BetterCloud WHITEPAPER

Trust and Security

MAY 2023

Introduction

Our customers include healthcare organizations, government agencies, financial services companies, and Fortune 500 companies who trust us with helping them streamline and automate critical work that boosts operational efficiency, preempts threats and keeps their data safe. We work hard to ingrain security, privacy and trust into everything we do to help ensure that your business operates smoothly while remaining protected.

At BetterCloud, we take an agile approach to managing risk and implementing compliance, security and privacy throughout our company. BetterCloud ensures security and privacy needs are considered early and continuously, starting with executive leadership, to ensure that security and privacy are handled both as a strategic function and as a differentiator for our customers.

We are committed to providing transparency into our security, privacy, and trust programs to earn and keep your confidence in us. What follows is an overview of the processes and technologies we employ to provide the assurance you and your business need.

The BetterCloud Platform

BetterCloud is the market-leading SaaS management platform, enabling IT teams to automate onboarding, offboarding and mid-lifecycle changes, SaaS application access and entitlements, and security policies in a multi-SaaS environment. Our platform only connects to the SaaS apps that your team decides to connect to our platform via our integrations or custom APIs. We only ingest data based on the permissions set by your team. Your IT and/or security teams are the users of our platform and they configure the application to automate certain workflows, actions, and alerts based on the needs of your company. For example, if a new employee joins the sales team, they may need to be provisioned with accounts for Google Workspace, join the Slack channels, and access the SaaS apps used by their team. If an employee leaves your company, your team will want to ensure they are deprovisioned promptly and correctly, and their files are transferred to their manager. BetterCloud helps with all these actions and others which are initiated and configured by your IT and/or security teams in our platform.

To learn more about BetterCloud's products, please visit:
https://www.bettercloud.com/product/

BetterCloud

Compliance

Certification and Attestations

BetterCloud has been certified to the ISO/IEC 27001:2013 standard. The compliance certificate can be viewed and downloaded here, and can be verified in Schellman's directory here.

BetterCloud maintains an annual SOC 2 Type 2 report, performed by an independent third party, in order to attest that our platform and related operational processes meets the rigorous requirements for security and confidentiality as defined by AICPA.

We also maintain an annual SOC 3 report, which provides a summary overview of the detailed assessment performed in our SOC 2 Type 2 report, which anyone can download here.

