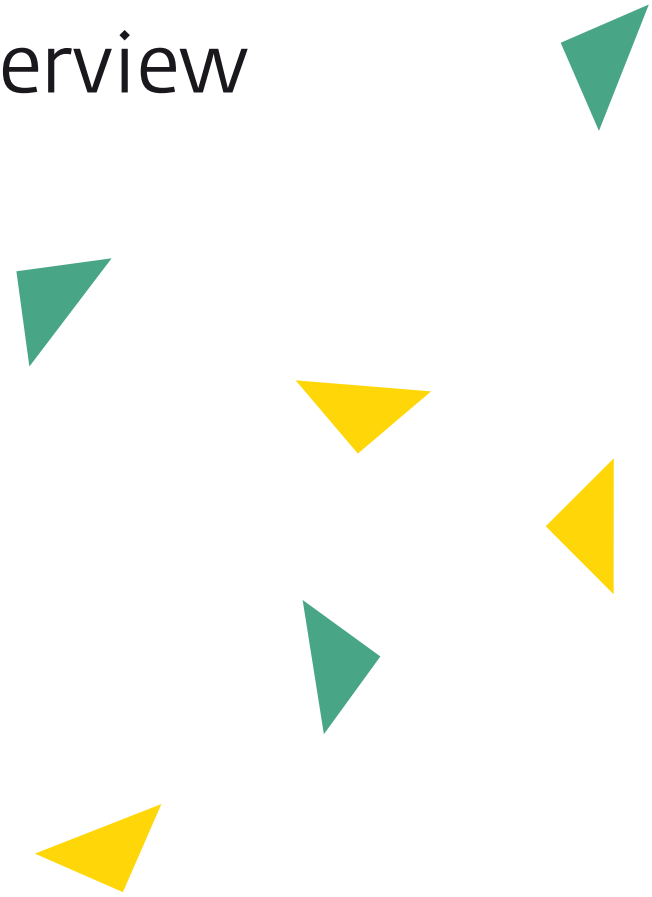
BeBanjo

# BeBanjo Infrastructure and Security Overview



Can you trust Software-as-a-Service (SaaS) to run your business? Is your data safe in the cloud? At BeBanjo, we firmly believe that SaaS delivers great benefits to our customers. Here are some of the things we do every day to provide SaaS with top security, performance and availability.

Can you trust Software-as-a-Service (SaaS) to run your business? Is your data safe in the cloud?

At BeBanjo, we firmly believe that SaaS delivers great benefits to our customers. It's easy to deploy to large teams in multiple locations, all users always work from the latest version of the software, our customers don't need to worry about hosting or maintenance…

We also recognise that business-critical applications require the highest level of security, availability and performance. BeBanjo products are aimed at enterprise customers and have been designed specifically with those concerns in mind.

Here are some of the things we do at BeBanjo every day to provide Software-as-a-Service (SaaS) with top security, performance and availability.

## Hosting

The BeBanjo applications are hosted on the Amazon Web Services (AWS) cloud computing platform. Some of the world's largest enterprises and most innovative start-ups trust AWS' cloud offering, *e.g.*, Adobe, Netflix, Pinterest… The AWS platform provides unrivalled scale, and sets the standards for cloud computing.

