responsible for designing, implementing, operating, and maintaining effective controls within BetterCloud, Inc.'s ("BetterCloud") BetterCloud Application system ("system") throughout the period January 1, 2018, to September 30, 2018, to provide reasonable assurance that BetterCloud's service commitments and system requirements relevant to security and confidentiality were achieved. Our description of the boundaries of the system is presented below and identifies the aspects of the system covered by our assertion.

We have performed an evaluation of the effectiveness of the controls within the system throughout the period January 1, 2018, to September 30, 2018, to provide reasonable assurance that BetterCloud's service commitments and system requirements were achieved based on the trust services criteria relevant to security and confidentiality (applicable trust services criteria) set forth in the 2016 TSP section 100A, *Trust Services Principles and Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy (AICPA, Trust Services Principles and Criteria*). BetterCloud's objectives for the system in applying the applying the applicable trust services criteria are embodied in its service commitments and systems requirements relevant to the applicable trust services criteria. The principal service commitments and system requirements related to the applicable trust services criteria are presented below.

There are inherent limitations in any system of internal control, including the possibility of human error and the circumvention of controls. Because of these inherent limitations, a service organization may achieve reasonable, but not absolute, assurance that its service commitments and system requirements are achieved.

We assert that the controls within the system were effective throughout the period January 1, 2018, to September 30, 2018, to provide reasonable assurance that BetterCloud's service commitments and systems requirements were achieved based on the applicable trust services criteria.

SYSTEM DESCRIPTION OF THE BETTERCLOUD APPLICATION SYSTEM

Company Background

Founded in 2011, BetterCloud, Inc. ("BetterCloud") is a provider of cloud management and security tools through the use of user lifecycle management, data discovery, and IT and security automation purpose-built for software as a service (SaaS) applications. BetterCloud began focusing initially on helping businesses use G Suite services through the use of G Suite services management tools. The company is headquartered in New York, New York, with an office in Atlanta, Georgia. BetterCloud, its flagship product, used by thousands of companies and millions of users worldwide, provides SaaS operations management to streamline user lifecycle management, data discovery, and information technology (IT) and security automation for a breadth of SaaS applications, integrated within a comprehensive and web-based interface. "Policies", BetterCloud's most recent expansion of the product provides expanded automation and workflow capabilities that enable IT and security teams to orchestrate complex processes to ensure accuracy, precision, and compliance across SaaS applications.

Description of Services Provided

BetterCloud provides SaaS administration services to customers via the BetterCloud application. BetterCloud application is a web-based cloud management tool designed to provide directory management, security, and facilitate administrators as they control and secure their cloud domains, delegate granular privileges to non-information technology employees, and automate common management tasks.

Depending on the complexity of customer organization's IT infrastructure, there can be a number of integrations with systems such as customer relationship management (CRM), enterprise resource planning (ERP), or accounting systems. BetterCloud application users include customer organizations that store their data in various cloud infrastructure. BetterCloud administrators utilize the application programming interfaces (APIs) to administer (monitor, delete, change access, create assets, etc.) on behalf of the customers.

While the BetterCloud application provides the ability for users to manage user accounts, secure domains, monitor activity, and automate administrative tasks, BetterCloud personnel only support the availability and functionality of the BetterCloud application through application design, authorized change management procedures, and availability oversight for the services provided by Google.

When a customer administrator installs the BetterCloud application, they grant permission for the application to access data in their connected SaaS applications.

BetterCloud Application Registration

BetterCloud registers the BetterCloud application with SaaS providers (e.g. Google, Okta, Salesforce, Dropbox, Box, etc.) to establish a trust relationship. This process requires the use of secret keys provisioned by the SaaS providers that uniquely identify, validate, and authorize the BetterCloud application for availability in the SaaS provider's marketplace. These uniquely-verified keys ensure that customers are using the authenticated BetterCloud application. BetterCloud customers and prospects request a BetterCloud application installation from the respective SaaS provider's marketplace. Next, they consent to the data that is going to be shared and/or acted upon by the BetterCloud application by approving "scopes" of access. Customer's SaaS administrators accept the scopes of access required by the BetterCloud application. They can then connect to other SaaS providers through similar mechanisms or through BetterCloud's 'Connectors' page.

Configuration Management

BetterCloud provides domain-level restriction based on specific tokens. BetterCloud administrators configure the various customer environments known as configurations. BetterCloud personnel manage these configurations on an ongoing basis.