Security

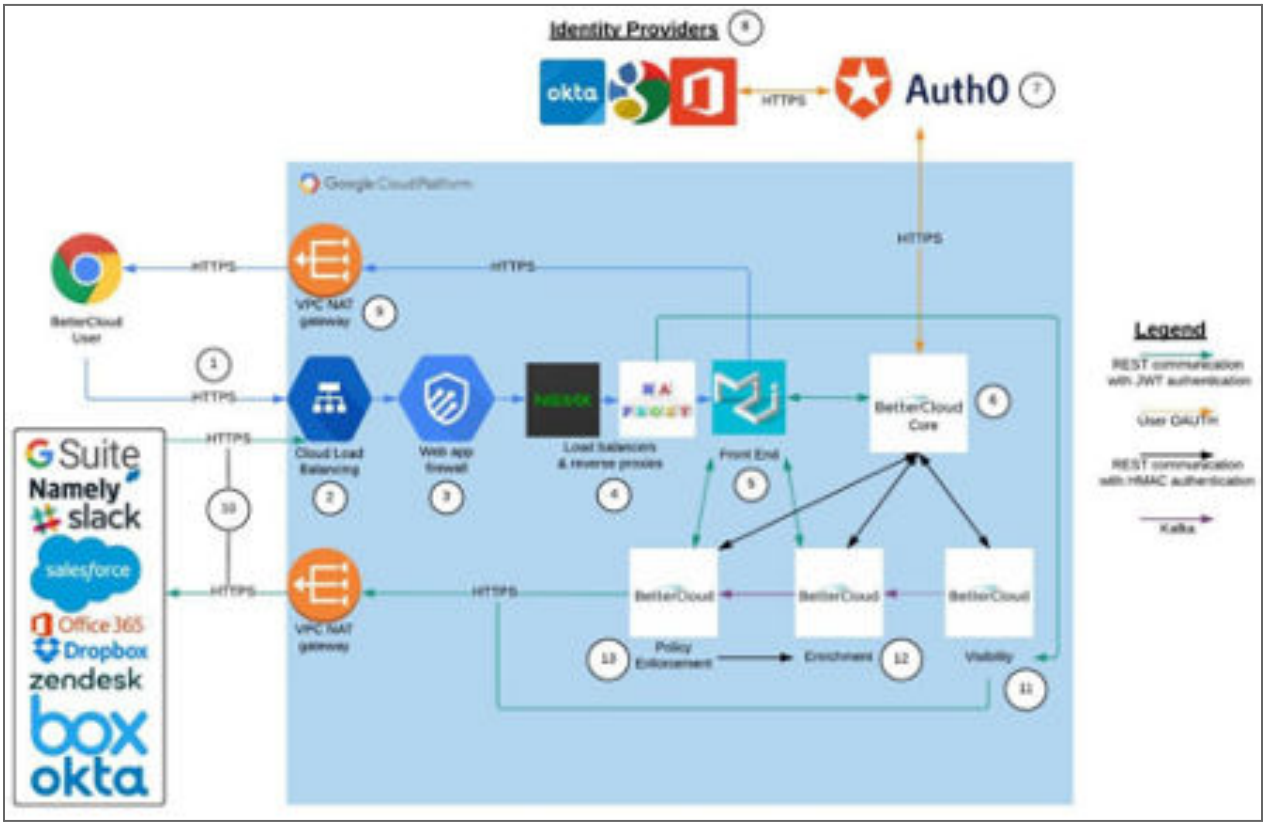
Infrastructure Security

The BetterCloud platform is built and hosted exclusively on Google Cloud Platform (GCP). This enables us to take advantage of Google's world-class physical and infrastructure security, which includes cameras, biometric access, and other controls for physical access. GCP's infrastructure also includes numerous safeguards to prevent services from breaking isolation, including the use of sandboxing, encryption, and other techniques. For more information on Google's physical and infrastructure security, please view Google's security whitepaper.

Additionally, we recognize that strong security within an infrastructure-as-a-service (IaaS) relies on a shared responsibility model, which is why we also leverage numerous other best practices to protect our platform and our customers. These practices include using hardened machine images for our virtualized servers, with secure container images for containerization, regular vulnerability scanning of our environment, and other measures. For more information regarding Google Cloud Platform Security, please view Google's own Security and Privacy Documentation: https://cloud.google.com/security/.

BetterCloud Architecture

Our application architecture, at a high-level, is illustrated and described below. We provide this level of transparency in an effort to further assure our customers and prospective customers that our platform is designed and deployed with security in mind.



Data flows are generally restricted using Google Compute Engine (GCE) firewalls and supplemented by other technologies illustrated in the diagram, such as NGINX and HAProxy routing rules and the VPC NAT gateway firewall. In GCE, data flows are dropped unless explicitly permitted by a rule. We leverage the default encryption-at-rest provided by GCP, which protects the data on disk with AES-256 or AES-128 encryption. Additional detail below.

1. All communication between the user's web browser and our platform is secured with HTTPS using TLS v1.2 or higher. Users can log into the application with identities provided by Google, Microsoft Office 365, or Okta.

2. All incoming traffic to our platform goes through the GCP front-end load balancer. Cloud Load Balancing is built on the same front-end serving infrastructure that

powers Google. It supports 1 million+ queries per second with consistent high performance and low latency. Traffic enters Cloud Load Balancing through 80+ distinct global load balancing locations, maximizing the distance traveled on Google's fast private network backbone.

