WHITE PAPER

MinuteMe Security

How MinuteMe protects your data

MinuteMe®

July 2022

Revision History

Revision	Date	Description of Changes
1.0	20-Jul-2022	Final version

This document is intended to provide an overview of minuteme.com's security practices in existence on the date of this publication, which are subject to change without notice. This white paper is for information purposes only and does not constitute legal advice or be perceived as supplementing or being incorporated into any terms and conditions in any contractual agreements.

© 2022 minuteme.com. All rights reserved.

Table of Contents

1. Introduction

MinuteMe is a cloud-based meeting management solution that enhances the meeting life cycle by reducing administration, improving accountability, and making meetings better. The platform caters for just about any meeting from small internal meetings such as 1:1's and team meetings, to large project management meetings involving multiple external parties where collaboration is key.

The product integrates with Google and Microsoft 365 calendar and task applications to take meeting and action management to the next level.

MinuteMe is mobile friendly and makes it easy to add agenda items, update actions, and complete pre-read on the go with your phone, tablet, or laptop.

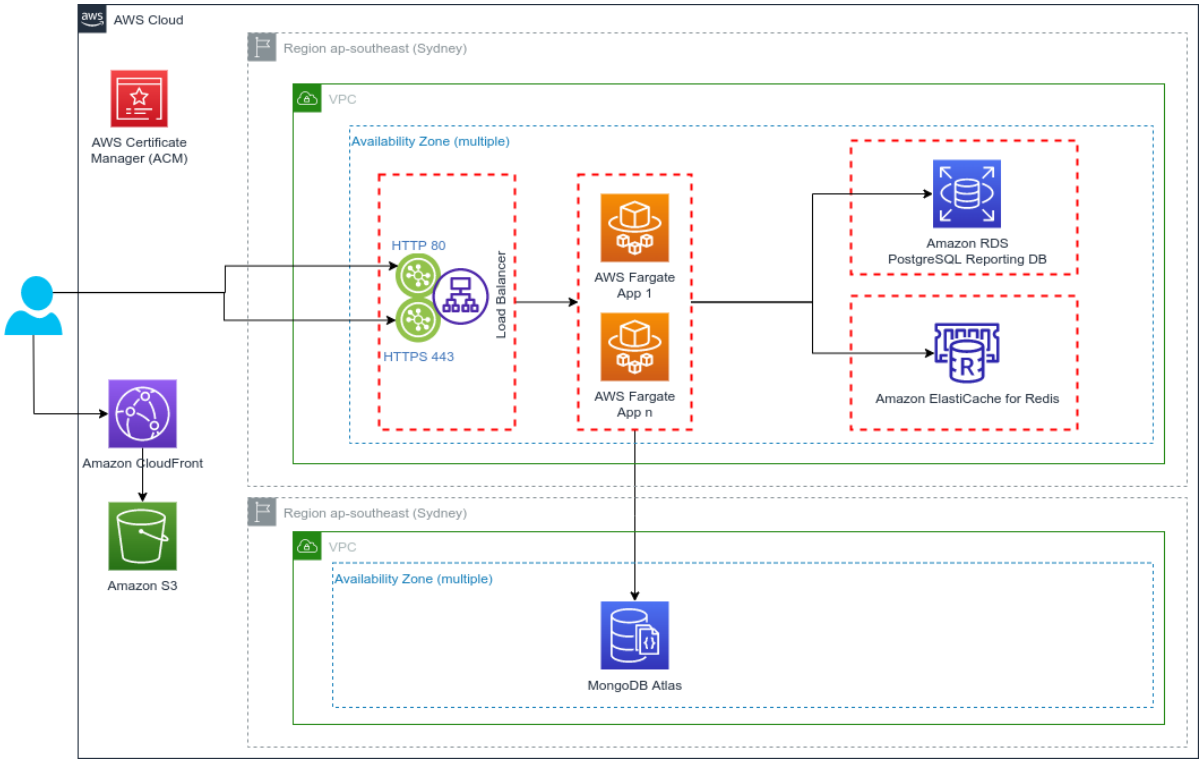
MinuteMe's mission is to transform the future of work with impact, by providing the means for productive, accountable, and less administrative meetings.

Our vision is to enable all meetings to be efficient, effective, and productive, to free up time for people to focus on what they do best.

