BetterCloud WHITEPAPER

Security and Compliance

JULY 2019

Introduction

Thousands of customers, including healthcare organizations, government agencies, financial services companies, and Fortune 500's trust us with helping them manage and secure their businesses through our Platform. As a result, security & privacy aren't just "taken seriously" here at BetterCloud, we work hard to ingrain them into everything we do to help ensure that your business operates smoothly while remaining protected.

Despite this, security is a moving target, and companies who rest on their laurels tend to pay a steep price. At BetterCloud, this means having an agile approach to managing risk and implementing security & privacy throughout our company, "shifting left" to ensure security needs are considered early and often, and addressing it at an executive level to ensure that security & privacy are handled both as a strategic function and as a differentiator for our customers.

We are committed to providing transparency into our security program to gain and keep your trust. What follows is an overview of the people, processes, and technologies we employ to give you the assurance you and your business need to feel confident we can help you manage and secure your digital workplace.

Organization & People

BetterCloud's Security team has only one responsibility, and that's the security and privacy of our Platform and our customers. Our Security team, led by a Chief Information Security Officer (CISO), focuses on numerous capabilities, including Platform Security, Security Operations, Identity Management, and Security Compliance. The Security Team is led by our Chief Information Security Officer, who also oversees internal information technology, and reports directly to BetterCloud's CEO, to ensure that security remains a strategic issue across our entire business.

Additionally, all employees at BetterCloud undergo background checks to ensure that we hire professionals we can trust, and each new employee undergoes mandatory security awareness training when they start with us. We supplement that each year with targeted phishing simulation exercises, security education & awareness for all employees, and other activities to ensure that our employees remain sufficiently educated on cyber security issues and threats.

Infrastructure Security

Infrastructure

Our Platform is built and hosted exclusively on Google Cloud Platform (GCP). This allows 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.

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/.

High Availability

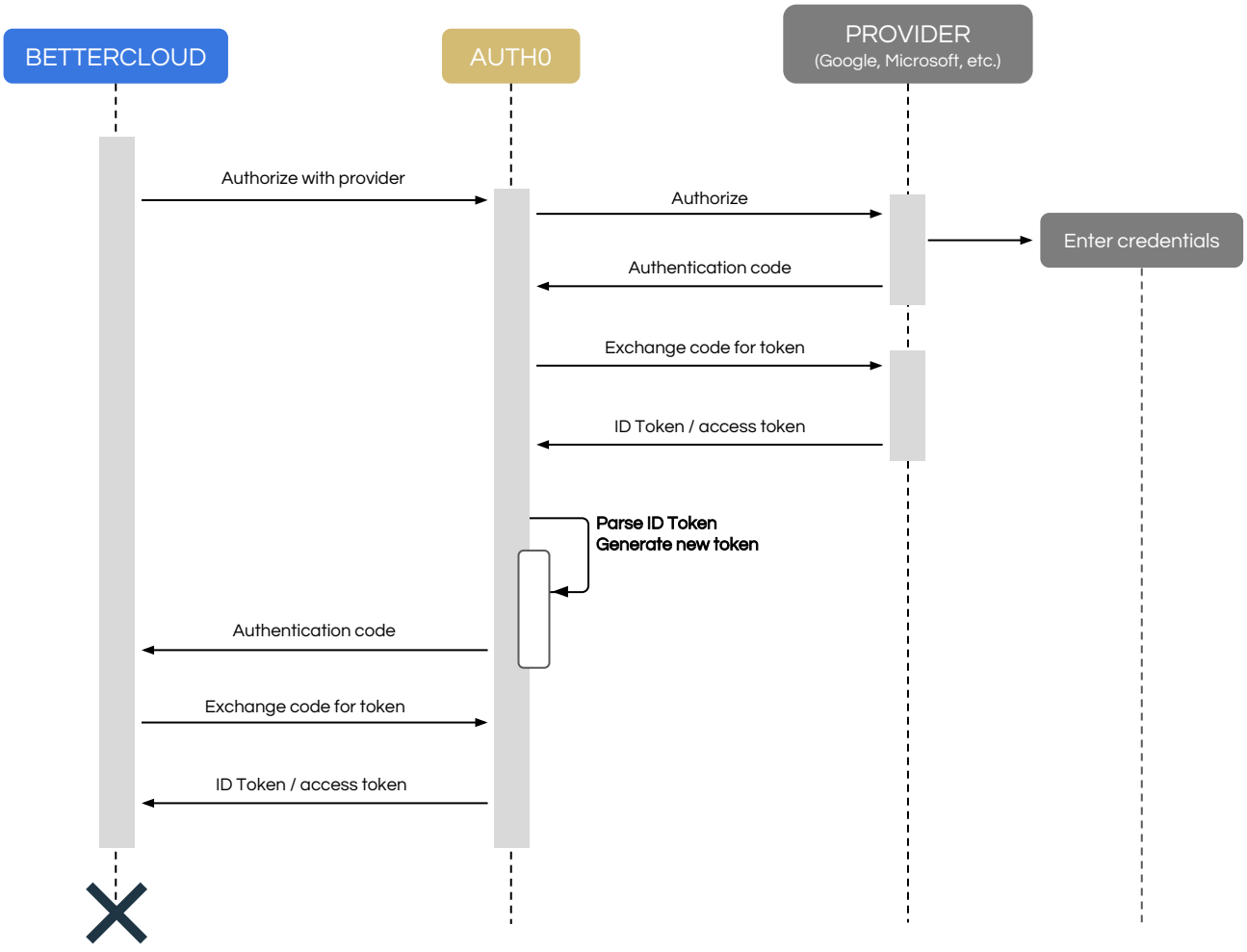
Establishing trust doesn't stop with ensuring we have a safe platform, we've also taken steps to keep our application online and accessible at all times. Using GCP, we have designed our Platform to operate in a load-balanced fashion across three geographically distinct data centers, called Availability Zones in GCP's environment, to ensure our Platform provides both fault tolerance and load balancing to ensure high availability.