3. All incoming traffic to the BetterCloud application goes through Google Cloud Armor, BetterCloud's web application firewall (WAF). The WAF protects data flows into the BetterCloud application by only allowing traffic from authorized sources. The WAF also blocks cross-site scripting and SQL injection attacks.

4. All REST requests are passed through a couple layers of load balancers and reverse proxies using Google Cloud Load Balancing, NGINX, and HAProxy.

5. Rest APIs enforce authentication with a custom BetterCloud JSON web token (JWT) for public endpoints.

6. The core microservices of our platform provide authentication, authorization, registration, customer information, and audit logs. Rest APIs use HMAC headers to enforce authentication for communication between internal endpoints. For user authentication, we use the OpenID Connect (OIDC) protocol, an extension of OAuth2, and Auth0 (an authentication and authorization service provider).

7. Our platform then informs Auth0 which identity provider (IdP) from step 1 should be used for authentication (this is done with Auth0 Custom Social Connections). Auth0 performs the OIDC handshake with the user's chosen IdP.

8. The IdP authenticates the user. If the authentication is successful, then an ID Token is provided to Auth0. Upon successful acquisition of the "ID Token," Auth0 executes a (configured) script, which a) parses the acquired ID Token, in order to extract user profile data; b) generates a new ID Token; and c) sends an authentication code back to BetterCloud.

9. After we use the acquired (short-lived, one-time-use) authentication code to request and validate the Auth0 ID Token and access token returned by the IdP, the Auth0 ID Token is parsed for user profile data and the BetterCloud application generates its own custom ID Token for the user (referred to as BC-JWT), which is signed with its own private key. From this point on, this BC-JWT is used to authenticate all the user's requests from their browser and doubles as the user's distributed session. Network

connections from internal hosts to external resources leave the environment via the NAT gateway, where all traffic is inspected.

10. Our platform uses OIDC to obtain the “access_token” needed to integrate with APIs provided by various SaaS applications. This token is then used as an authentication mechanism to make API calls against the respective SaaS provider. By using a full library of SaaS application APIs, we ingest all metadata for a customer’s connected SaaS applications into our centralized platform.

11. The BetterCloud microservices for visibility use the ingested metadata to provide clarity around user settings, data sharing, administrator privileges, and more. This enhanced visibility into the SaaS environment helps customers identify areas of concern that were previously impossible to see between multiple systems.