At the core of our team culture at MinuteMe are our values:

1. Security – the security of our infrastructure and user data is our major priority. We manage and maintain security through our process, procedures, and policy, and it is ingrained in the way we operate.
2. Integrity – honesty, trust and respect are core principals of our team and the way we work. We have a 'safe to speak up' culture that ensures transparency and ethical behaviours in our team.
3. Accountability – we get things done by taking accountability and do not make promises we cannot meet.
4. Improvement – we continuously seek improvement opportunities from within our team and also from our users.
5. Teamwork – we pride ourselves by working things out as a team, where we respect each other's opinions and experience, to create great things together!
6. Authenticity – we pride ourselves on being genuine and holding true to our purpose.

2. Infrastructure



2.1. Web client

MinuteMe is a web-based application accessed via https://my.minuteme.com which runs in a user's standard web browser on both desktop and mobile devices. Connections using http are redirected to use https.

The major current browsers and versions are supported for use, and Internet Explorer is not supported.

The browser-based code is a Single-Page Application (SPA) written using the React framework and served to a user from an Amazon CloudFront S3 origin.

2.2. Application servers

The MinuteMe Application servers are containers running on Amazon Elastic Container Service (ECS) using AWS Fargate. The containers are load-balanced behind the AWS Load Balancer (ALB). The ALB has a defined set of rules to reject invalid requests based on the target host and path and supports a minimum SSL protocol of TLSv1.2.

The Web/Application servers that process user data and deliver the application functionality to MinuteMe users are restricted to traffic from the ALB and within the MinuteMe Virtual Private Cloud (VPC).

2.3. Databases

2.3.1. MongoDB Atlas

The main user data database is a NoSQL database hosted with MongoDB Atlas – a cloud hosted Database-As-A-Service (DBaaS) offering.

The MongoDB Atlas database is hosted in a peered VPC in the AWS Sydney region.

Access to the database is via a connection string that is stored within the AWS Systems Manager Parameter Store and is encrypted using a customer-managed key stored in the AWS Key Management Service (KMS). As this database is hosted in a separate VPC, the connection to it is encrypted using TLS/SSL.

2.3.2. Amazon ElastiCache for Redis

MinuteMe uses a Redis cache database hosted with AWS ElastiCache for session state management and other application functionality that requires high speed access to temporary data. Access to the database is restricted to traffic from the Web/Application servers.

2.3.3. Amazon Relational Database Service for PostgreSQL

The event reporting database is a PostgreSQL relational database hosted with AWS Relational Database Service (RDS). This is used for back-end reporting and does not provide any direct service to the MinuteMe web application.

Access to the database is via a connection string that is stored within the AWS Systems Manager Parameter Store and is encrypted using a customer-managed key stored in the AWS Key Management Service (KMS).

2.4. File storage

MinuteMe utilises the Amazon Simple Storage Service (S3) for file storage and distribution.

There is no direct public access to any data stored in S3. User access to files stored in S3 is only via a CloudFront distribution and supports a minimum SSL protocol of TLS v1.2.

The following types of files are stored in S3:

- User files that are uploaded via the Web client or created in response to a user action within MinuteMe:
  - User avatars
  - Workspace logos
  - Inline images included in meeting notes (sensitive)
  - Files uploaded from a user's computer file system and attached to meetings (sensitive)
  - Agenda and Minutes PDF files created by MinuteMe (sensitive)
- MinuteMe application files:
  - Client browser files (html/javascript)
  - Help site content
- System data generated by the back-end servers and services:
  - Service log files (private)

Access to the items marked **sensitive** in the above list can only be made using a time-limited Amazon S3 presigned URL generated by the application.

Items marked **private** in the above list are not accessible via CloudFront.

2.5. Encryption and key management

2.5.1. Encryption in transit

Data in transit across open networks to my.minuteme.com are encrypted with AES-128 GCM and authenticated with RSA. The key exchange mechanism is ECDHE. The minimum SSL protocol supported is TLSv1.2. SSL connections are terminated at an AWS Application Load Balancer.

Logins and sensitive data transfers are performed over TLS only - all insecure connections are upgraded to use HTTPS.