[Intentionally Blank]

System Boundaries

A system is designed, implemented, and operated to achieve specific business objectives in accordance with management-specified requirements. The purpose of the system description is to delineate the boundaries of the system, which includes the services outlined above and the five components described below: infrastructure, software, people, procedures, and data.

Infrastructure and Software

Infrastructure supporting the BetterCloud application is owned and managed by Google. The software associated with the BetterCloud application is the application itself, code development tools and source code repository (Bitbucket and Google Container Registry), and the underlying code execution infrastructure (Google Cloud Platform). Google Cloud Platform is also utilized for configuring firewall rules to allow or deny traffic to and from the virtual machines.

The in-scope infrastructure is shown in the table below:

Primary Infrastructure			
Production Application	**Business Function Description**	**Hardware Platform / Operating Systems**	**Physical Location**
BetterCloud	Monitoring and administration of cloud applications.	Google Cloud Platform / Google proprietary Linux, Ubuntu / MySQL database	Servers reside in Google data centers within the United States.

People

The personnel involved in the operation and support of the system include, but is not limited to, the following:

- Executive Management – responsible for overseeing company-wide activities, establishing, and accomplishing goals, and overseeing objectives.
- Security Team – responsibilities include, but is not limited to, the following:
    - The review, maintenance, and compliance of BetterCloud security policies
    - The review of BetterCloud utilized systems and devices
    - Risk management and identification
    - Monitoring and review of security and confidentiality issues and incidents
- Platform Services personnel – responsibilities include, but is not limited to, the following:
    - Monitoring and maintenance of the production system and support systems
    - Provision and assignment of application infrastructure
    - Automation of production system promotion and analysis
- Engineering and Functional QA personnel – responsible for designing, coding, testing, and implementing BetterCloud applications into the Google cloud.
- Human Resources (HR) and Administration personnel – responsible for evaluating and screening candidates and the daily non-technical operations within the office.
- Customer Support, Enablement, Success, Sales and Marketing personnel – responsible for managing relationships with current customers and performing marketing and sales activities to attract new customers.

Procedures

BetterCloud security and confidentiality policies and procedures are documented and available to employees on an internal website. Employees are required to acknowledge that they have read and understood the applicable cohesive set of security and confidentiality policies and procedures as part of the onboarding process. Detailed policies and procedures are defined and include, but are not limited to, the following categories of functions: information security, risk assessment, incident response, system reviews, change management, data classification and usage, third party reviews, hiring, and HR.

Logical Access

The BetterCloud application environment is comprised of production environments managed by BetterCloud and the customer-controlled environment. Because the BetterCloud application is an administration management tool, the overall security of the customer data and information is highly dependent upon the customer-controlled environment and the related security policies and procedures. The following description is specific to the BetterCloud application environment managed by BetterCloud and the logical access safeguards in place at BetterCloud only.

The BetterCloud application production environments are hosted on the Google Cloud Platform at Google data centers. Logical access into the hosted production environment requires a Google account with multi-factor authentication and access to virtual machines requires an SSH key pair with multi-factor authentication.

BetterCloud Application Access Administration

BetterCloud employees are required to sign a Proprietary Information and Invention Assignment Agreement (PIIAA) upon hiring, which requires their acceptance and agreement to adhere to protecting the confidentiality of information, including customer information. BetterCloud utilizes a documented user access provisioning process for granting BetterCloud personnel access to the BetterCloud application production environment. Users are required to request access to the application and production resources via a standardized Secure System Access Request form. User access is based on pre-defined user roles. The form requires the requestor to document the level of BetterCloud application and production resource access requested and business justification for access. Requests for application and production resource access are approved by the security team prior to granting access to the application or production resource.

Logical access to the BetterCloud application production environment is limited to authorized personnel based on job responsibility and areas of oversight. Administrators remove (de-provision) user account privileges assigned to terminated employees. Access to the application secret keys is restricted to user accounts accessible by authorized personnel.

BetterCloud Application Authentication

BetterCloud users are required to authenticate to the application via single sign-on (SSO) with a supported identity provider (Google, Microsoft, or Okta). The OAuth 2.0 open standard allows customers to authorize BetterCloud to access their SaaS application without sharing user credentials. OAuth tokens are transmitted securely using TLS and set to expire in 24 hours.