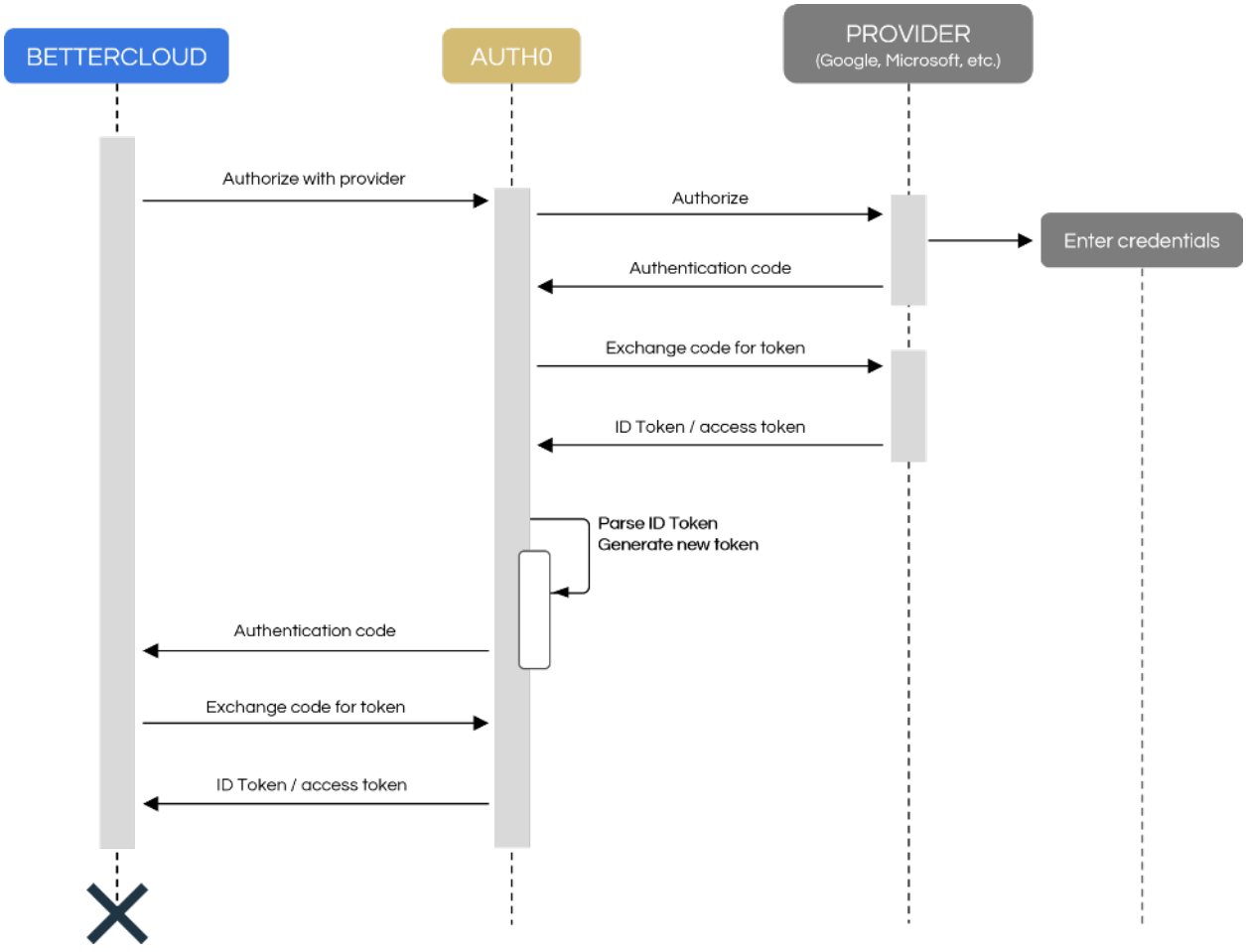
12. BetterCloud uses Confluent.io’s distribution of Kafka as well as Google PubSub for asynchronous messaging to the microservices that transform and enrich SaaS data across applications. Using an intelligent normalization model, BetterCloud produces a complete view of a file or user’s attributes across applications, unlocking contextual information that cannot be found in any other system. The enhanced context makes it quick and easy to respond to one-off issues and enforce policies.

13. We continuously monitor your SaaS applications for changes, flag policy violations as they happen, and automatically run a series of administrator actions when a user, setting, or file violates a company policy. One-off administrator actions and on-demand workflows enable teams to automate routine tasks. Our policy enforcement microservices leverage Rest APIs for synchronous communication with the enrichment microservices.

Platform Security

Authentication

Our Platform exclusively leverages single sign-on (SSO) technologies for authentication, meaning that we never create, give, or store passwords for our customers. By leveraging the OAuth 2.0 open standard, customers can confidently rely on their own identity providers (i.e. G Suite, Microsoft Azure AD, or Okta) and federation technologies to obtain OAuth tokens used to authenticate into our service. User access tokens are never stored by BetterCloud.



The diagram above illustrates how we use OpenID Connect (OIDC) via Auth0 to authenticate customers to our service and to the SaaS applications they integrate with us.

1. BetterCloud tells Auth0 which one of the (preconfigured) providers should be used for authentication (this is done with Auth0 Custom Social Connections).