Data in transit across open networks from uploads.minuteme.com is encrypted with AES-128 GCM. The minimum SSL protocol supported is TLSv1.2. SSL connections are terminated at AWS CloudFront.

Data in transit between the MinuteMe application servers and the MongoDB Atlas database is encrypted using TLS.

2.5.2. Encryption at rest

MinuteMe guarantees encryption at rest for user data with AES-256 GCM in the following services:

- Amazon Simple Storage Service (S3)
- Amazon Simple Queue Service (SQS)
- Amazon Simple Notification Service (SNS)
- Amazon Relational Database Service for PostgreSQL (RDS)
- Amazon CloudWatch Logs
- MongoDB Atlas

Encryption keys are stored and managed using the AWS Key Management Service (KMS).

The following services do not encrypt data at-rest:

- Amazon CloudSearch. This service does not support the encryption of indexed data at-rest. MinuteMe is hosted on AWS who are responsible for the protection of the Data Layer. Requests to CloudSearch (for both indexing and searching) are performed over HTTPS and access to the CloudSearch domains is restricted to traffic from the Web/Application servers using Amazon Identity and Access Management (IAM).
- Amazon ElastiCache for Redis. This is a temporary data store where data resides in-memory. Due to the temporary volatile nature of data in this database, it is not backed-up to disk.

2.6. Backups

Further to the information provided in section 2.3 Databases, differing backup strategies are used depending on the use of the database.

2.6.1. MongoDB Atlas

Snapshots of the primary user data database in MongoDB Atlas are taken Monthly, Weekly, Daily and 6 hourly. Additionally, Continuous Cloud Backup is used to permit a restore to any point in time within the past 7 days. This meets a recovery point objective (RPO) of 1 minute.

Backups are stored in Amazon S3 and encrypted at-rest using AES-256 GCM encryption.

2.6.2. Amazon ElastiCache for Redis

Due to the temporary volatile nature of data in this database, it is not required to be backed-up.

2.6.3. Amazon Relational Database Service for PostgreSQL

Snapshots of the event reporting database in RDS are taken Daily. Additionally, transaction logs are used to permit a restore to a 5 minute window within the past 7 days. This meets a recovery point objective (RPO) of 5 minutes.

Backups are stored in Amazon S3 and encrypted at-rest using AES256-bit encryption.

2.7. Scalability and reliability

The MinuteMe service - excluding databases - is fully containerised and operates on AWS Fargate across multiple Availability Zones (AZs). This provides for highly scalable and reliable infrastructure, suitable for dealing with increasing user demand while providing a quality experience for end-users. The service consists of several microservices to ensure minimal impact on system health in the case of failure of one or more components.

The Application servers operate in a Cluster (with multiple active servers) where the health of each server is monitored by an AWS Application Load Balancer. Should a server be considered ‘unhealthy’ then a new server will be started to maintain a minimum amount of running servers.

Infrastructure-as-code is used via Terraform to ensure audibility and maintainability of infrastructure resources.

All databases are synchronously replicated across multiple AZs operating in a Hot-Standby configuration.

MinuteMe monitors performance metrics for all its infrastructure components and builds its infrastructure for scale. Furthermore, we hold quarterly scale reviews with both infrastructure engineers and management to ensure that our roadmap provides quality service to an ever-growing number of users and product features.

2.7.1. Availability

Deployments for updates to the MinuteMe service are made using the blue/green deployment technique. This is supported by the features offered by the AWS Application Load Balancer and AWS Elastic Container Service that enable new releases to be deployed without any downtime.

The databases used as part of the service are deployed in a Hot-Standby configuration which allows servers to be upgraded without affecting service availability. In the event that

there is maintenance that requires down-time, this is planned during periods of least system usage.

With the High Availability (HA) techniques described above and incorporated into the service, MinuteMe commits to a 99.8% availability for its users.

3. Product security features and functionalities

3.1. Login security

MinuteMe provides 3 options for sign-up or sign-in, based on where the user's email account is hosted.

3.1.1. Sign up with Microsoft

Users whose email account is a Microsoft Work/School or Personal account can use the Sign up / Sign in with Microsoft option. The user identity is stored in and authenticated against Azure Active Directory.

Microsoft users can take advantage of any multi-factor authentication provided with their Microsoft Azure AD account.