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 whole 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.

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, which are encrypted at rest and never stored in plain text.



The diagram on the previous page 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

An important point for security and compliance professionals to understand about our service is the data elements that we store and process, which consists almost entirely of metadata on 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.

Secure Internet Connectivity (HTTPS)

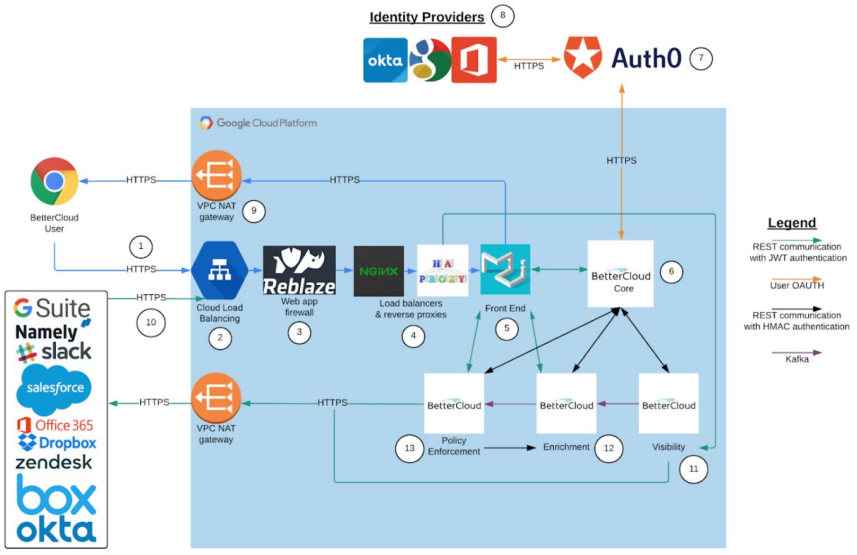
Inline with today's modern industry standards, all BetterCloud externally-facing services use HTTPS to ensure encryption in transit of all Customer information, whether that connection is established from a customer's local web browser, or an API endpoint at one of the many SaaS solutions with which we integrate. Wherever possible, we negotiate TLS at version 1.2, however we still support TLS 1.1 in certain cases to support compatibility with older operating systems and browsers.

