BetterCloud WHITEPAPER

Security and Compliance

MARCH 2018

Introduction

BetterCloud empowers IT to define, remediate, and enforce management and security policies for SaaS applications. Every day, thousands of customers rely on BetterCloud to set up custom event detectors, audit activity, quickly take action, and fully automate policy remediation.

BetterCloud is headquartered in New York City with engineering offices in Atlanta, GA.

Application Security

Authentication

SSO

Usernames and passwords are never created, given, or stored by BetterCloud, as all user logins are verified using Single Sign-On. This creates an added level of security as well as a seamless integration between customers' SaaS applications and BetterCloud.

OAuth 2.0

The OAuth 2.0 open standard allows customers to authorize BetterCloud to access their SaaS application without sharing personal account credentials. This minimizes risk as customer passwords are never known, stored or shared with BetterCloud. OAuth tokens are encrypted at rest and not stored in plain text. Encryption keys are rotated at least annually.

Metadata

BetterCloud accesses API for: Users, User Email Settings, Groups, Organizational Units, Contacts, Calendar, Calendar Resources, Documents, Domain settings, and 3rd Party Application scope approvals. BetterCloud does not retain email or Slack messages. When interfacing with HR systems, BetterCloud does not retain social security numbers, family member information, or any other personal information that is not necessary for an IT admin to manage and secure their domain.

In the case of cloud documents, such Google Drive, OneDrive, Box, and Dropbox, the metadata is indexed by BetterCloud so that the customer can perform real-time searches, as real-time API calls are not always feasible. Metadata includes: Owner, Owned by OU, Doc Title, Shared With, Exposure Level, Last Updated, Doc Type, File Extension, Doc Size. The content of the documents is not stored.

Secure Browser Connections (HTTPS)

HTTPS provides a secure internet connection between the BetterCloud application, which runs on Google Cloud Platform, and a customer's local computer. This secure connection provides a bidirectional encryption of communications.