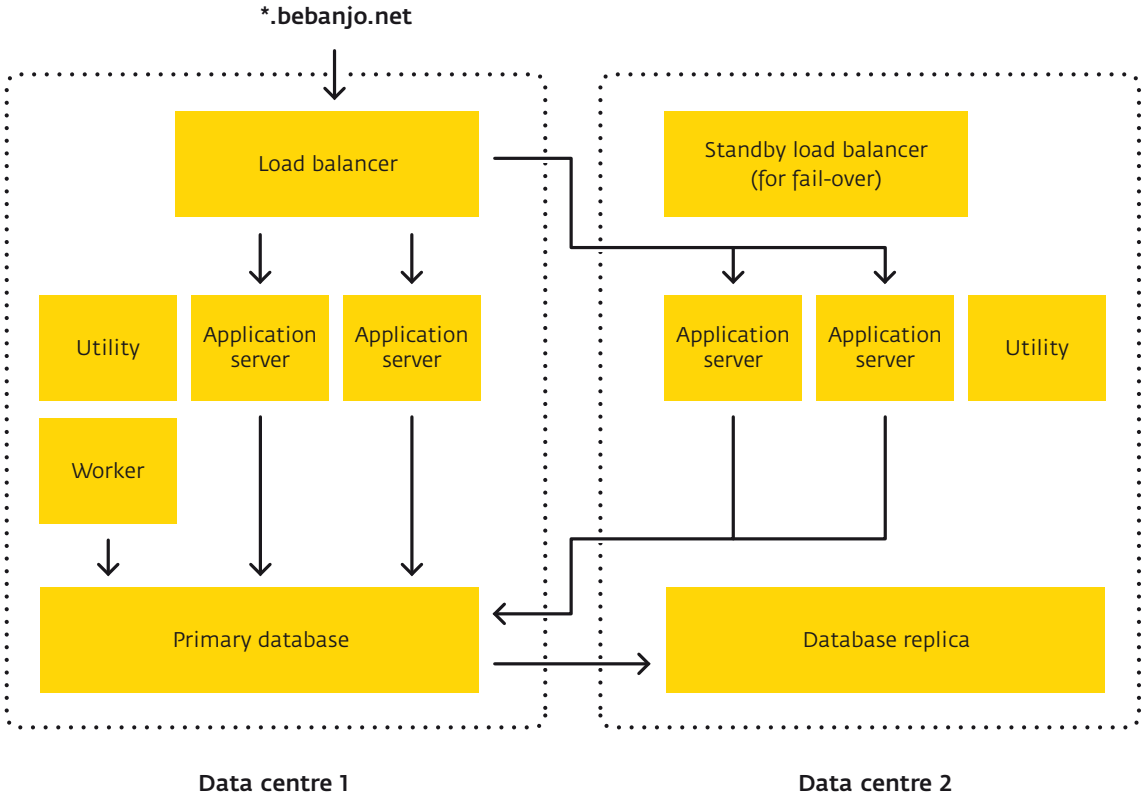
AWS manages data centres in multiple locations around the world. The BeBanjo applications are hosted in several AWS data centres in Ireland.

## Architecture

BeBanjo software has been developed for high-performance and high-availability, using a multi-tier architecture:

- Requests to the end-user interface or to the web service APIs are dispatched to application servers through a load balancer tier.
- Application servers in the application tier handle synchronous requests.
- Worker servers in the application tier handle background asynchronous jobs.
- Databases in the database tier persist the data for all servers. The database tier is replicated across multiple data centres.

In addition, a utility tier provides shared services to all servers (*e.g.*, messaging services, cacheing services…)




Logical view of BeBanjo's resilient and scalable infrastructure

## Performance and scalability

The architecture of the solution allows for high-performance and scalability:

- The computationally-expensive application tier is horizontally scalable. New application servers can be added to the pool of application servers, in order to handle the performance requirements of additional customers.
- The solution uses cacheing technology (*e.g.*, memcached) to maximise performance
- The architecture intentionally separates the handling of synchronous requests from background processing jobs, in order to always provide a highly-responsive user experience.
- The database tier allows for the deployment of database read replicas. This enables - for instance - intensive reporting tasks without affecting user experience.

## Environments

Distinct environments are provided, to carry out testing activities before any software is released to production:

- Production environment.
- Pre-production environment.
- Staging environment.

## Configuration and deployment

All our infrastructure configuration is managed with Chef, a Ruby-based configuration management engine, and stored under source control. All software is deployed to Virtual Machines (VMs), through reliable scripted deployment using Capistrano.

## Resilience and redundancy

There is no Single Point Of Failure (SPOF) in the production environment. All components (*e.g.*, load balancers, application servers, database servers...) are set-up using a redundant N+1 configuration, ensuring that failure of any one component cannot result in a failure of the solution.

## Disaster Recovery (DR)

A Disaster Recovery (DR) solution is in place. Following a catastrophic failure at the primary data centre, the production environment can resume servicing customers from a secondary data centre. The database tier being continuously replicated to the secondary data centre in near real-time, no data loss would be incurred in such an event.

## Application monitoring

The availability and performance of the BeBanjo products are constantly monitored using the following tools and services:

- Pingdom.
- PagerDuty.
- New Relic.
- Monit.
- Librato.
- AWS CloudWatch.

BeBanjo support staff are automatically alerted in case of any incident.

