Semble

Security overview

Introduction

Semble's mission is to improve healthcare. We are committed to transforming the clinic experience for clinicians, their admin staff and patients with our integrated clinical software. With Semble, healthcare organisations are improving their efficiency, while focusing on personalisation of care and ultimately improving outcomes. We are committed to being transparent about our security practices and helping you understand our approach.

Table of Content

Security and Risk Focus

Semble's primary security focus is to safeguard our customers' data. This is the reason that Semble has invested in the appropriate resources and controls to protect and service our customers. This investment includes the implementation of Corporate Security and Product Security personnel. These team members are responsible for Semble's comprehensive security program and the governance process. We are focused on defining new and refining existing controls, implementing and managing the Semble security framework as well as providing a support structure to facilitate effective risk management. Our Chief Technology Officer oversees the implementation of security safeguards across Semble and its products.

Security and Risk Management Objectives

We have developed our comprehensive security framework using best practices in the SaaS industry. Our key objectives include:

- Customer trust – consistently deliver superior products and services to our customers, whilst safeguarding the data they entrust us with.

- Business continuity – ensure ongoing availability of the service and access to data for all authorised individuals. We proactively minimise the security risks threatening service continuity.
- Data and service integrity – ensure that customer information is never corrupted or managed inappropriately. Protecting the confidentiality, integrity and availability of customers' data, at all times, is of paramount importance.
- Compliance with standards – we design our security program around the industry cybersecurity best practice guidelines including the National Cyber Security Centre (NCSC), as evidenced by our Cyber Essentials Plus certification. We are fully UK GDPR compliant and our controls governing the confidentiality, integrity and availability of customer data are also designed to be ISO 27001 compliant.

Security Controls

Product Infrastructure

Cloud Infrastructure Security

Semble does not host any product systems within its corporate offices.

Semble outsources hosting of its product infrastructure to leading cloud infrastructure provider, Amazon Web Services (AWS). Our hosting provider guarantees between 99.95% and 100% service availability ensuring redundancy to all power, network, and air conditioning services.

Semble's AWS product infrastructure resides in the London region. AWS maintains an audited security program, as well as physical, environmental, and infrastructure security protections. Business continuity and disaster recovery plans have been independently validated as part of their SOC 2 Type 2 and ISO 27001 certifications.

Compliance documentation is publicly available on the AWS Cloud Compliance Page.

Network Security and Perimeter Protection

Our product infrastructure enforces multiple layers of filtering and inspection of all connections throughout the platform.

Firewalls are configured to deny network connections that are not explicitly authorised by default, and traffic monitoring is in place for the detection of anomalous activity.

Configuration Management

Automation drives our ability to scale with our customers' needs. The product infrastructure is a highly automated environment that expands capacity and capability as needed. Our application is containerised and runs on AWS servers that we don't have access to. We rely on the AWS Shared Responsibility Model to ensure that the configuration of these servers is maintained throughout their lifecycle. The servers that we do use are deployed with their hardened configuration and patch via infrastructure as code. This ensures consistency of security practices throughout.

We maintain a robust collection of audit logs which help us get insight into any changes to our infrastructure. These logs are segregated from the rest of our operations to ensure that they can't be tampered with.

Alerting and Monitoring

Not only does Semble fully automate its build procedures, we also invest in automated monitoring, alerting and response capabilities to continuously address potential issues. Our product infrastructure is instrumented to alert engineers and administrators when anomalies occur. In particular, error rates, abuse scenarios, application attacks, and other anomalies trigger automatic responses and alerts to the appropriate teams for response, investigation, and correction. As unexpected or malicious activities occur, automated systems bring in the right people to ensure that the issue is rapidly addressed.

Many automated triggers are also designed into the system to immediately respond to unforeseen situations. Traffic blocking, process termination, and similar functions kick in at predefined thresholds to ensure that the platform can protect itself against a wide variety of undesirable situations.

Application Protection

Web Application Defences

All customer content hosted on the platform is protected by a Web Application Firewall (WAF). The WAF is configured with a combination of industry standards and custom rules that are capable of automatically enabling and disabling appropriate controls to best protect our customers. These tools actively monitor real-time traffic at the application layer with the ability to alert or deny malicious behaviour based on behaviour type and rate.

The rules used to detect and block malicious traffic are aligned with the best practice guidelines documented by the Open Web Application Security Project (OWASP), specifically the OWASP Top 10 and similar recommendations. Protections from Distributed Denial of Service (DDoS) attacks are also incorporated, helping to ensure customers' websites and other parts of our products are available continuously.