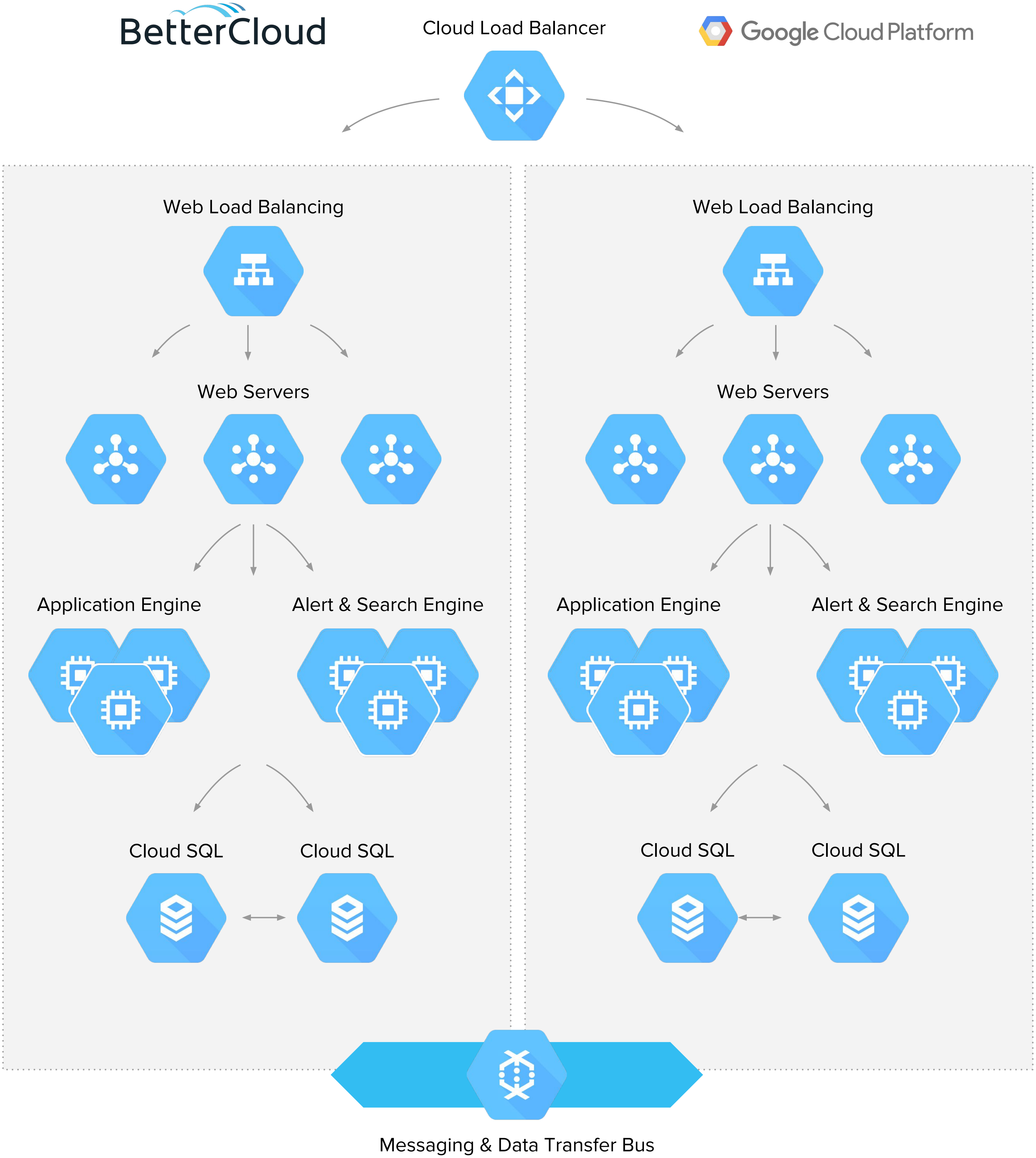
Uninstall

Uninstalling BetterCloud connections and authorizations will cut off all communication between the customer’s domain and BetterCloud for that connection. Customers can submit a request when they uninstall or follow the instructions in our privacy policy to have all of the metadata removed from the BetterCloud Data Store.

Security and the 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 the software development life cycle (SDLC). Once approved by architecture and security, all third party products must be obtained through approved and verified channels. These products then integrate completely through our software development life cycle, and are tested by static and dynamic application testing, as well as our internal and external penetration testing. Approved software products are inventoried and monitored for security vulnerability/CVE alerts, with risk management and remediation progress tracked by our security team.

BetterCloud Architecture



Hosting Security

Google Cloud Platform

BetterCloud is built and hosted exclusively on the Google Cloud Platform (GCP) platform. Thus, the physical securities of BetterCloud are equivalent to that of Google Cloud Platform, which Google uses to run G Suite as well. BetterCloud uses the Google Datastore, which is an object datastore that provides scalable storage, and other industry best practice databases that use cloud storage that is encrypted at rest by default.

For more information regarding Google Cloud Platform Security, please view Google's own Security and Privacy Documentation: https://cloud.google.com/security/.

High Availability

BetterCloud tracks uptime of the application using externally hosted commercial vendors. Our application run in three different Google Cloud Platform availability zone for high availability, and critical data is backed up for recovery in the case of unexpected failures.

Backups

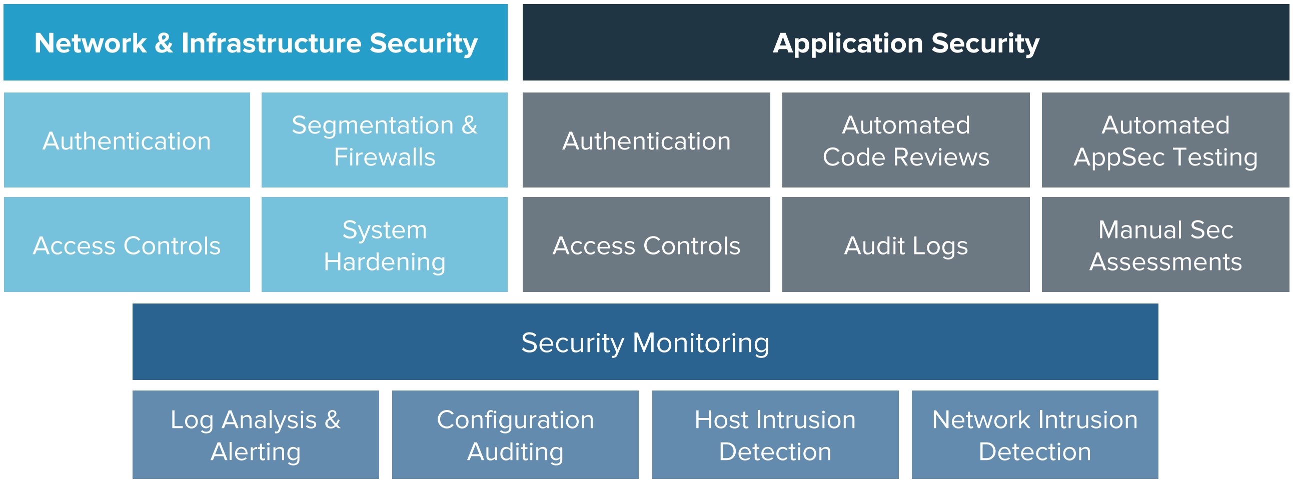
All data is actively stored across three availability zones and encrypted at rest. Database and search index backups are performed daily and instantly replicated to geographically distributed data centers.