3.1.2. Sign up with Google

Users whose email account is a Google Workspace (formerly G Suite) or Gmail account can use the Sign up / Sign in with Google option. The user identity is stored in and authenticated against Google Cloud Identity.

Google users can take advantage of any multi-factor authentication provided with their Google Workspace account.

3.1.3. Sign up using your email address

Users whose email account is hosted elsewhere or their organization prevents sign up using the Microsoft or Google option can sign up using their email address. The user identity is stored in and authenticated against Amazon Cognito. The user will need to verify their email address using a verification code during the sign-up process.

Our password policy requires a user to have a "strong" password of at least 8 characters consisting of at least one lowercase letter, one uppercase letter and one number.

3.2. Authorization

3.2.1. Microsoft Azure AD and Google Workspace Scopes

When users sign-up with Microsoft/Google they will be asked to grant MinuteMe access to specific information from their Microsoft/Google account. Some organization's security and identity administrator teams like to manage the consent for MinuteMe to access their

employee's data on their behalf. If this is the case the user's organization will be required to approve access to MinuteMe before they can sign up using their Microsoft/Google account.

In order to sign up with Microsoft/Google only minimal access to the user's account is required. MinuteMe uses an incremental and dynamic consent to request access to additional data should the user make the choice to opt-in to additional features inside the app. These additional features are:

- searching for contacts to invite to a meeting
- synchronising action items with Microsoft ToDo/Google Tasks
- importing Outlook/Google calendar events

Detailed information about the scopes required from Microsoft/Google for access to specific MinuteMe features can be found in the Accessing MinuteMe section in the MinuteMe Help Center.

3.3. User provisioning and deprovisioning

3.3.1. Creation of a workspace

The top level of authorization in MinuteMe is a workspace - all meetings are created in a workspace. The first user of a team, group or organization who signs up with MinuteMe must create a workspace and becomes the first Owner of the workspace.

The workspace Owner is the custodian of the data within the workspace, and they are responsible for payment required for their subscription.

During the creation of a workspace, it is recommended to configure trusted email domains. These are the email domains owned by the workspace's team, group or organization and are used during user provisioning as described below.

3.3.2. User added directly to a workspace

Workspace Owners can add their contacts to the workspace via the Manage Workspaces page inside MinuteMe by entering an email address and choosing a role. The contact's email domain will determine if they need to accept an invitation or not:

- If the contact's email domain is one of the workspace's trusted email domains, the person will automatically be an accepted member of the workspace.
- If the contact's email domain is not one of the trusted email domains, the person will receive an email invitation to join the workspace.

A user can only view meetings in a workspace once they are an accepted member of the workspace **and** have been granted access to individual series/meetings within the workspace as described in the next section.

3.3.3. User added directly to a series/meeting

Workspace members that create a new series or meeting become the first Admin of the series/meeting.

Meeting admins can add their contacts to a meeting by entering an email address and choosing an access level. If the contact is not already a member of the workspace, the contact will be added to the workspace and their email domain will determine their role and whether they need to accept an invitation to join the workspace or not:

- If the contact's email domain is one of the workspace's trusted email domains, the person will be assigned the Member role and are not required to accept an invitation to join the workspace.
- If the contact's email domain is not one of the trusted email domains, the person will be assigned the Guest role and will be required to accept an invitation to join the workspace.

When a user is already an accepted member of a workspace, they will not be required to accept subsequent invitations to any meeting within the workspace.

3.3.4. User removed from a workspace

A user is removed from a workspace by deleting them from the Manage Workspaces page inside MinuteMe.

A user that is deleted from the workspace will no longer see the workspace when they sign in to MinuteMe. Their access is removed from the workspace and they are unable to see any meetings they created or were added to by other meeting admins in the workspace.

3.3.5. User removed from a series/meeting

A user can be removed from a series, or meetings within a series, by a meeting admin.

A user that is removed from an individual meeting within a series may still have access to other meetings within the series.

A user that is removed from a series will have no access to future meetings in the series but may still have access to past meetings within the series.

A user that is removed from a series or meeting is not automatically removed from the workspace.

3.3.6. User removed from Microsoft Azure AD and Google Workspace

A user that uses Sign in with Microsoft or Sign in with Google and has their account removed or locked in Microsoft Azure AD or Google Workspace will no longer be able to sign-in to MinuteMe.