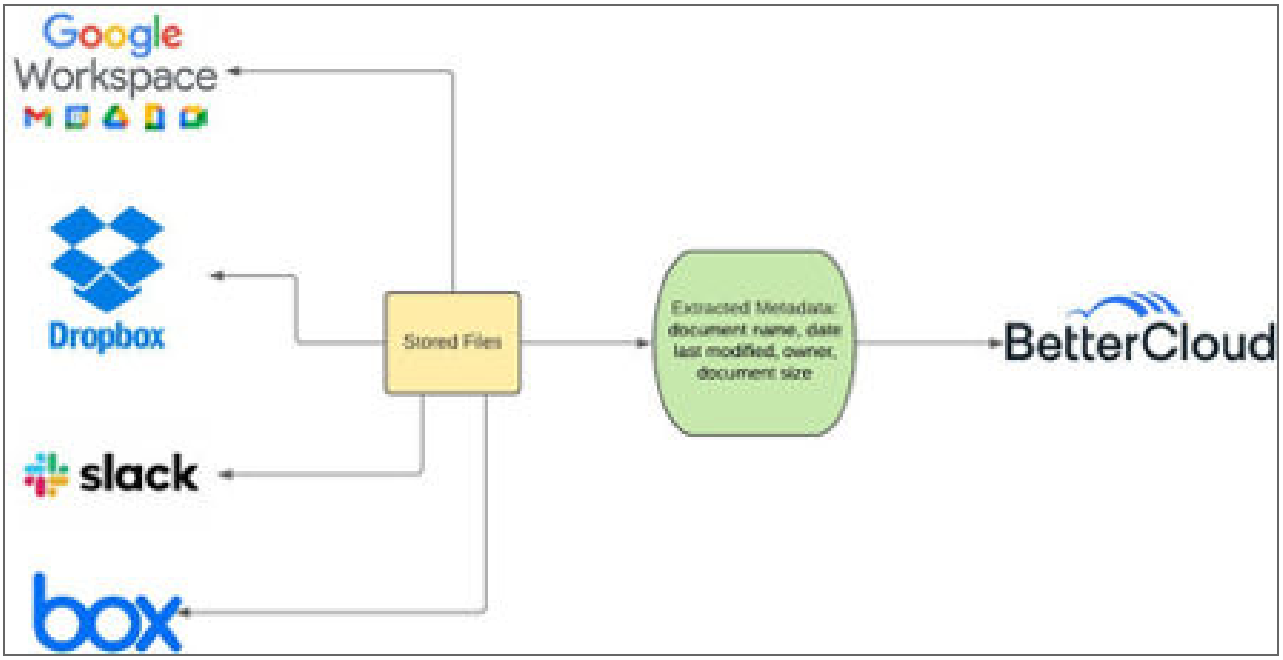
2. Auth0 performs the OIDC handshake with the respective Identity Provider (IdP).
3. Upon successful acquisition of the "ID Token," Auth0 executes a (configured) script, which a) parses the acquired ID Token, in order to extract user profile data; b) generates a new ID Token; and c) sends an authentication code back to BetterCloud.
4. BetterCloud then uses the acquired (short-lived, one-time-use) authentication code to request the newly generated ID Token and access token returned by the IdP.
5. Finally, BetterCloud validates the signature on the ID Token, parses it for the user profile data, and generates its own custom ID Token (referred to as BC-JWT), which is signed with its own private key.

We use a customized JWT (BetterCloud JSON Web Token or BC-JWT), rather than JWTs offered by Auth0, to provide more flexibility within our microservices architecture, while also enabling us to enhance security by customizing the JWT for each customer/tenant in our Platform. Additionally, this design helps insulate our Platform from potential vulnerabilities involving Auth0. As a result, we routinely have this portion of our architecture evaluated for security vulnerabilities or penetration tested by internal and external parties.