# Technology

Our technology stacks favours open-source components, and includes the following:

| Component | Role |
|---|---|
| Ubuntu Linux | Operating system |
| Apache | Web server |
| Phusion Passenger | Apache module for deploying Ruby apps |
| Ruby (Enterprise) | Development language |
| Ruby on Rails | Web application framework |
| MySQL | Database tier |
| Sphinx | Search / indexing engine |
| Memcached | In-memory cache |
| RabbitMQ | Message queue |
| JQuery | Core JavaScript library |
| Backbone | MVC framework for rich JavaScript apps |

# Service levels

Performance and availability of the BeBanjo applications are backed by a Service Level Agreement (SLA). The SLA defines measurable targets, reporting mechanisms, and service credits due by BeBanjo, should the targets not be met.

# Physical security

AWS ensures physical security of the data centres where the BeBanjo applications live. AWS has completed multiple SAS70 Type II audits. They publish a Service Organization Controls 1 (SOC 1) report, under both the SSAE 16 and the ISAE 3402 professional standards. In addition, they have achieved ISO 27001 certification.

The data centres use state-of-the art electronic surveillance, are staffed 24x7 by trained security guards, and access is authorised strictly on a least privileged basis.

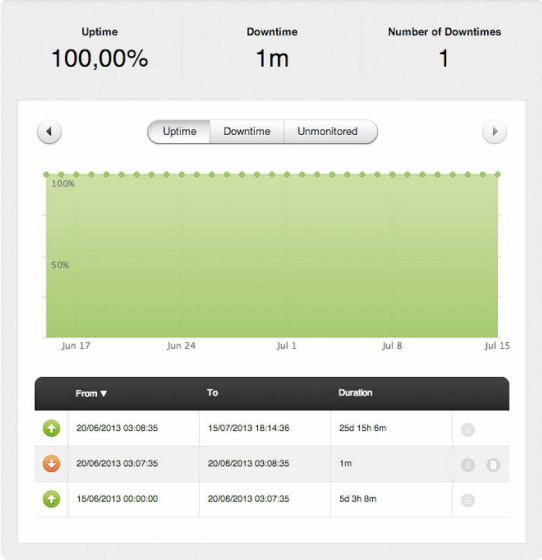
# Encryption

All communication with BeBanjo servers is encrypted using HTTPS. This applies to communication with both end-user browsers and with external systems integrated through the BeBanjo APIs. Any attempt to connect over plain HTTP is automatically redirected to a secure HTTPS connection.  Connections use TLS 1.1 and the AES_256_CBC 256-bit encryption algorithm, with SHA1 for message authentication and RSA as the key exchange mechanism.

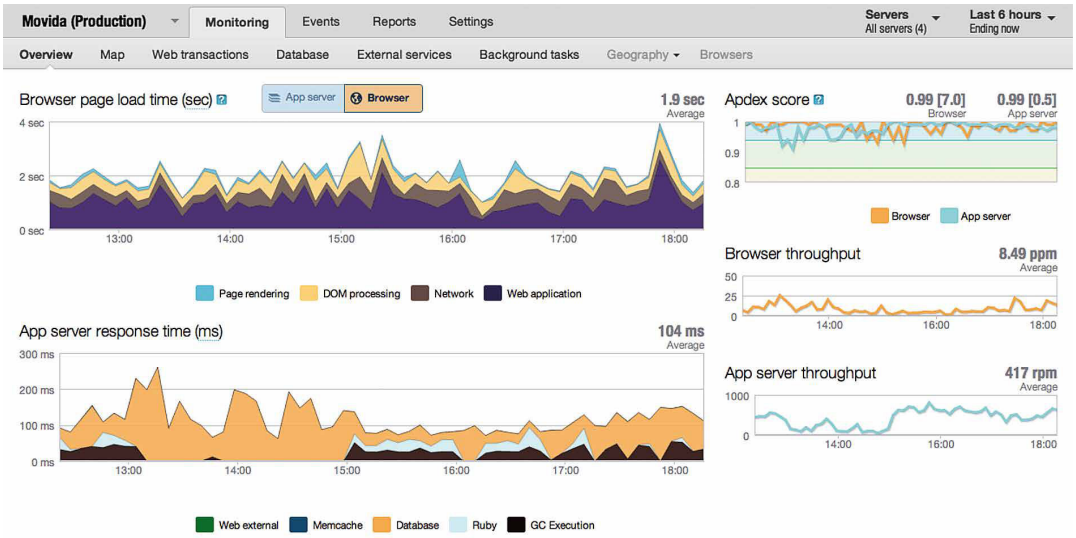
Your credentials and data are never transmitted in the clear over the public Internet.

