BetterCloud

BetterCloud, Inc.

Independent Service Auditor's SOC 3 Report For the BetterCloud Application System

For the Period of January 1, 2019, to September 30, 2019

Attestation and Compliance Services

schellman
Quality, above all.

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 the BetterCloud Application system ("system") were effective throughout the period January 1, 2019, to September 30, 2019, 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 TSP section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy (AICPA, Trust Services 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 the BetterCloud Application system were effective throughout the period January 1, 2019, through September 30, 2019, 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 14, 2019

ASSERTION OF BETTERCLOUD 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, 2019, to September 30, 2019, 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, 2019, to September 30, 2019, 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 TSP section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy (AICPA, Trust Services 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, 2019, to September 30, 2019, 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 information technology (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 San Francisco, California, and technology office in Atlanta, Georgia. The BetterCloud application is used by thousands of companies and millions of users worldwide, provides SaaS operations management to streamline user lifecycle management, data discovery, and 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. The 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 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 that is required for SaaS operations management.

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.

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.

Principle Service Commitments and System Requirements

BetterCloud documents and communicates their security and confidentiality service commitments and system requirements via the security rider which is incorporated into the Master Subscription Agreement (MSA). The principal service commitments and system requirements are described below.

Commitments

Access Management

BetterCloud shall access customer data only in accordance with the terms of the MSA or as otherwise agreed by the customer in writing.

All BetterCloud personnel accessing customer data shall be identified by a unique user ID. Access to the BetterCloud systems and customer data located thereon shall require a user ID and password. Passwords for access to customer data shall be stored securely using industry standard encryption, not in plain text, on a separate server or file from customer data.

Personnel Management

BetterCloud personnel will only be granted access to customer data if they have a need to access customer data to provide the services, and only to the extent necessary to perform such services. BetterCloud will promptly revoke or delete all access rights to customer data for any terminated or transferred (if such transfer eliminates the business need) BetterCloud personnel. BetterCloud will require BetterCloud personnel to return or destroy any customer data within such BetterCloud personnel's possession within 48 hours of such BetterCloud personnel's termination or transfer.

Customer data may not be stored by BetterCloud personnel on personal accounts (e.g., individual e-mail or cloud services accounts) and customer data may not be accessed by BetterCloud personnel on personal accounts (e.g., individual e-mail or cloud services accounts).

BetterCloud shall maintain policies that require BetterCloud personnel to report suspected violations of BetterCloud's data security policies to BetterCloud management for investigation and action. BetterCloud will require that all BetterCloud personnel who access customer data to: (i) attend confidentiality and security awareness training at least once per year; (ii) are fully informed of BetterCloud's data security policies and standards, and (iii) are subject to disciplinary action (and/or legal action where appropriate) for violations of same.

Except as provided herein, BetterCloud, or its agent, shall perform a background check on all BetterCloud personnel. The background check shall include: (i) criminal convictions involving a dishonest act (including but not limited to fraud, theft, and embezzlement), and (ii) injury or threatened injury to another person. BetterCloud shall not permit any BetterCloud personnel with a criminal record falling into categories (i) and (ii) above to be granted access to customer data. BetterCloud shall not be obligated to conduct a background check where prohibited by applicable law.

System and Network Security

BetterCloud shall implement industry standard firewalls to manage and restrict network traffic and shall properly segment its network and systems storing customer data.

BetterCloud shall use an industry standard intrusion detection system to detect inappropriate, incorrect, or anomalous activity, and BetterCloud shall regularly monitor system logs for suspicious activity. BetterCloud shall establish and follow commercially reasonable operational procedures to stop or mitigate any real or reasonably foreseeable potential attack or attempted attack.

BetterCloud will maintain vulnerability and patch management processes and tools to regularly assess software for security vulnerabilities and to deploy software patches and updates.

BetterCloud is under no obligation to retain any customer data. The services do not replace the need for customer to maintain regular data backups or redundant data archive.

Encryption

BetterCloud will use industry standard encryption to secure customer data in transit outside of BetterCloud systems and at rest in all locations where it is stored. BetterCloud will use TLS 1.1 or 1.2 when transferring customer data over the Internet.

Full disk or device encryption is required for all portable devices and removable media used by BetterCloud personnel (e.g., laptops, flash drives, CD-ROMs, external hard drives, etc.) that store customer data.

Audits and Reporting

BetterCloud shall monitor the effectiveness of its security program by conducting self-audits and risk assessments of the BetterCloud systems against the written policies and procedures maintained by BetterCloud as required herein no less frequently than annually, including penetration and vulnerability tests conducted by a reputable third party on at least an annual basis.

BetterCloud shall use external auditors to verify the adequacy of its security measures. Such audits: (a) will be performed according to AICPA SOC 2 standards for security and confidentiality or such other alternative standards that are substantially equivalent to AICPA SOC 2; (b) will be performed by independent third-party security professionals; and (c) will result in the generation of an audit report ("Report"). BetterCloud will provide customer with access to a copy of such Report upon request, but no more frequently than once per calendar year during the term of the MSA. Reports will be treated as BetterCloud's confidential information.

Data Breach Notification

BetterCloud will notify customer of any data breach affecting customer data without undue delay, but no more than seventy-two (72) hours after BetterCloud becomes aware of such data breach. BetterCloud will take reasonable and appropriate steps to mitigate the harm resulting from a data breach and will provide updates to customer as deemed reasonably appropriate by BetterCloud based upon the severity of the data breach.

Requirements

BetterCloud maintains its information security program in a manner that enables the company to meet the security requirements of the laws, regulations, and industry standards listed below.

