mediagenix | On-Demand

Technology & Security

You need confidence you can trust Mediagenix On-Demand products at the heart of your organisation. So here is a glimpse of what we do every day to architect, build, and support business critical applications.

API documentation [https://developers.bebanjo.com]

Enterprise-ready platform

Mediagenix On-Demand applications are hosted on a Virtual Private Cloud (VPC) 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., Netflix, Spotify, Twitch, Airbnb, and Slack. It provides unrivalled scale and sets the standards for cloud computing.

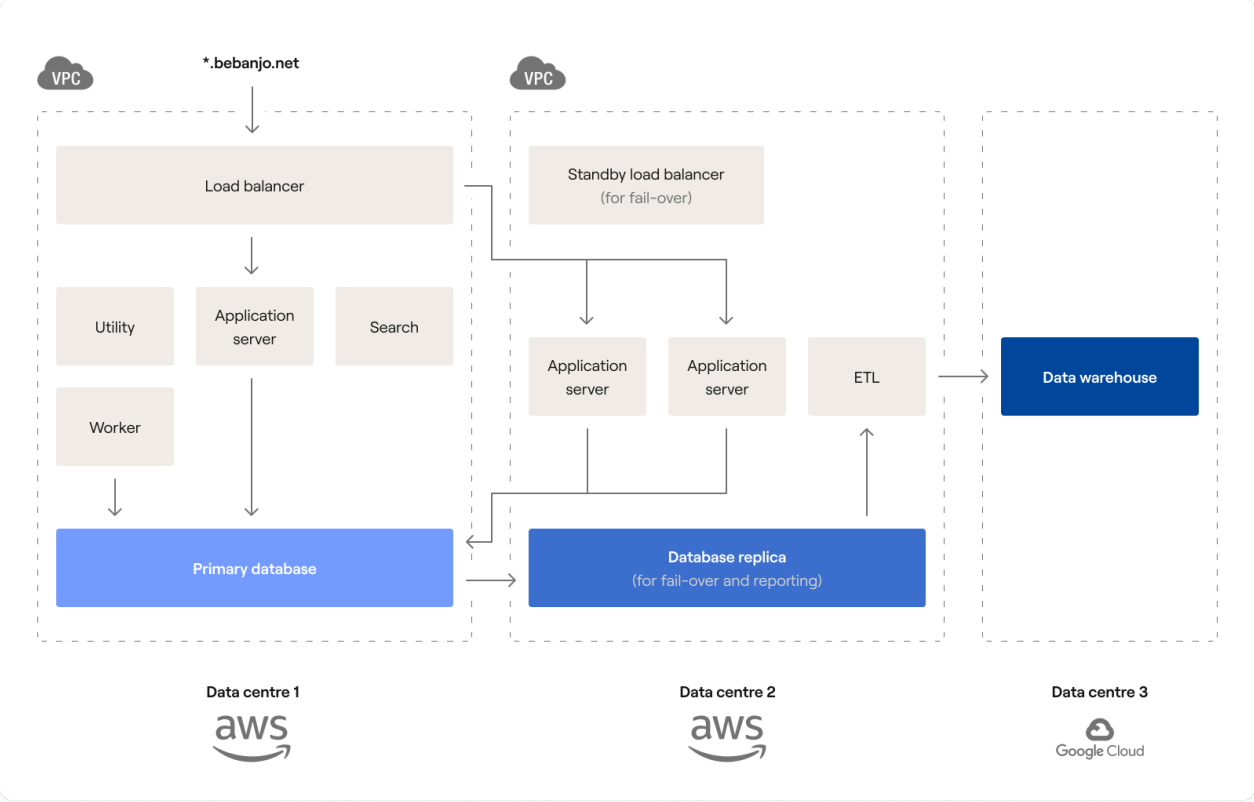
In addition to AWS, we use Google Cloud Platform to securely replicate data backups in multiple regions and to enable high-performance analytics using BigQuery.

High-performance multi-tier architecture

Mediagenix On-Demand software has been developed for high performance and high availability, using a multi-tier architecture made of:

- A load balancer tier that dynamically distributes requests to the application tier.

- An application tier that handles all synchronous UI and API requests. It is based on last-generation Intel Xeon Platinum® processors, and is horizontally scalable, i.e., new servers can be added on demand in order to handle the performance requirements of additional customers.
- A worker tier that handles all asynchronous work. Moving complex and long-running operations to the worker tier allows us to always provide a highly-responsive user experience.
- A database tier replicated across multiple data centres and made of a principal node that persists data for all servers and several read-only replicas that enable, among other things, extensive reporting capabilities without impacting the user experience.
- A search tier that provides fast and powerful searching capabilities to the application tier.
- A utility tier with shared services used across all infrastructure: caching, monitoring, SFTP, etc.



