BrainStorm Security Overview

The purpose of this document is to provide your organization with an understanding of the BrainStorm Ppatform and the security capabilities BrainStorm has deployed to keep your data safe and secure. Please use this link to access BrainStorm's Security Profile on Whistic and gain access to pre-filled security questionnaires, pen test results, and more.

WHAT IS THE BRAINSTORM PLATFORM

The new workplace requires new learning models. BrainStorm is an enterprise software solution that drives real end-user behavior change with the applications they use to do their jobs. The BrainStorm adoption platform gives software vendors – and licensed organizations – a central, intelligent platform for driving adoption and results from their applications. Software vendors can add content packs comprised of learning workflows (courses) to the platform's marketplace where licensed organizations can select and administer packs to their end users. Learning workflows are courses that include videos, guides, assessments, polls, and responsive branching. Platform admins can customize select workflows, create end-user communication campaigns; they can also review usage data, workflow consumption data, and aggregated end-user insights. BrainStorm creates organization alignment around licensed technology – delivering digital transformation to leadership, ease and automation to IT, and hyper-relevancy to end users.

The BrainStorm platform includes two applications: the Admin Portal and the End-User Portal.

The admin portal is used to create user groups, issue licenses, prioritize, and distribute content to users, and review reporting. Admins may use additional administrator roles to assist with the management of an organization. For example, one user could be given admin rights to the Human Resources group, which would then allow them to group users, add licenses, and distribute content for that group. If the BrainStorm account has the Create Content add-on, the admin portal can be used by admins to upload their own videos and PDFs, and modify some existing flows. They may also create assessments, surveys, communications, and form this custom content into their own courses or flows.

Admins can use the flow designer to create unique courses for their users. This flow designer is a sophisticated tool that allows admins to create branches based on triggers or how users answer certain questions.

The BrainStorm platform has two types of triggers: a standard trigger and an external trigger. A standard (or internal) trigger uses user learning behavior to proactively tailor and engage end users in their learning flows. For example, a survey could be placed at the end of a flow to ask users if they want to continue learning or end the course. The flow would then continue if the user selected the continue option.

An externa trigger uses user software behavior and or role criteria to proactively tailor and engage end users in their learning flows. As another example, if a Microsoft Graph integration is configured, an external trigger could applied to send a Microsoft Teams course automatically to users that have not used specific functionality within Teams.

The end-user portal is where users go to find required learning, search for additional learning, and complete the learning. Content that has been specifically shared with users will show up for them automatically when they login. End users may also search for more courses and content if the administrator has given them access to do so.

SECURITY OVERVIEW

BrainStorm's ultimate goal is to maintain the security and integrity of our customers' and partners' data. We have invested heavily in the necessary controls and processes to achieve this goal. The BrainStorm Security Committee oversees the implementation and success of BrainStorm's security program. We have undergone two ISO 27001 certification audits and five SOC 2 examinations for BrainStorm's QuickHelp system over the past 5 years, and applied that deep knowledge of the highest-regarded security standards to the BrainStorm platform. We are currently under SOC 2 Type 2 surveillance for the BrainStorm platform and expect to have an audit report published in April 2024.

Data Collected

At the center of our security philosophy is the concept of "privacy-by-design.” This means we collect the minimum amount of Personally Identifiable Information (PII) from our customers on their end-users as is necessary to provide our services. This PII is provided by your organization in order to provision accounts, segment users, and identify their country (for compliance purposes). The PII we collect from your organization on end-users is essentially the same type of information contained in an email signature: Name, email, title, department, IP address, profile picture (optional). That's it.

Sharing Data

If you are a BrainStorm direct customer, BrainStorm will only surface your data to your organization. We do not and will never sell your end-users' PII, and we will not share that data with anyone except to provide the services (such as our subprocessors who provide key features and functionality in the platform) and as set forth in our Terms of Service. For more information on what BrainStorm does with this data, please review our Privacy Policy.

If you were provided access to the BrainStorm platform by a third-party Solution Provider or Managed Services Provider, then those organizations will have access to your data within the BrainStorm platform.

In addition, if you purchase a third-party published pack in the BrainStorm Platform's Marketplace, the publisher of that content will receive access to the platform’s user-level data for that content pack, such as user PII, user platform behavior, etc.