BetterCloud Application Access Monitoring

The security team performs a review of production user account listing on a quarterly basis. During this review, the security team ensures access privileges are commensurate with the user's role, job responsibilities and areas of oversight. This review also includes review of the users with access to the application secret keys.

Anti-Malware

To protect the production environment from malicious software, a central endpoint protection and response (EDR) system is configured with anti-malware software to protect registered workstations. The software is configured to perform updates on the virus definitions and scan the registered clients on-demand.

[Intentionally Blank]

Change Management

The goal of the change management process is to manage operational changes to configuration items with minimum disruptions, risk and complexity while maintaining service level agreements (SLAs). This includes ensuring that there is a business reason behind each change, identifying the specific configuration item and IT services affected by the change, planning the change, testing the change, and having a back-out plan should the change result in an unexpected state of the configuration item. Development teams and IT management conduct separate meetings throughout each week to discuss ongoing and upcoming projects for their respective areas. The results of those meetings are published in a bi-weekly technology update that is sent to employees via e-mail.

The change management process handles any valid change. A valid change can be a request within the scope of the SLA or BetterCloud configuration changes within the standard service agreement. The change request may be generated internally or externally through customer requests.

Change management controls the flow of activities from the request being received by the organization until the change is successfully implemented, including keeping the requestor of the change aware of its progress from request / project initiation until the final sign-off. It controls the change analysis, development, testing, back-out plan, and change sign-off and acceptance.

Management utilizes an automated workflow and ticketing system (JIRA) to systematically enforce the process flow through pre-defined authorization levels, and document changes made to the production application. This is performed for the following change types:

- Bug fixes (standard changes) follow a routine change control process
- Bug fixes ("blocker" changes) have a higher priority and may follow an expedited change control process

Bug Fixes (Standard Changes)

Bug fixes are changes that are executed with regular frequency. A requestor or "bug reporter" will create or open a ticket in the JIRA ticketing system. The Bug Reporter documents the relevant details for the bug fix and determines if the bug fix is standard or if it is a higher priority (blocker) ticket. The process for blocker changes are described in the next section below.

Once prioritized, a technical leader assigns a version parameter, estimated development time, and a developer to the bug fix record. The bug fix record would also be modified to include any relevant directions for solution and comments, as necessary. While under technical review, the priority can be adjusted to a blocker, if necessary, and the bug fix would follow the blocker change process noted below. Otherwise, the technical leader assigns the developer based on priority and queue volume.

The assigned developer works the assigned tickets from their ticket queue in an "in progress" state. Once complete, the developer enters the relevant change details in the JIRA ticket (including a brief summary of the cause and the bug fix performed). The developer performs his/her own internal code testing then submits the code for code review by a technical leader. Features are required to be functionally reviewed by product owners in addition to the code review.

The developer then moves the ticket into an "in review" status pending independent review by a quality analyst. The developer and quality analyst cannot be the same individual.

The quality analyst verifies the fix and then either promotes the bug fix status to a "verified" state or rejects the fix and returns it to the assigned Developer's queue as an "in progress" status. Verified fixes are assigned a release date and release number, and a functional analyst or DevOps engineer determines when the change will be released into the production environment.

The deployer verifies the build, ensures the required fields within the ticket have been completed, and performs any additional documentation steps, as needed. They then coordinate the move to implementation and close the ticket within JIRA, with a "closed" status.

Prior to implementation, an authorized code reviewer approves the code change by merging it into a secured source branch. Once approved and merged, a Functional Analyst or Platform Services engineer will deploy the code into the production environment utilizing build deployment tool (Jenkins). The tool deploys the code to

production. BetterCloud application secret keys are secured separately and are either deployed bundled with application to the Google Cloud Platform or injected at service startup time. Deployments are performed using an authenticated service account where its secret key is validated by Google for authenticity. If the secret key is determined to be authentic, the code is deployed in the production environment.

Implementation access to the build deployment tool is limited to the security team, development operations personnel, and quality assurance (QA). The use of the build deployment tool is systematically logged and captures the date and time stamp of the deployment event, the specific user account responsible for the deployment, and the build package/version. Developers do not have the ability to approve changes or implement changes into the production environment.