Development and Release Management

One of Semble's greatest advantages is a rapidly-advancing feature set, and we constantly optimise our products through a modern continuous delivery approach to software development.

New code is proposed, approved, merged and deployed daily. Code reviews, testing (where applicable), and merge approval are performed before deployment. Approval is controlled by designated repository owners. Once approved, code is automatically submitted to Semble's continuous integration environment where compilation, packaging and unit testing occur.

All code deployments create archives of existing production-grade code in case failures are detected by post-deploy hooks. The deploying team manages notifications regarding the health of their applications. If a failure occurs, roll-back is immediately engaged.

Semble features seamless updates, and as a SaaS application, there is no downtime associated with releases. Major feature changes are communicated through in-app messages and/or product update posts and emails.

Newly developed code is first deployed to the dedicated and separate Semble QA environment for the last stage of testing before being promoted to production. Network-level segmentation prevents unauthorised access between QA and production environments.

Vulnerability Scanning, and Penetration Testing

Semble manages a multi-layered approach to vulnerability scanning, using a variety of industry-recognised tools to ensure comprehensive coverage of our technology stack.

We bring in industry-recognised third parties to perform penetration tests at least annually. The goal of these programs is to iteratively identify flaws that present security risks and rapidly address any issues. Penetration tests are performed against the application layers and network layers of the Semble technology stack.

Customer Data Protection

Logical/Physical Tenant Separation

Semble provides a highly scalable, multi-tenant SaaS solution and a physically segregated single tenant for customers that require it.

For our multi-tenant solution, the Semble user interface and APIs restrict access to authorised content exclusively. Semble logically segments the data using practice IDs and associates that unique ID with all data and objects specific to a customer. Information is made available via the user interface or APIs to be produced for a specific Semble portal, without the risk of cross-portal access or data pollution.

Authorisation rules are incorporated into the design architecture and validated on a continuous basis. Additionally, we log application authentication and associated changes, application availability, and user page views.

For our single-tenant solution, we offer several layers of customisation options depending on the customer's requirements.

Confidential Information and Patient Data

Semble is a practice management system is designed to collect highly sensitive medical data. As such we offer the customer a suite of features such as custom roles and access groups designed to control who can read what information.

We offer the ability to collect payments from patients using Stripe as a partner. Credit card data never reaches our servers and as such we have not been audited by a PCI-certified auditor nor are we a PCI Service Provider. You should read Security at Stripe to ensure that their security meets your requirements.

Encryption In-Transit and At-Rest

All sensitive interactions with our products (e.g. API calls, authenticated sessions, etc.) are encrypted in transit with TLS version 1.2, or 1.3 and 2,048 bit keys or better.

Semble leverages several technologies to ensure stored data is encrypted at rest. Platform data is stored using AES-256 encryption. User passwords are hashed following industry best practices and are encrypted at rest.

Key Management

Encryption keys for both in-transit and at-rest encryption are securely managed by AWS. TLS private keys for in-transit encryption are managed through AWS CloudFront. Volume and field-level encryption keys for at-rest encryption are stored in a hardened Key Management System (KMS). Keys are rotated at a frequency that's dependent upon the sensitivity of the data they're encrypting. In general, TLS certificates are renewed annually.

Semble is unable to use customer-supplied encryption keys at this time.

Data Backup and Disaster Recovery

System Reliability and Recovery

Semble is committed to ensuring the availability of our systems by using commercially reasonable efforts to meet a Service Uptime of 99.95% for our Subscription Service in a given calendar quarter.

Additionally, we provide real-time updates and historical data on system status and security via Semble's status site.

All Semble product services are built with full redundancy. Server infrastructure is strategically distributed across multiple distinct availability zones and virtual private cloud networks within our infrastructure providers, and all web, application, and database components are deployed with a minimum of n+1 supporting containers.

Disaster Recovery

Semble maintains a disaster recovery plan that is tested annually as a part of our ISO27001 controls.

All of Semble's systems are cloud based and as such, in the event of a disaster such as an earthquake or a massive power failure, our responsibilities are shared with AWS under the the AWS Shared Responsibility Model. We have procedures in place to ensure the safety and security of our staff and to ensure the continuity of our service to our customers. These procedure rely on the fact that all of our staff are setup to work from remote locations and are distributed in various locations. AWS has procedures in place to assure the resilience and availability of their infrastructure in the event of a disaster which help us maintain the availability of our application.