Secrets Management

BetterCloud's Platform API allows our customers 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.

BetterCloud Architecture

Our application architecture, at a high-level, is illustrated and described below. We provide this relatively unusual 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.

1. All communication between the user's web browser and our platform is secured with HTTPS using TLS v1.1 or greater. 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 goes through our Reblaze web application firewalls. Reblaze protects data flows into our platform by only allowing legitimate traffic into a unique private cloud. The web application firewall blocks hostile Internet traffic such as malicious payloads, code and SQL injection, cross-site scripting, form manipulation, cookie and session poisoning, protocol exploits, and more.

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. *See Authentication in BetterCloud for more information.*

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 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.

Secure Development Lifecycle

Software development for our platform undergoes numerous reviews to ensure that security is 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 (SDL), include:

- **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 feature and hardening requirements in line with best practices, our security team participates in the requirements development process by helping our business analysts develop both use and abuse cases for security. This helps ensure that each aspect of our platform is designed to not only do what it's supposed to do, but also be resilient against what it should never be able to do.
- **Design & Implementation:** Security 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) to evaluate our source code, all new source code undergoes manual code reviews by the security team to provide an additional degree of assurance we are building a safe and trusted platform.

- **Testing:** 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.
- **Use of commercial and open source code:** All software and source code originating from a third party — from commercial off-the-shelf products (COTS) to open source — are kept secure through integrated processes throughout our SDL. Once approved by Architecture and Security, all third-party products must be obtained through approved and verified channels, with risk management and remediation progress tracked by our security team.

Security Assurance

We're committed to demonstrating to each of our customers that security is taken extremely seriously at BetterCloud, which is why, in addition to the above, we've sought out and maintained the following assessments, attestations, and certifications of our service.

BetterCloud maintains an annual SOC 2 Type 2 report, performed by an independent third party, in order to certify that our platform and related operational processes meets the rigorous requirements for security and confidentiality as defined by AICPA. We share this report upon request with customers and prospective customers under a non-disclosure agreement (NDA).

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 from our Security & Compliance page on our website.

BetterCloud also maintains an annual Privacy Shield certification, which is a worldwide benchmark that helps assert that an organization's privacy and data collection practices align appropriately with European regulatory requirements.

To learn more about Privacy Shield, visit www.privacyshield.gov.

As a Data Processor as defined by the European Union's (EU) General Data Protection Regulation (GDPR), we have comprehensively evaluated GDPR requirements and implemented numerous privacy and security practices to ensure we are meeting GDPR requirements. These practices include:

- Training employees on security and privacy practices
- Conducting privacy impact assessments
- Establishing Data Processing Addendums (DPAs) with all of our sub-processors
- Providing sufficient data transfer methods to our customers
- Maintaining records of processing activities

You can also view the GDPR FAQ on our Security & Compliance page and our Privacy Policy to learn more about how we meet existing GDPR obligations and better protect our customers' privacy.

The Cloud Security Alliance's (CSA) Security, Trust & Assurance Registry (STAR) is a free, publicly-accessible registry that offers a security assurance program for cloud services, helping users assess the security posture of the cloud providers they currently use or are considering using.

BetterCloud has achieved Level 1 status with the CSA STAR program. You can view our registry entry with the CSA STAR program, along with the results of our self-assessment and related supporting documentation, by visiting https://cloudsecurityalliance.org/star/registry/bettercloud/.

Conclusion

Our customers rely on us because they demand a SaaS management and security partner they can trust with managing their SaaS-powered business operations. Whether it's through building an effective team, ensuring our platform is designed and built securely from the outset, leveraging technical safeguards in our infrastructure, or working with independent organizations to ensure our platform is safe and trusted, security and privacy are more than just taken seriously at BetterCloud. 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.