Here is a list of the subprocessors that BrainStorm uses to provide key features of the BrainStorm platform:

Name	Location	Description of Processing
Microsoft Azure	USA	Hosting services provider
SendGrid	USA	In-application email messaging
Aha!	USA	Customer feedback portal
HubSpot	USA	Email campaign management
Snowflake	USA	Data warehouse
Ironclad	USA	Clickwrap management
Freshdesk	USA	Support desk solution
Productboard	USA	Customer feedback portal and product roadmap
DataDog	USA	Platform monitoring and analytics

De-Identified Data

Like all SaaS solution providers, gaining insights from how our customers and users interact with our platform and content is extremely valuable to improving the quality of our offering. BrainStorm utilizes the de-identified data and metadata relating to each customer's use of the BrainStorm platform, such as, platform and content usage statistics, diagnostic data, telemetry data, and/or Third-Party software usage data (i.e., Microsoft, Google, Zoom, etc.), to learn about and improve the platform. This De-identified Usage Data does not contain any personally identifiable information about Users, the identity of Customer, Customer Data or Customer Content. This data is not individually identifiable and in most cases is aggregated.

What do we do with this De-Identified User Data?

- Make improvements to the platform and content,
- Fix bugs and issues that arise,
- Make strategic business decisions,
- Gain helpful insights to better support your, and
- Surface aggregated data points across the platforms.

Security Measures and Controls

The BrainStorm platform is currently under SOC 2 Type 2 surveillance for the 2023-2024 audit period. A SOC 2 Type 2 report will be published in April of 2024. BrainStorm has successfully passed SOC 2 Type 2 audits in each of the past 5 years on BrainStorm's other SaaS platform, QuickHelp, and we are confident we will do the same for this new platform. BrainStorm's security policies and controls have not changed, and we have applied that deep knowledge of the highest-regarded security standards to the BrainStorm platform. BrainStorm can provide a letter of attestation from our auditor upon request. A summary of our controls and security policies can be found by reviewing our SOC 2 report for QuickHelp through our Whistic security profile.

BrainStorm has also received its ISO 27001 certification for its QuickHelp platform in 2022 and successfully passed a surveillance audit in 2023. These same risks and controls for this ISO certification have been applied to the BrainStorm platform.

BrainStorm is able to transfer personal data outside of the EU to the United States by means of our Data Protection Addendum that incorporates the European Commission's Standard Contractual Clauses as the transfer mechanism. Additionally, BrainStorm follows Privacy Shield Principals. BrainStorm has taken careful steps to build this new platform to be compliant with GDPR requirements.

Infrastructure

BrainStorm does not receive, host, store, or process customer data in our corporate offices. BrainStorm uses Microsoft Azure as its hosting services provider. The BrainStorm platform is hosted on Azure US data centers, North Central region. Azure has ISO 27001 and SOC 2 Type 2 certifications, among several others.

All connections to the BrainStorm platform are encrypted by default, in both directions using modern ciphers and cryptographic systems. We maintain an A+ rating from Qualys/SSL Labs. We encrypt in transit utilizing TLS 1.2.

Some additional infrastructure details:

- BrainStorm utilizes tools that monitor threats and vulnerabilities to our infrastructure in real time.
- All customer data is logically segregated within Azure. All encryption keys managed by Azure.
- Azure is geo-redundant, which means that BrainStorm is able to reconstitute its infrastructure to another Azure data center if necessary.
- BrainStorm has employed point-in-time backup configuration. BrainStorm adheres to a CICD (Continuous Integration; Continuous Deployment) methodology.

Access Controls

BrainStorm employs a least privileged, need-to-know access approach. Our employees in a sales, product, architecture, customer support, or client success role will have access to your data to support your organization and users.

Other Security Details

- Enforces Azure's optimal password policy, which requires a minimum 8 characters, three out of four of lower and upper case letters, special symbols, and numbers. Click here for more information about this default policy.
- We run monthly pen tests and vulnerability scans. We do not, however, allow customers to run their own.
- Current version of most used web browsers.
- We conduct annual disaster recovery tests.
- Each employee must complete BrainStorm's security training within the first 90 days of hire. This training is reassigned annually for each employee.
- Extensive criminal background check (7 years) are performed on each new hire prior to gaining access to BrainStorm systems.