Security and Reliability

KEEPING YOUR DATA SAFE

Table of Contents

Introduction from our CTO

If you are reading this document, then you are serious about security. So am I.

I recognise that breathe has both a legal and moral responsibility to ensure that we comply with data protection legislation and industry standards, but our company value is to “do the right thing” and that means not just ticking boxes to ensure your data is safe, but questioning everything we do with the intent of making it safer.

It’s not just the right thing to do, it’s good business sense. We survive by ensuring your data is safe. We thrive by constantly looking for ways to make it even safer.

It’s my intent that all common security questions should be answered here. However, I am always delighted to be contacted if you have questions that are not addressed in this document so please do not hesitate to drop me an email at security@breathehr.com.

Gareth Burrows
Chief Technical Officer, breatheHR

Physical Security

Where is my data held?

breatheHR utilises the world's most popular application hosting company, Amazon Web Services (AWS). Specifically, breathe utilises AWS EU-WEST region, with all our databases restricted to their IRELAND location. We have a failover site with AWS in FRANKFURT in Germany. This means we never store your data, or indeed any of our backups, outside the EU. Naturally, we keep abreast of changing political landscape and review this decision regularly.

How secure are the AWS datacentres?

The data centres are surrounded by three physical layers of security, all of which are under constant patrolling and monitoring by professional staff, and as battery of electronic intrusion detection systems. All visitors and contractors are required to present identification and are signed in and continually escorted by authorized staff. AWS only provides data centre access and information to employees and contractors who have a legitimate business need for such privileges. When an employee no longer has a business need for these privileges, his or her access is immediately revoked, even if they continue to be an employee of Amazon or Amazon Web Services. All physical access to data centre by AWS employees is logged and audited routinely.

Zone 1 (the outer perimeter) is a fence which is either crash-rated to prevent a vehicle from penetrating it or backed by the state of the art Jersey Barriers.

Zone 2 (electrical systems and generators) requires both a badge swipe and a personal pin to access. The only entrants are authorized engineers. Each door is under video surveillance with the feed monitored both locally and remotely. The space between perimeters is studded with internal trip-lights that are also monitored and managed around the clock.

Zone 3 (data servers and networking) requires another badge swipe and pin number for entry. They are also equipped with metal detectors. No transportable media (such as USB keys) are allowed in or out of the building.

How is the data centre protected against environmental issues?

Fire Detection and Suppression

Automatic fire detection and suppression equipment has been installed to reduce risk. The fire detection system utilizes smoke detection sensors in all data centre environments

Power

The electrical power systems are designed to be fully redundant and maintainable without impact to operations, 24 hours a day, and seven days a week. Uninterruptible Power Supply (UPS) units provide back-up power in the event of an electrical failure. Generators are used to provide back-up power for the entire facility.

Climate and Temperature

Climate control is required to maintain a constant operating temperature for servers and other hardware, which prevents overheating and reduces the possibility of service outages.

Storage Device Decommissioning

When a storage device has reached the end of its useful life, AWS procedures include a decommissioning process that is designed to prevent customer data from being exposed to unauthorized individuals. AWS uses the techniques detailed in the industry standard NIST 800-88 (“Guidelines for Media Sanitization”) as part of the decommissioning process.

Network Security

breatheHR electronic access to infrastructure and data

Access to the AWS network and resources is strictly controlled at breathe. The employee roles and access levels are defined below. All access to AWS infrastructure, codebase and client data is revoked at the termination of employment. Individual access to client data and AWS infrastructure is reviewed by a security team that meets monthly.

Role	Access	Requirements
CTO	Root Level to AWS	2 Factor authentication pin code > 16 characters in length
Developer	Access to AWS and Data only for Diagnostic, release or development	2 factor authentication for front end access Access to servers using SSH
Support	Access to client data	Pin code > 10 characters in length Specific active client authorisation

Marketing / Sales	Access to aggregated data only	Data provided by development team. No direct access

AWS access to network and data

AWS does not access or use breathe content for any purpose other than as legally required and to provide the AWS services to breathe and its end users. AWS never uses customer content or derives information from it for other purposes such as marketing or advertising.

The AWS Production network is segregated from the Amazon Corporate network and requires a separate set of credentials for logical access. The AWS Production network requires SSH public-key authentication through a bastion host.

AWS developers and administrators on the Amazon Corporate network who need to access AWS cloud components must explicitly request access through the AWS access management system. All requests are reviewed and approved by the appropriate owner or manager. User accounts are reviewed every 90 days; explicit re-approval is required or access to the resource is automatically revoked. Access is also automatically revoked when an employee's record is terminated in Amazon's Human Resources system. Windows and UNIX accounts are disabled and Amazon's permission management system removes the user from all systems.