All user passwords and system passwords are encrypted and stored as one-way hashes that cannot be decrypted, not even by BeBanjo.

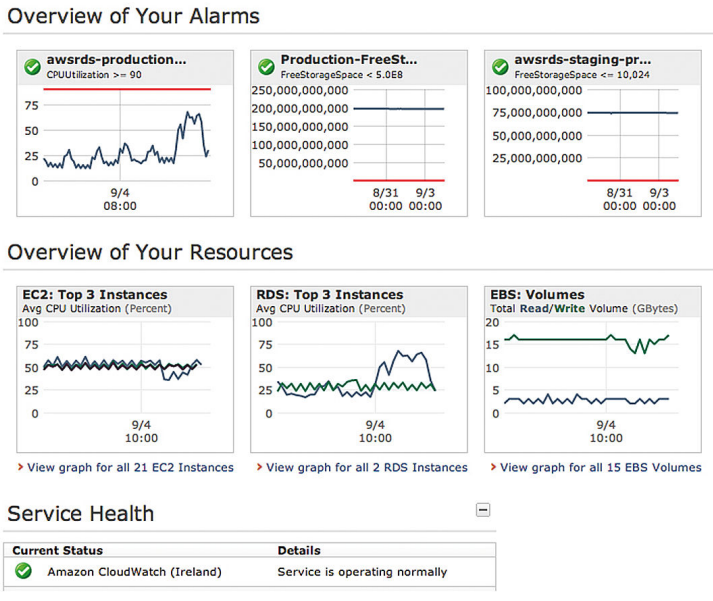
*Screengrab of Pingdom: monitoring application uptime*




*Screengrab of New Relic: monitoring application performance*




*Screengrab of AWS CloudWatch: monitoring infrastructure resources*



## Infrastructure-level security

The BeBanjo applications live behind firewalls configured to only allow traffic through authorised ports: notably port 443 for HTTPS, and port 80 for redirection to a secure HTTPS connection.

Connection to the servers for administration purposes is authenticated using RSA keys, that provide security superior to password authentication.

## Application-level security

Our development process has security at its heart. We code against application-level vulnerabilities such as SQL injections, by using:

- A modern web development framework (*i.e.*, Ruby on Rails) constantly updated by the community.
- Our own specific tools, *e.g.*, the automated test suite running on our Continuous Integration (CI) server.

In addition, any code change made by a developer is independently checked for quality and security, by another developer, prior to release.

## Data segregation

Our automated test suite constantly validates correct segregation of customer data. Whenever a change is made to any of the BeBanjo applications, and before any deployment can be envisaged, the automated test suite running on our Continuous Integration (CI) server checks for data segregation. It automatically validates that users (*e.g.*, a scheduler at Channel 5) can only access the data they are entitled to (*i.e.*, the Channel 5 schedules), and nothing else.

## Security monitoring

We constantly monitor independent security lists to be alerted of new vulnerabilities identified by the development community. Upon discovery of a new vulnerability that might affect our applications, we immediately deploy the relevant patch. Thanks to our redundant hosting infrastructure with no single point of failure, such emergency maintenance can usually be carried out without any interruption to the service. Centralised hosting of BeBanjo applications on a single - yet resilient - infrastructure means we can easily keep the platform up-to-date, and very rapidly close any newly found vulnerability.

## Third-party security audits

Some of our enterprise customers (*e.g.*, Channel 5, British Telecom) have stringent internal security processes. Before selecting our products they carried out due diligence of our security standards, sometimes using third-party tools or partners (*e.g.*, IBM Rational AppScan). We are always looking for ways to improve our solution, and we welcome a fresh pair of eyes on our security practices.

Arkena

**About BeBanjo**

We are an agile company of talented developers, designers and Video On-Demand specialists and we like to take good care of our customers; that is why we focus on making easy to use, easy to learn, collaborative tools that our users love. We make Video On-Demand operations easier, faster, better, so that our customers are free to concentrate on really running their Video On-Demand business. A wide range of companies successfully operating in the on-demand space already trust us. BeBanjo was founded in 2008 and is part of Arkena.