Customer Metadata

It is crucial for security and compliance professionals to understand the nature of data that we store and process in our service, which comprises mainly of metadata related to user objects, group objects, and documents. Our service works by using APIs to access certain metadata for each SaaS application that our customers connect to our platform. These APIs can access data for users, user email settings, groups, organizational units, contacts, calendars, calendar resources, documents, domain settings, and third-party application scope approvals.

Our platform allows our customers to scan documents and files in cloud systems, such as Google Drive, Box, Slack, and Dropbox for certain attributes. However, we never store the content of those searches. In these instances, we only store the metadata related to these documents (e.g., document name, date last modified, owner, document size) for actions by an administrator or an automated workflow or process.



Data Security: Secure Internet Connectivity (HTTPS)

In-line with today's modern industry standards, all BetterCloud externally-facing services use HTTPS TLS version 1.2 or higher to ensure encryption in transit of all customer information, whether that connection is established from a customer's local web browser, or an API endpoint at one of the many SaaS solutions with which we integrate.

Secrets Management

BetterCloud's Platform API provides our customers with the ability to store secrets, such as API keys needed to make web calls or passwords to third-party services in the application, in our service (via our Secret Store) when writing scripts and webhooks, ensuring customers never have to store sensitive credentials in scripts or code. We store and protect these secrets using HashiCorp Vault (https://www.vaultproject.io/). Secrets stored in our Vault environment are protected using AES-256 encryption, with 96-bit nonces which are randomly generated for each encrypted secret. Access to all customer keys is highly restricted, logged, and monitored for suspicious activity.

Corporate Security

Incident Management & Threat Detection

BetterCloud has in place a security incident response plan that includes procedures to be followed in the event of any unauthorized disclosure of customer data by BetterCloud or its agents. Once a potential incident has been identified, BetterCloud shifts operations into an incident investigation and then incident response posture. Incident management also includes processes to assess effectiveness of resolutions and after action reviews to mitigate root causes and increase efficacy.

Supply-Chain/Vendor Management

Our vendor management policy involves assessing and approving our vendors based on a set of criteria. Before onboarding new vendors, we take the time to comprehend their service delivery processes and perform risk assessments. To maintain our security posture, we establish agreements with vendors that require them to adhere to confidentiality, availability, and integrity commitments we have made to our customers. We also conduct regular reviews of their controls to ensure the effective operation of their processes and security measures.

More specifically, the trust team completes a risk assessment of all vendors based on the nature of the services and reviews the vendor's security and compliance audit documentation, such as a SOC 2 report and/or ISO 27001 certification, prior to approval and implementation. The trust team works closely with the vendor, where needed, to resolve any outstanding issues.

Personnel Security

Confidentiality Obligations: At the time of hire, BetterCloud mandates that all personnel acknowledge in writing, via a confidentiality agreement, their commitment to safeguard all customer data continuously.

Background Checks: Our goal is to recruit individuals who will contribute to the development of our security-focused culture. As part of this effort, we conduct background checks on all new hires in compliance with applicable local laws. Depending on the position, the background checks may entail verifying criminal history, education,

employment, and credit records. These checks help us in the process of hiring people who will positively impact the security-oriented culture we have established.

Security, Privacy and Phishing Training: Each new employee undergoes mandatory security awareness and policy, training and privacy training when they start with us. We supplement this each year with frequent targeted phishing simulation exercises, trust and security education and awareness for all employees, and other activities to ensure that our employees remain sufficiently educated on cybersecurity issues and threats.

Identity and Access Controls: BetterCloud has implemented policies, procedures, and logical controls to restrict access to its information systems and facilities to only authorized individuals. These measures are designed to prevent unauthorized personnel and others from gaining access and to promptly revoke access when there is a change in job responsibilities or job status.

BetterCloud implements controls to ensure that access to customer data is restricted to only those personnel who have a genuine need-to-know. These measures are based on the principle of least privilege to ensure that only authorized individuals are granted access to customer data. Additionally, unique user identifiers are required to identify BetterCloud personnel to whom they are assigned, and shared or group User IDs are not permitted for personnel access to customer data. Additionally, BetterCloud conducts periodic access reviews to ensure that access to customer data is only available to those BetterCloud personnel that still require it.