Configuration of AWS network

breatheHR utilises an AWS VPC. This enables us to make use of the following functionality to enhance security

Security groups — Act as a firewall for associated Amazon EC2 instances, controlling both inbound and outbound traffic at the instance level

Network access control lists (ACLs) — Act as a firewall for associated subnets, controlling both inbound and outbound traffic at the subnet level

Flow logs — Capture information about the IP traffic going to and from network interfaces in your VPC

Database access – The breathe production database is not available in any manner outside the VPC. This means the database cannot be directly hacked Indirect access is available to developers who need to perform maintenance by use of SSH access to the database server secured with a public / private key.

Web server access – The breathe web servers are only accessible by breathe developers using SSG secured by public private key. All server instances are rotated out every 24 hours to prevent brute force attacks and repeated attempts using incorrect credentials generate an alarm and lockout..

Application Security

How is the breathe application secured?

Server Operating systems

The linux-based web instance operating systems are patched weekly for regularly updates and immediately if security alerts are released. This ensures that the core operating systems are always up to date with the latest security patches

Development Languages and Frameworks

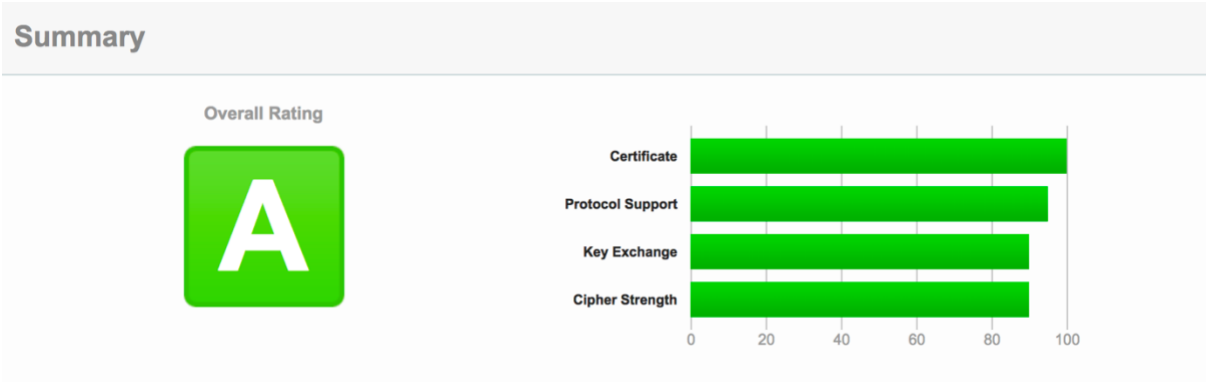
breathe has been built using Ruby on Rails. It is our policy to ensure that we are always running on supported versions of both the language and framework so that we have access to the latest security patches. Patches are tested in our staging environment before being released into the production environment.

SSL / TLS

Transport Layer Security (TLS) and its predecessor, Secure Sockets Layer (SSL), both frequently referred to as "SSL", are cryptographic protocols that provide communications security over a computer network. Websites can use TLS to secure all communications between their servers and web browsers.

Breathe uses a 2048 bit encryption key issues by Amazon with the signature algorithm being SHA256 with RSA to secure communication between client browsers, administrative tools, and the back end infrastructure.

Industry leader Qualys reports the breathe servers as obtaining a grade A



Credential security.

Security credentials (user passwords) are the only encrypted data in the database. These are encrypted, and are encrypted using a one way hashing model. The encryption tool we have selected has a significant advantage over a simply salted SHA-256 hash as it uses a modified key setup algorithm which is timely quite

expensive, which means it is considerably more difficult to accelerate brute force attacks using available consumer hardware.

How is the application hardened against software hacking ?

Session hijacking and session replay attacks.

Company and employee information is not stored in user cookies or session stores. The session is encrypted before being stored in a cookie. This prevents the user from accessing and tampering the content of the cookie. The encryption is done using a server-side secret key accessible only by the breathe developers. Sessions are deleted on logout and reset on login to prevent session fixation attacks.

Cross-Site Request Forgery (CSRF) attacks

To protect against forged requests, we introduce a required security token that our site knows but other sites don't know. We include the security token in requests and verify it on the server. In addition the application adheres to the Restful request model where possible. We also include an unobtrusive scripting adapter, which adds a header called X-CSRF-Token with the security token on every non-GET Ajax call.

Injection attacks.

SQL injection attacks aim at influencing database queries by manipulating web application parameters. A popular goal of SQL injection attacks is to bypass authorization. Another goal is to carry out data manipulation or reading arbitrary data to prevent this, breathe developers adhere to the following principles.

- Avoid using client side form data directly in SQL statements server-side
- Sanitise all user input to prevent injection of invalid data or executable code
- Scope all executed code to the specific user to prevent privilege escalation
- Cross-site scripting (XSS) attacks

XSS attacks are the most widespread, and one of the most devastating security vulnerabilities in web applications is XSS. This malicious attack injects client-side executable code. There are two key principles to fend of XSS attacks – Whitelists Input filtering and output escaping, both of which are principles followed by the breathe development team.