- European Union (EU) General Data Protection Regulation
- EU-US and Swiss-US Privacy Shield
- Trust Services Criteria for Security and Confidentiality
- Cloud Security Alliance Cloud Controls Matrix (CSA CCM)

In accordance with our assertion, and the description criteria, the aforementioned service commitments and requirements are those principal service commitments and requirements common to the broad base of users of the system and may therefore not fully address the specific service commitments and requirements made to all system users, in each individual case.

Infrastructure and Software

Infrastructure supporting the BetterCloud application is owned and managed by Google. The software associated with the BetterCloud application are the Google Cloud Platform services, microservices, continuous integration and continuous deployment (CI/CD) tools, Google Container Registry, and version control system. 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 consists of multiple applications, operating system platforms and databases, as shown in the table below:

Primary Infrastructure			
Production Application	**Business Function Description**	**Operating System Platform**	**Physical Location**
BetterCloud: -g.bettercloud.com -app.bettercloud.com -api.bettercloud.com	BetterCloud optimizes management of cloud applications and secures the user interactions	Google Cloud Platform / Google proprietary Linux, Ubuntu, Distroless	Servers reside in Google data centers within the United States.

Personnel involved in the operation and use of the system are:

- Executive Management – responsible for the establishment and achievement of objectives for the BetterCloud application
- IT & Security – responsibilities include, but are not limited to, the following:
  - Provisioning, management, and configuration of employee devices
  - 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
- Service Delivery – responsibilities include, but are 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
- Product Management, Software Engineering and Quality Assurance – responsible for designing, coding, testing, and implementing BetterCloud applications into the Google Cloud Platform
- People & Culture – responsible for the onboarding, management, and offboarding of the workforce that develops, implements, and supports the BetterCloud application
- Customer Experience – responsible for the implementation, support, and successful use of the BetterCloud application by 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. Topics covered in the detailed policies and procedure include the following categories of functions: information security, physical access, business continuity, risk management, human resources security, acceptable use, data classification, data backup and retention, third-party procurement, device management, change management, confidential data, systems access, password management, network security, messaging security, and incident management.

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.

Access, Authentication and Authorization

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 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.

Logical access to the BetterCloud application production environment is limited to authorized personnel based on job responsibility and areas of oversight. Access to the application secret keys is restricted to user accounts accessible by authorized personnel.

Access Requests and Access Revocation

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 managers prior to the security team granting access to the application or production resource. Administrators remove (de-provision) user account privileges assigned to terminated employees.

The security team performs a review of production user access annually. 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.

Change Management

The goal of the change management process is to manage all changes to the BetterCloud application and platform with minimum disruptions, risk, and complexity necessary to achieve business objectives. This includes ensuring that all code changes are prioritized in the project management system, managed, and authorized in the version control system, and completed with documented test plans, test results, version information, and rollback plans.

Engineering and Product Management teams conduct weekly meetings to discuss ongoing and upcoming projects. Project status updates are tracked by the Product Operations team.

Change requests 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 manages the change analysis, development, testing, rollback plan, and release.

Management utilizes an automated workflow and ticketing system (Jira) to systematically enforce the process flow and document changes made to the production application. This is performed for the following change types:

- New features, standard changes and bug fixes follow a routine change control process for production application source code and infrastructure
- Emergency changes (“blocker fixes”) have a higher priority and may follow an expedited change control process

New Features, Standard Changes and Bug Fixes

Product Managers prioritize Jira tickets for Software Engineering work on new features, standard changes, and bug fixes. Engineering teams assign tickets to developers.

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 their own internal code testing then submits the code for independent review and approval.

After the technical review is complete, approved code changes are merged into a secured branch of the version control system, the code is built and deployed for quality assurance testing using the CI/CD tool. The developer and tester cannot be the same individual.

The quality assurance testing verifies changes and either promotes them to the next environment for testing until they reach production or rejects the change and returns it to the assigned Developer’s queue for additional work and review. Releases to production are documented with a version number and release date and the ticket is closed.

The use of the CI/CD tool is systematically logged and captures the date and time stamp of each deployment, the specific user account responsible, and the build package/version. Developers do not have the ability to approve their own changes or implement their own changes into the production environment without independent review.

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.

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.

System Monitoring

The Site Reliability Engineering 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. A web application firewall is utilized to analyze, report, and protect the production environment from network events such as intrusions and denial-of-service attacks. A performance monitoring tool is utilized to monitor the system up-time and performance.

Anti-Malware

To protect the production environment from malicious software, a cloud-based next generation antivirus system is configured to protect registered workstations. The software is configured to perform updates on the virus definitions and scan the registered clients on-demand.

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 all customer data received from SaaS providers to be confidential. Examples of confidential customer data include customer usernames, sharing statuses and any other named information needed for the BetterCloud application to provide SaaS operations management services. 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, application and infrastructure source code and repositories stored in the version control system, and infrastructure images in the Google Container Registry.

The secret keys used to authenticate the BetterCloud application with connected SaaS providers are considered Restricted data, with access limited to the Security and Site Reliability Engineers.

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
• Application and infrastructure source code • Infrastructure system images	Used internally to build and implement application and infrastructure changes to the production environment.	Confidential

Data Used and Supported by the System		
Data Description	**Data Reporting**	**Classification**
Secret keys	Used to authenticate to connected SaaS applications and uniquely identify, validate, and authorize the application for SaaS operations management.	Confidential

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.	CC6.4 CC6.5
Google is responsible for enforcing encryption on production infrastructure that transmits to other public networks.	CC6.6 CC6.7
Google is responsible for implementing procedures to protect production infrastructure from computer viruses, malicious code, and unauthorized software.	CC6.8
Google is responsible for maintaining system components including configurations for the production infrastructure.	CC8.1