Backup Strategy

Systems Backups

Systems are backed up on a regular basis with established schedules and frequencies. Backups are kept for any database in a way that ensures restoration can occur easily. Backups are monitored for successful execution, and alerts are generated in the event of any exceptions. Failure alerts are escalated, investigated, and resolved.

Data is backed up daily to their local region. Additionally, backups are copied periodically to a separate cloud provider for recovery in the event of a complete outage from AWS. Monitoring and alerting are in place for replication failures and are triaged accordingly.

All production data sets are stored on a highly available file storage facility like Amazon's S3 that use version control and long-duration life cycle policies.

Physical Backup Storage

Because we leverage public cloud services for hosting, backup, and recovery, Semble does not implement physical infrastructure or physical storage media within its products. Semble does not generally produce or use other kinds of hard copy media (e.g., paper, tape, etc.) as part of making our products available to our customers.

Backup Protections

By default, all backups are protected through access control restrictions on our product infrastructure networks and access control lists on the file systems storing the backup files.

Customer backup Options

For customers who would additionally like to back up their data, our platform provides many ways of making sure you have what you need. Many reports are available within Semble and we offer a full suite of public APIs that can be used to synchronise your data with other systems.

Identity and Access Control

User Management

Our products allow for granular authorisation rules. Customers are empowered to create and manage users of their portals and assign the privileges that are appropriate for their accounts and limit access to their data features.

Login Protections

Our product allows users to login to their Semble accounts using the built-in S emble login. The built-in login enforces a uniform password policy which requires a minimum of 8 characters and a combination of lower and upper case letters, special characters, and numbers. Customers cannot change the default password policy.

Customers are also encouraged to set up two-factor authentication for their Semble accounts.

Production Infrastructure Access

Access to Semble's systems is strictly controlled and follows the principle of least privilege. Semble employees are granted access using a role-based access control (RBAC) model.

Day-to-day access is minimised to only the individuals whose jobs require it. Procedures are in place for emergency access (e.g. alert responses /troubleshooting).

Direct network connections to application servers are impossible due to our containerised approach and all database access is logged.

Semble Employee Access to Customer Accounts

Customer Support, Services, and other customer engagement staff may request Just In Time Access (JITA) to customer portals on a time-limited basis. Requests for access are limited to their work responsibilities associated with supporting and servicing our customers. The requests require explicit in-writing authorisation from customers. All access requests, logins, queries, page views and similar information are logged.

Corporate Authentication and Authorisation

Access to the Corporate network, both remotely and while in the office, requires multi-factor authentication (MFA), and most SaaS applications in use by Semble require Single Sign On (SSO) with MFA in order to facilitate centralised access control.

Password policies follow industry best practices for required length and complexity. We also make use of password managers and end-to-end encrypted messaging platforms to exchange sensitive information.

Organisational and Corporate Security

Background Checks and Onboarding

Semble employees undergo a background check prior to the commencement of their employment.

Upon hire, all employees must read, and acknowledge Semble's Acceptable Use Policy (AUP) and Code of Conduct - which help define employees' security responsibilities in protecting company assets/data (including, but not limited to protecting mobile devices, and securing corporate equipment).

Policy Management

To help keep all our employees on the same page with regard to protecting data, Semble documents and maintains a number of written policies and procedures. Semble maintains a core Written Information Security Policy - the policy covers data handling requirements, privacy considerations, and responses to violations, among many other topics.

Policies are reviewed and approved at least annually and stored in the company wiki. Policies requiring acknowledgement by employees are incorporated into mandatory annual training.

Security Awareness Training

We consider employees to be our first line of defence and we ensure Semble employees are well-trained for their roles. Semble requires all employees to undergo security awareness training that covers general security best practices on an annual basis. In addition to awareness training, Semble keeps

employees aware of recent security news or initiatives with internal knowledge articles.

More specialised content is available based on an employee's role or resulting access. For example, Semble has a security program, required from developers on the product teams that covers training on security development, common risk, threats, and issues.

Risk Management

Semble has an Enterprise Risk Management (ERM) program that includes a documented ERM policy, continual risk assessments, and a formal risk register. Risk mitigation and remediation activities are tracked via a ticketing system and reviewed at a designated cadence. This is part of our ISO27001 suite of controls.

Vendor Management

We leverage a number of third-party service providers who augment the Semble products' ability to meet your marketing, sales, services, content management, and operations needs. We maintain a vendor management program to ensure that appropriate security and privacy controls are in place. The program includes inventorying, tracking, and reviewing the security programs of the vendors who support Semble.