CSS Injection

CSS Injection is explained best by the well-known MySpace Samy worm. This worm automatically sent a friend request to Samy (the attacker) simply by visiting his profile. Within several hours he had over 1 million friend requests, which created so much traffic that MySpace went offline. CSS Injection is actually JavaScript injection, because some browsers (IE, some versions of Safari and others) allow JavaScript in CSS

This form of attack is prevented in breathe by simply preventing breathe users from styling the application.

Other forms of attack and conclusion

In addition to the common attacks mechanisms described above, there are others used less frequently but still real, which means they must be defended against. Breathe developers consider header injection, command line injection, unsafe query generation, and many other forms of attack. It is not the intent of this document to outline in details our approach to security, or indeed to provide a hacker's manual. If you have further specific questions regarding application security please do not hesitate to call.

How is breatheHR tested?

breatheHR security is tested externally twice yearly with a penetration test conducted by The Security Bureau of Brighton. This test last a week and comprises a comprehensive test using both automated tools and manual techniques. The test is conducted by CREST accredited consultants and results in an action plan which is then actioned.

THE SECURITY BUREAU

How security maintained through the release cycle?

To ensure new code does not degrade the security of the application, it follows a standard procedure before being committed to the production system.

Developer Review - all developers are held accountable for the security of their own code and are thus required to sign off any code they commit from a perspective of security

Peer Review - no code commits are permitted without a peer review. Code cannot be added directly to the production branch without CTO oversight.

Automated testing – code able to be unit tested is committed alongside appropriate automated tests

QA review - code that passes automated testing and peer review is then assessed by our QA team from a perspective of functionality and security. This assessment is conducted in a secure staging environment before being authorised for release.

Release - once a release candidate has passed QA it goes for approval by our release manager, who has final go / no-go authorisation on release.

Availability and Robustness

How is availability ensured?

Platform - breathe maintains superb availability, with an average annual uptime of greater than 99.995%. This is achieved by utilising AWS Elastic Beanstalk load balancing as our primary web technology. AWS Elastic Beanstalk is an orchestration service offered from Amazon Web Services for deploying infrastructure which orchestrates various AWS services, including EC2, S3, Simple Notification Service (SNS), CloudWatch, auto scaling, and Elastic Load Balancers. It means breathe can spin up as many server instances are necessary to ensure availability.

Failover – Monthly exercises are run by the technical team to ensure a new environment could be spun up in the event of a complete failure of an AWS availability zone, or even an entire AWS region. This process currently takes approximately an hour.

Monitoring - All web and data instances are monitored on a moment to moment basis using industry leader NewRelic Application Performance Monitoring, with automated alarms and alerts set to trigger if the application goes down for more than 60 seconds, or server resources reach a point where they need to be scaled up.

Backup – Encrypted AWS RDS snapshots are taken at approximately midnight daily (AWS provide a 30 minute window in which they run the backup). Backups are kept for 10 days. We maintain a point in time backup / restoration solution which means we can backup to any point in the retention window. Backups are proprietary to AWS and cannot be downloaded, making them extremely secure.

How robust is breathe from DDOS attacks?

The fundamental design of the breathe infrastructure makes it inherently resistant to DDOS attacks. Firstly, The ability to scale up instantly means that most DDOS attack techniques can simply be out scaled until the problem has been neutralised. In addition, the fact that web servers cannot be rotated out in less than 60 seconds means IP based attacks are largely irrelevant. On top of this we utilise AWS web shield to combat common DDOS attacks such as SYN floods and UDP reflection attacks. Finally, AWS gives us the tools to monitor network traffic for suspicious behaviour.

Data Protection

Summary

We are registered with the Information Commissioner's Office (ICO) for the purpose of handling your confidential data within the UK. Strict data handling procedures ensure our staff don't have visibility of passwords and access beyond their ability to

support your system. We do not undertake any work involving your data without your permission and hold no responsibility for the maintenance and content of your data.

Our internal processes are regularly audited in line with current legislation and the breatheHR terms and conditions.

GDPR Compliance

At breathe, we have always taken data security and privacy extremely seriously and believe that the GDPR is an important step forward for clarifying and enabling individual privacy rights. As such we are committed to GDPR compliance when enforcement begins May 25, 2018. For more information see 'Our approach to GDPR compliance'

Payment data

For our credit card payments we use RealEx Payments gateway and Allied Irish Bank Merchant Services (AIB). Their highly secure systems ensure that your card data is always safe and no card information is held on our servers. In addition AIB require us to partake in regular reviews of our PCI DSS compliance status to further protect your card data.