Environments

Several distinct environments are provided to carry out testing activities before any software is released to production:

- A Staging environment where we test the most recent developments and product features.

- A Preproduction environment running the same code as Production, where clients can perform any kind of integration testing prior to releasing their integrations.
- A Production environment. Where the real work happens!

Full redundancy

There is no Single Point Of Failure (SPOF) in the Production environment: all components (load balancers, application and worker servers, database and search servers) are set-up using a redundant N+1 configuration, ensuring that a failure in one component does not result in a failure of the solution.

Disaster Recovery

Following a catastrophic failure at the primary data centre in Ireland, the Production environment can resume operations from a secondary data centre in less than 24 hours. To test and further refine this Disaster Recovery process we run a complete internal simulation every year.

To avoid any data loss in such an event, the database is being continuously replicated to a secondary data centre in near real-time, and regular backups are stored encrypted on a different cloud provider and different regions.

Infrastructure-as-code

All our infrastructure configuration is managed with Chef, a Ruby-based configuration management engine, and with Terraform, a Go-based infrastructure-as-code software, and stored under source control with GitHub. Any change to the infrastructure configuration follows a strict development process and it gets peer-reviewed before being applied to Preproduction and Production.

A modern and robust software stack

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

Component	Role
• Ruby on Rails	• Web application framework
• MySQL	• Database
• Elasticsearch	• Search tier
• Memcached	• In-memory cache
• Sidekiq	• Background processing for Ruby
• Redis	• In-memory database
• Vue.js, Stimulus and Turbo	• JavaScript libraries to build rich user interfaces

We keep all software components regularly updated to ensure that all the latest security patches are applied.

A high bar for security

Exceptional physical security

AWS ensures physical security of the data centres where Mediagenix On-Demand applications live. AWS has completed multiple SAS70 Type II audits, and they publish a Service Organization Controls 1 (SOC 1) report, under both the SSAE 16 and the ISAE 3402 professional standards. In addition to that, they have earned an 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 your data is sent encrypted to Mediagenix On-Demand servers using TLS, and any attempt to connect over plain HTTP is automatically redirected to a secure HTTPS connection. Connections use TLS 1.2 and the AES 256-bit encryption algorithm, with SHA1 for message authentication and RSA as the key exchange mechanism. That means that neither your credentials nor any of your data are ever transmitted in the clear over the public internet.

User and system passwords are encrypted and stored as one-way hashes that cannot be decrypted, not even by Mediagenix On-Demand.

And even though the traffic between the applications and the database tier happens within a VPC that is secure by definition, all data is encrypted in transit and at rest.

Infrastructure-level security

Mediagenix On-Demand 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.

Password authentication is disabled across all infrastructure and remote access is only enabled via RSA keys through a single monitored access point. Administrative privileges are only granted to key senior people from the team, and follow strict processes to revoke permissions immediately when they are no longer required, e.g., after someone leaves the company.

Employees are trained on our strict security guidelines from their on-boarding, with policies being updated and reminded to the team regularly. Our practices range from secure credential management, to enabling multi-factor authentication in all external third party services, to workstation encryption to non-technical matters like phishing awareness.

Application-level security

- A modern, regularly updated and widely adopted web development framework: Ruby on Rails.
- A security advisor that automatically keeps track of vulnerabilities and important security upgrades for any library in use.
- An extensive automated test suite running on our Continuous Integration (CI) platform - based on Buildkite and hosted on Google Cloud.
- A strict development process where every change is peer-reviewed for quality and security 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 Mediagenix On-Demand 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.

Internal security assessments

We run automatic vulnerability assessments through AWS Inspector that help us improve the security and compliance of our VPC infrastructure, network and applications based on the highest standards. On top of that, we constantly monitor independent security lists to recognize new vulnerabilities identified by the development community. All findings are triaged and integrated into our regular workflow, and critical patches are applied immediately.

Having a redundant hosting infrastructure with no Single Point of Failure and highly automated deployment processes means that most emergency maintenances can usually be carried out without any interruption to the service. Centralised hosting of Mediagenix On-Demand 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.

External security audits and penetration tests

Most of our enterprise customers (e.g., WarnerMedia, BBC) have stringent internal security processes and before selecting our products they typically carry out due diligence of our security standards, sometimes using third-party tools or partners. We are always looking for ways to improve our solution, and we welcome a fresh pair of eyes on our security practices.

Application monitoring and incident management

All applications and systems are monitored in real-time by several tools and services that allow us to react, debug and identify availability and performance problems promptly.

We keep a dedicated Support team that gets alerted 24/7 in case of an event of any kind, and we maintain an extensive set of processes and workflows to mitigate and communicate incidents in a short time.

Service levels

Performance and availability of Mediagenix On-Demand applications are backed by a Service Level Agreement (SLA). The SLA defines measurable targets and reporting mechanisms, as well as service credits - not that you will receive those much!