Bug Fixes ("Blocker" Changes)

For bug fixes designated as blocker changes, the initiation process is identical to the standard change, whereby the Bug Reporter creates or opens the JIRA ticket. The emphasis is on swift execution of the change request. Upon assignment of the blocker priority, however, the bug reporter will not promote the change to the technical reviewer, but instead will send out a company-wide e-mail and notify a product owner directly (in person, via phone, instant message, etc.) and provide the JIRA ticket number. The product owner then works closely with a technical leader to set an expedited development priority, determine resolution instructions, and document any other items pertinent to the fix.

Developers that receive blocker items work those items immediately and will postpone development on any standard bug fixes. At this point, the process follows an identical workflow as the standard fix process described above, but in an expedited manner.

The JIRA ticket documents the assigned developer, quality analyst, and product owner, as well as their indication that the required review and approval steps have been completed. Deployments are required to be approved by the quality analyst.

System Monitoring

The Platform services team is responsible for assembling, operating, and monitoring the performance of infrastructure resources, including the systems, dependent services, and logical configurations of the production environment. The Security team is responsible for securing the environment. Several monitoring systems are in place to monitor the production environment for system events and administrative actions. An IDS is utilized to analyze and report network events. A performance monitoring tool is utilized to monitor the system up-time and performance.

Incident Response

Incident response and escalation policies and procedures are in place to manage unexpected incidents impacting the business. The procedures are reviewed on a periodic basis to ensure they are still effective in meeting the business objectives. The procedures outline the following:

- Assignment of roles and responsibilities for the design, implementation, maintenance, and execution of the incident response program
- Containment of the incident and threat
- Mitigating the effects of ongoing security incidents
- Remediation of the incident
- Communication protocols and timing to affected parties (if applicable)
- Lessons learned

Management utilizes a ticket system for documenting, communicating and collaborating to resolve any identified incidents with customers. The security monitoring systems are configured to automatically generate a ticket when potential incidents occur. Compliance personnel are alerted immediately when an incident involves unauthorized use or disclosure of confidential information. Security personnel complete incident postmortem reports. Closed security incidents are reviewed and approved by management on a weekly basis to ensure that the incident

response procedures were followed and that the incident was resolved. Corrective measures or changes that occur as a result of incidents and identified deficiencies follow the standard change control process.

Data

The BetterCloud application is used to provide SaaS administration services to customers by accessing the data in connected applications that is granted by a customer. Data that is used and supported by the system are the applicable source code, secret keys for authentication to SaaS applications, and customer data from connected applications.

BetterCloud considers customer data received from SaaS providers as confidential. Examples of customer confidential data include customer user names, sharing statuses and any other named information needed for the Google App Engine and Google Compute Engine to process BetterCloud application administration requests. Confidential data used to support the system that is not derived from customer information includes any information proprietary to the company requiring special considerations in handling and usage. This would include system architecture information and the secret keys for authentication to SaaS providers.

BetterCloud has classified aggregate customer metadata as Restricted. Such data should not be shared outside the company but is not subject to the extra scrutiny of confidentiality. Application source code and repositories stored in Bitbucket and Google Container Registry used to support the system are also considered Restricted data.

The following table describes the information used and supported by the system.

Data Used and Supported by the System		
Data Description	**Data Reporting**	**Classification**
Connected application data	Used to provide customers with a wide array of tools, such as domain monitoring, user management, e-mail monitoring and delegation, and sharing policies.	Confidential
Secret keys	Used internally to authenticate to the connected application and uniquely identify, validate, and authorize the application.	Confidential
Application source code	Used internally to build and implement code changes to the production environment.	Restricted

Subservice Organizations

The data center hosting services provided by Google were not included within the scope of this examination. The following table presents the applicable Trust Services criteria that are intended to be met by controls at Google, alone or in combination with controls at BetterCloud, and the types of controls expected to be implemented at Google to meet those criteria.

Control Activity Expected to be Implemented by Google	Applicable Trust Services Criteria
Google is responsible for securing physical access to authorized personnel to the facility that houses production infrastructure and backup media.	CC5.5

Control Activity Expected to be Implemented by Google	Applicable Trust Services Criteria
Google is responsible for enforcing encryption on production infrastructure that transmits to other public networks.	CC5.6 CC5.7 C1.3
Google is responsible for implementing procedures to protect production infrastructure from computer viruses, malicious code, and unauthorized software.	CC5.8
Google is responsible for maintaining system components including configurations for the production infrastructure.	CC7.1