Software Development Security

Software development for our platform undergoes numerous reviews to ensure that security, trust, and privacy are embedded into every release — from ideation, to deployment into production, to ongoing operations — to ensure our platform is defended against attacks. Some highlights of our software security program, at each phase of our secure development lifecycle (SDLC) are noted below.

Product Management

During the conceptualization and roadmapping phases of product development, we take steps to ensure that planned new features do not create unnecessary privacy implications for our customers, while also determining the appropriate product security touchpoints to be embedded into each new feature.

Requirements & Analysis

In addition to providing effective security features and hardening requirements in line with best practices, our security and trust teams participate in the requirements development process by helping our business analysts develop both use and abuse cases for security and privacy. This helps ensure that each aspect of our platform is designed to not only function as designed, but also be resilient against what it should never be able to do.

Design & Implementation

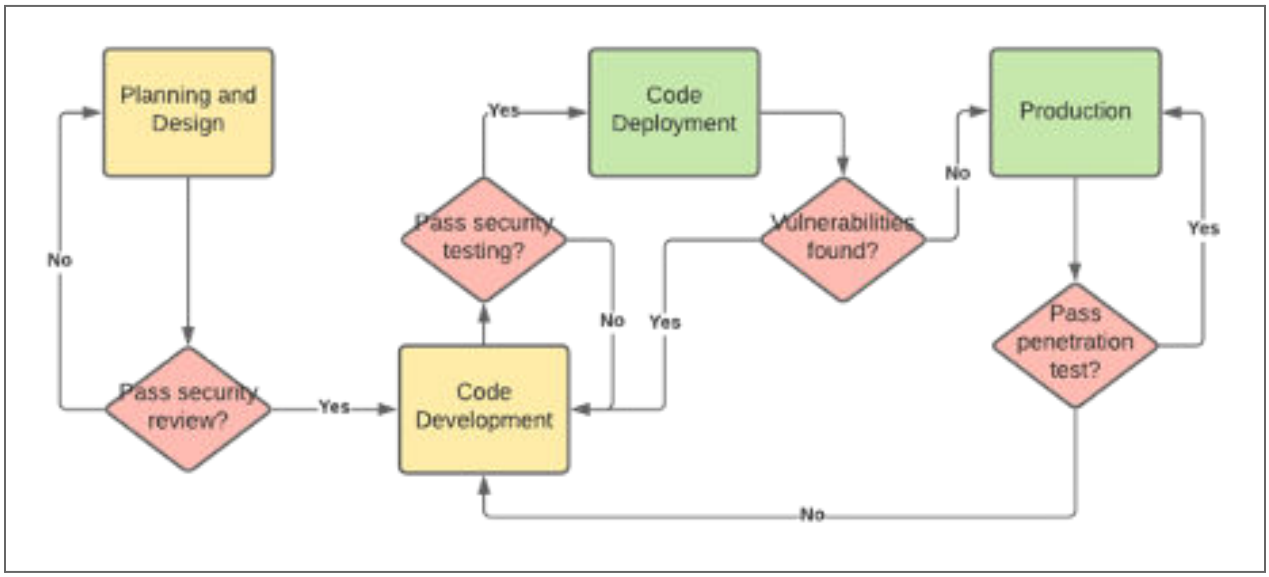
Security and privacy design reviews include both architectural and individual component evaluations, with the goal of reducing BetterCloud's attack surface. Proper error handling, avoiding dangerous code methods, encryption, and input validation are all included to ensure that the fundamentals of good multi-level security are in place. In addition to using static analysis tools (SAST and SCA) to evaluate our source code, all new source code undergoes periodic manual code reviews by the security team to provide an additional degree of assurance we are building a safe and trusted platform.