NOTE: If the user had previously signed-up using their email address as described in section 3.1.3, they may still sign-in using that email address as this is not linked with their Microsoft Azure AD or Google Workspace account.

3.4. Permissions

3.4.1. Workspace permissions

The role applied to a user in a workspace determines the permissions that are applied to the user in the workspace.

The user who creates a workspace becomes the first Owner, and they can assign other users to the workspace. The roles that can be assigned are Owner, Admin, Member or Guest.

Refer to the Workspace permissions help guide for an outline of the Workspace permissions.

3.5. Series permissions

A Series groups together ‘like’ meetings around a specific topic/event/client/project.

Series permissions are defined by assigning access levels to users for each series added to a workspace.

When a series is created, the creator becomes the first Admin. They can assign access to other users (including other Admin users).

When access levels are added to the series, these become the default access levels for each meeting created in the series. The access levels can be overridden for each meeting when they are created, or at a later time.

Refer to the Series permissions help guide for more information on each of the access levels.

3.5.1. Meeting Permissions

Meeting permissions are defaulted from the Series permissions. In addition, it's possible to give a user access to one or more individual meetings in the series.

When a meeting is modified for the first time (i.e. attendees or permissions are changed, the agenda is updated, minutes or action items are added), the permissions are copied from the series to the meeting. This means that any future changes made to the permissions of the series are **not** automatically applied to each meeting. In this case, each meeting will need to be updated separately.

Conversely, this also means, if you add permissions for a user to a meeting, these permissions will not automatically flow up to the series or across to other meetings, and therefore won't apply to any other meetings created in the series.

Refer to the Meeting permissions help guide for more information on each of the access levels.

MinuteMe provides the 'non system access' level of 'None' to allow for a meeting invitee to participate in a meeting without having any system access. This is particularly useful for external guests to meetings or for presenters at meetings who are not invited to the full Series of meetings and do not need to be active user as they do not add meetings, create agendas/minutes or create/update action items.

4. Operational security

4.1. Information security

MinuteMe is committed to information security to ensure that the appropriate controls are in place to maintain information security for its customers.

MinuteMe onboarding processes and company polices outline the importance of ensuring that all user data remains confidential and that access to such data is only for completing tasks related to their job including providing service to our users. Our **Information Security Policy** also states the importance of maintaining confidentiality of any user data and the appropriate disposal mechanisms of any printed data.

All MinuteMe employees sign a **Confidentiality and Information Security Agreement** and undertake a formal **Cybersecurity Awareness Training** as part of onboarding, (and undertake yearly refresher training).

In addition to process, policy and training, MinuteMe also have strict entry points to access user data. Refer to our Privacy policy for further information.

4.2. Identity and access management

MinuteMe uses Microsoft Azure Active Directory (AAD) for our enterprise identity provider and the Azure AD standard password policies are in use. All employees are required to use 2-factor authentication (2FA).

Access to AWS is granted based on role through AAD in accordance with the need-to-know and least privilege principles.

A quarterly user access review is conducted where access that is no longer necessary is removed. When employees terminate their employment with MinuteMe all access to systems is revoked.

4.3. Email protection

MinuteMe uses Microsoft 365 as our staff email provider, Amazon Simple Email Service (SES) for sending emails from the MinuteMe application and Intercom for sending customer support emails. DMARC and SPF are in place for these domains.

Employees are continuously instructed regarding phishing avoidance best practices.

4.4. Network security

The workstations of MinuteMe staff are on a dedicated Virtual Local Area Network (VLAN) that is restricted for use of the MinuteMe staff only.

4.5. Access to user data

MinuteMe treats all data that users submit to the service, which is processed by us solely on a user's behalf, as a "black box". This means that user data is generally not accessed for the performance of the MinuteMe service, and that we treat all submitted user data with the highest level of sensitivity and confidentiality.

Access to user data by MinuteMe staff is limited in accordance with our Terms of Use or respective agreement with the user, on a case-by-case basis.