Corporate Security

- **People:** A dedicated security team, including a senior officer in the company, is chartered with ensuring the security, confidentiality, and integrity of company and customer data. Employee desktops auto-lock after minutes of inactivity.

- **Process:** Industry-leading policies on security and privacy practices, aligned with both ISO 27000 and NIST-800 standards, ensure comprehensive risk management coverage.
- **Technology:** BetterCloud has a defense in-depth strategy, utilizing commercial and open source tools, to provide a multi-layered defense.
- **Education:** Regular and comprehensive security and privacy training is done at all levels of the company in order to ensure vigilance. All employees must go through an annual testing and certification process to ensure training effectiveness.
- **Restricted Access**: Access to all BetterCloud facilities is restricted, with facilities protected utilizing one of the most advanced authentication services available: Sequr. Compliance with corporate security policies is enforced through system software, and access to customer data is limited to only those with a need to know.
- **Assessments:** BetterCloud regularly conducts both internal and external vulnerability assessments, ranging from simulated phishing attacks to external penetration testing and application scanning.

Software Development Design and Life Cycle Focused Around Security



Network & Infrastructure Security

- Authentication
- Segmentation & Firewalls
- Access Controls
- System Hardening

Application Security

- Authentication
- Automated Code Reviews
- Automated AppSec Testing
- Access Controls
- Audit Logs
- Manual Sec Assessments

Security Monitoring

- Log Analysis & Alerting
- Configuration Auditing
- Host Intrusion Detection
- Network Intrusion Detection

BetterCloud's Security Architecture

- **Requirements/Analysis:** Close attention is given to how systems interoperate, ensuring projects start on a solid foundation. Business analysts write use cases outlining what systems should, and more importantly, should not do. Information security participates in this process to describe how a malicious user might interact with certain systems. Additionally, risk analysis is an essential part of the requirements phase. This helps teams understand the value of information and the potential implications of an exploit. This analysis identifies what business processes are necessary to help prevent and limit the impact of an unlikely compromise.

- **Design/Implementation:** Security design reviews include both architectural and individual component evaluations. These focus primarily on how to reduce BetterCloud's attack surface area. 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.

- **Testing phase:** 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.

- **Deployment:** Secure methods of deployment, including operating system maintenance, encrypted network connections, logging, and monitoring ensure that code is deployed with appropriate evidentiary support for forensics and incident response. All deployments are documented and audited to confirm that the changes deployed match the changes executed.

Our commitment to security is verified through internal and external third-party reviews by independent auditing firms. BetterCloud maintains annual SOC 2 Type 2 attestations and Privacy Shield certification.

A SOC 2 Type 2 attestation reports on controls relevant to security, availability, processing integrity, confidentiality or privacy. SOC 2 Type 2 is intended to meet the needs of a broad range of users that need detailed information and assurance about the controls at a service.

To learn more about SOC 2 Type 2, visit www.aicpa.org.

Privacy Shield certification ensures that BetterCloud's privacy and data collection practices are in line with European regulatory requirements.

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

BetterCloud is diligently working on and is on-track for GDPR compliance when it goes into effect in May 2018.