Penetration Testing & Vulnerability Scanning

Security testing is performed with every release, both in an automated and manual fashion. To maximize overall program security, testers focus on key components based on the risk analysis performed in the requirements phase. We also perform regular vulnerability

scanning, as well as hire independent penetration testers to regularly evaluate the design and implementation of our service.

The following diagram illustrates the various gates that application code must pass through before being merged into production.



Reliability

High Availability

BetterCloud has taken steps to ensure our application is online and accessible at all times. Using GCP, we have designed our platform to operate in a load-balanced fashion across three geographically distinct data centers, called Availability Zones in GCP's environment, to ensure our Platform provides both fault tolerance and load balancing to ensure high availability.

Backups & Recovery

To safeguard our ability to recover from a disaster impacting all three data centers, we backup our entire platform nightly so that we can recover the system quickly, if needed. All of our application, database, and other system backups are always encrypted at rest and promptly replicated to geographically distributed data centers.

Privacy

Data Processing Addendum: GDPR and UK Privacy Laws

Our DPA contains the standard contractual clauses and the UK Addendum to ensure all the necessary GDPR requirements and obligations are included. Here you can review and sign our DPA, and optionally receive a fully executed DPA via email.

CCPA/CPRA

BetterCloud does not sell any personal information it receives from its customers. See section 3.3 of our MSA for more on BetterCloud and CCPA compliance.

Personal Information

BetterCloud only processes certain personal information of the employees and other individuals with log-in access to the SaaS applications your IT or security team connects to BetterCloud. We refer to these people as “end user accounts.” BetterCloud needs to process such personal data to provide our services. The type of personal information we process from end user accounts to provide our services is generally limited to account profiles for those SaaS applications (such as a Gmail profile) which typically include first and last name, email address, work address, username, and IP address. For admins of our platform (your IT and security teams), we’ll also have access to the IP addresses they uses to log-in, admin activity in the platform (e.g., last sign in), helpdesk tickets submitted, and satisfaction data (e.g., a response to a question like “please rate your experience”).

Based on how your teams use our platform, we may also process metadata related to the documents and emails (e.g., Owner, Doc Title, Shared With) stored in the SaaS applications (e.g., Google Drive, Dropbox, Box) that are connected to our platform. Please note our access is based on the permissions set and controlled by your IT and security teams and we generally do not access the content of those documents or emails. Please note that we do not process sensitive information such as payment cards or protected health information.

Subprocessors

We engage a number of subprocessors that perform various functions for us in our provision of the services to you, such as hosting, security, support, notification, and

subscription management services. You can review a list of our current subprocessors and the services they provide here. Our relationship with each of them is subject to our third-party security management program to ensure they meet our rigorous security and privacy standards. Each of them has entered into a Data Protection Agreement ("DPA") with us including the applicable Standard Contractual Clauses under the GDPR/UK GDPR and CCPA/CPRA provisions. If and when we add new subprocessors, or replace them, you will be notified and would have an opportunity to object pursuant to the terms of your DPA provided you register for these updates here.

Transparency Report

Please note that BetterCloud has never been requested or subpoenaed to provide any customer data to any law enforcement, intelligence, security, government or regulatory agency from the US or elsewhere. You can also review our Transparency Report for more details. We regularly update this report to provide continued transparency about requests for user information.

Conclusion

Our customers rely on BetterCloud as a SaaS management and security partner they can trust with managing their SaaS-powered business operations. We continually strive to earn your trust through building an effective team, ensuring our platform is designed and built securely from the outset, leveraging technical safeguards in our infrastructure, and working with independent organizations to ensure our platform is safe and trusted. By employing an effective combination of people, processes, and technology, we continue to work tirelessly to ensure that our platform remains resilient against today's modern cyber threats.

Contact Us

If you have any questions about Trust & Security Whitepaper please contact us at Trust@BetterCloud.com.