4.6. Vulnerability management

MinuteMe regularly performs a security audit of its code base to find and fix known vulnerabilities in dependencies that could cause data loss, service outages, unauthorized access to sensitive information, or other issues. Any vulnerabilities identified are recorded in a development backlog and classified based on our evaluation of their impact on the confidentiality, integrity, and availability of the service and of user data. MinuteMe engineers carry out any remediation according to our internal **Patch Management Policy**.

4.7. Software development lifecycle

MinuteMe uses the git revision control system with Atlassian Bitbucket Cloud for all source code. Changes to MinuteMe's code base go through a suite of automated tests and are peer reviewed as part of the Continuous Integration / Continuous Deployment (CI/CD) process.

Code changes that are approved are first pushed to a staging server where MinuteMe employees are able to test changes before an eventual push to production servers and our user base.

4.8. Incident response

MinuteMe takes incident management seriously and has an **Incident Response Procedure** that outlines how incidents are managed. An incident is defined as an unplanned event such as a data breach, interruption to service or a reduction in quality of a service. An incident is also an issue that has been raised where the service previously worked and now does not work as expected. The procedure outlines how MinuteMe assesses, contains, evaluates, notifies, and reviews and monitors incidents.

All incidents are recorded in the **Incident Response Register** and learnings from incidents are used to improve our process, procedures, systems, and tools as part of continuous improvement.

4.9. Disaster recovery and Business continuity

MinuteMe maintains a **Business Continuity Plan** for dealing with disasters affecting our physical office (where no part of our production infrastructure is retained).

In addition, we maintain a **Disaster Recovery Plan** (DRP) for dealing with disasters affecting our production environment, that were assessed as critical unplanned events as part of the Incident Response process, which includes the restoration of the service's core functionality from another location. MinuteMe's primary data center is hosted on AWS in Sydney (Australia), with redundancy in the same AWS region. In the event of a single AWS data center loss, recovery procedures would bring up nodes in another data center without human intervention. Testing is conducted at least once a year. MinuteMe's DR test may be in the form of a walk-through, mock disaster, or component testing.

4.10. Data retention and disposal

4.10.1. Data retention

MinuteMe will retain your information that MinuteMe controls for the period necessary to fulfill the purposes outlined in our **Privacy Policy**. Data that MinuteMe processes on behalf of our users will be retained in accordance with our Terms of Use and other commercial agreements with such customers.

4.10.2. Data deletion

MinuteMe customers retain full control of their submitted data, and may modify, export, or delete it at all times using the means available through the application.

Upon termination of an account, users are able to request deletion of their data as part of the account closure procedure. User data will then be deleted within 90 days of the request, which includes a 30-day period to allow for rollback and an additional 60 days to proceed with the deletion process.

Alternatively, users may opt to keep the account's data in the platform, in which case we may continue to retain it, but may also delete it at any time at our discretion.

4.11. Data destruction

Our service is hosted on AWS who implements proprietary data distribution and deletion strategies to allow for safe storage of sensitive data in a multi-tenant environment. Storage media decommissioning is performed by the AWS using the techniques detailed in NIST 800-88.

4.12. Monitoring

MinuteMe collects and monitors network logs using traffic logs from edge locations and load balancers, application-level logging for tracing and auditing events, and system-level logging for auditing access and high-privilege operations. All logs are stored in either Amazon S3 or Amazon CloudWatch and are retained indefinitely.

MinuteMe monitors the capacity utilization of infrastructure resources to ensure service delivery matches service level agreements. In addition:

- Amazon CloudWatch and Amazon GuardDuty are used to trigger automated event-based messaging for critical infrastructure alerts.
- Airbrake.io is used to trigger automated event-based messaging for application alerts.

4.13. Privacy

Refer to our Privacy policy.

4.14. Office security

Access to the offices, and lifts is restricted via access cards. Building security have a number of procedures in pace to routinely monitor the building and floor access. The security system embedded on each floor tracks door usage, and an access report is able to be obtained from building security. The desk spaces are under 24-hour CCTV coverage and the premises also have roving security guards across the precinct. CCTV video records are stored and held for 18 months.

The Chief Commercial Officer is responsible for updating the Building Management Team of any changes to employees to obtain or revoke access to a building access card.

4.15. Data centre security

MinuteMe relies on the AWS Data Centre controls such as site selection, redundancy, availability, and capacity planning to maintain an appropriate level of security. MinuteMe does not host any of its own servers.