Appropriate safeguards are assessed relative to the service being provided and the type of data being exchanged. Ongoing compliance with expected protections is managed as part of our contractual relationship with them. Our Security, Legal, and Compliance teams coordinate with our business stakeholders as part of the vendor management review process.

We also maintain a list of our Sub-Processors that is available on our Website.

Corporate Physical Security

Semble offices are secured in multiple ways. Security guards are employed at Semble offices to help create a safe environment for Semble employees. Door access is controlled using RFID tokens tied to individuals, which are automatically deprovisioned if lost or when no longer needed (e.g., employee termination, etc). Video surveillance and many other protective measures are implemented across Semble offices.

Corporate Network Protections

Centrally managed application firewalls are deployed for High Availability at Semble's Corporate offices. Our guest networks are separate from our corporate network and are serviced by separate firewalls. Firewalls are set up to filter unauthorised inbound traffic from the Internet and are configured to deny inbound network connections that are not explicitly authorised by a rule.

Endpoint Protection and Antivirus/Malware Protection

Semble leverages Endpoint Detection and Response (EDR) capabilities to protect its systems. This enables us to have extensive visibility into anomalous system behaviour as well as to rapidly investigate and take appropriate action through either automated event triggers or manual containment of a system. Our EDR platform is integrated with other tools in our security stack so as to create an optimised, multi-tooled ecosystem to effectively defend our business.

Incident Management

Incident Response

Semble's team is trained to respond quickly to all security and privacy events. Semble's rapid incident response program is responsive and repeatable. Pre-defined incident types, based on historical trending, are created in order to facilitate timely incident tracking, consistent task assignment, escalation, and communication. Many automated processes feed into the incident response process, including malicious activity or anomaly alerts, vendor alerts, customer requests, privacy events, and others.

In responding to any incident, we first determine the exposure of the information and determine the source of the security problem, if possible. We provide periodic updates as needed to ensure the appropriate resolution of the incident.

Our Chief Information Technology Officer reviews all security-related incidents, either suspected or proven, and we coordinate with affected customers using the most appropriate means, depending on the nature of the incident.

Privacy

The privacy of our customers' data is one of Semble's primary considerations. The protections described in this document and other protections that we have implemented are designed to ensure that your data stays private and unaltered. Our products are designed and built with customer needs and privacy considerations at the forefront. Our privacy program incorporates best practices, customers' and their contacts' needs, as well as regulatory requirements.

Data Retention / Data Deletion

Customer data is retained for as long as you remain an active customer. Semble provides active customers with the tools to export their data.

Former customers' data is removed from live databases upon a customer's written request or after an established period following the termination of all customer agreements.

Information stored in replicas, snapshots, and backups is not actively purged but instead naturally ages itself from the repositories as the data lifecycle occurs. Semble retains certain data like logs and related metadata in order to address security, compliance, or statutory needs.

For customers on physically segregated instances, we offer the ability to define custom data retention periods.

Privacy Program Management

Semble's Compliance, Technology, and several other teams collaborate to ensure an effective and consistently implemented privacy program. Information about our commitment to the privacy of your data is described in greater detail in our Privacy Policy.

Breach Response

The Information Commissioner's Office (ICO) broadly defines a data breach as a security incident that has affected the confidentiality, integrity or availability of personal data.

If we become aware of a data breach affecting your data, we will inform you within 72 hours (or sooner if possible), as required under the GDPR. We will continue to keep you informed and work with you to meet any reporting requirements that may arise under the applicable data protection legislation.

Compliance

GDPR

Semble is fully compliant with the UK GDPR and Data Protection Act 2018. We have a dedicated Data Protection Officer (DPO) registered with the UK Information Commissioner's Office. Confidentiality, integrity and availability of the data we control and process are of paramount importance to us; with data protection training compulsory for all staff, and board-level oversight in place.

Other regulation

Semble complies with all applicable legislation, including Bribery Act 2010, Modern Slavery Act 2015, Computer Misuse Act 1990, Privacy and Electronic Communications (EC Directive) Regulations 2003 (PECR), and all relevant HR-related legislation. Our Legal & Compliance department maintains a comprehensive Legal Register, which is regularly reviewed and updated.

Document Scope and Use

Semble values transparency in the ways we provide solutions to our customers. This document is designed with that transparency in mind. We are continuously improving the protections that have been implemented and, along those lines, the information and data in this document (including any related communications) are not intended to create a binding or contractual obligation between Semble and any parties, or to amend, alter or revise any existing agreements between the parties.