SMARTABASE SECURITY

OVERVIEW

SMARTABASE

SMARTABASE is a J2EE application which is hosted on a military specification Linux derivative. SMARTABASE complies with HIPAA Title II requirements and with PIPEDA.

OUR GUIDING PRINCIPLES

The security infrastructure and policies underpinning SMARTABASE were created and are maintained using the following guiding principles:

- AVAILABILITY
- INTEGRITY
- CONFIDENTIALITY
- DURABILITY

THIS DOCUMENT

- SECURITY SUMMARY
- SECURITY FEATURES
- SYSTEM ARCHITECTURE
- BACKUP SOLUTIONS
- HOSTING OPTIONS

FUSION SPORT PTY LTD
76 Neon Street
Sumner Park QLD 4074
Australia

info@fusionsport.com
www.fusionsport.com
Ph: +61 (07) 3123 7124
Fax: +61 (07) 3123 4201

ABN: 70 103 526 147

Contact: Dr Markus Deutsch
Chief Executive Officer
Ph. +61 (07) 3123 7124
Mob: +61 423 837 410
markus.deutsch@fusionsport.com

Stay Connected!

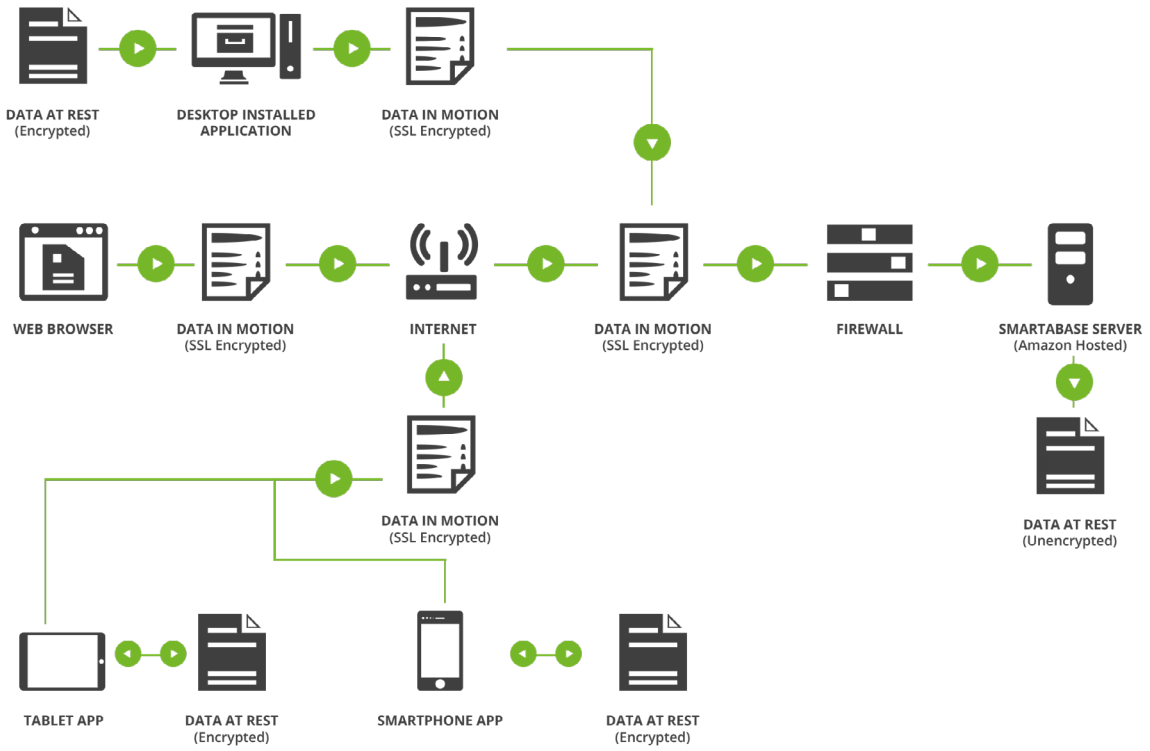
FusionSportInc

@FusionSport

HIPAA COMPLIANCE

PIPEDA

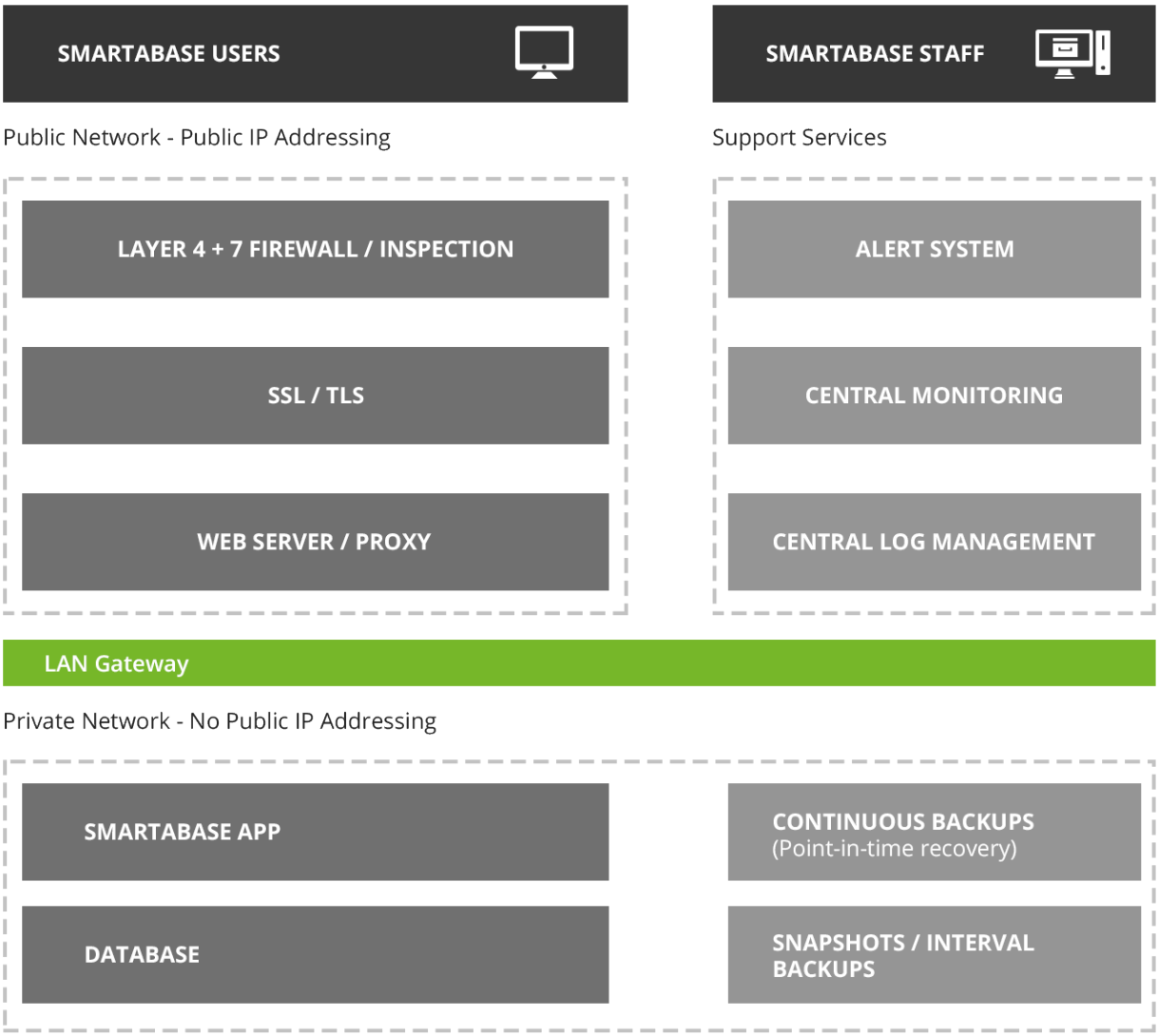
SECURITY SUMMARY



Fusion Sport uses controls on access to information which include procedures for authorising and authenticating users and infrastructure-accessing staff, as well as software controls for restricting access, and techniques for protecting data, such as encryption. Fusion Sport utilises isolated private networks with no public IP addressing of back-end assets that hold data. The SMARTABASE application's front-end is protected by proxies with both layer 4 and layer 7 traffic inspection and firewalling.

With regard to the security of SMARTABASE data, Amazon ensures that all data owing in and out of SMARTABASE (diagram) is encrypted using 128 bit SSL. This is the same technology used to protect internet banking transactions and is approved for HIPAA compliant medical data applications. All running volumes and data at rest is fully encrypted and backed up using systems designed to provide 99.999999999% durability and 99.99% availability of objects over a given year. When using the installed version of SMARTABASE, data at rest is stored in an Adobe Air database using the Advanced Encryption Standard (AES) with Counter in CBC-MAC (CCM) mode. When using the SMARTABASE app on a tablet or mobile phone, data at rest is protected within an SQLite database with SQLCipher providing 256-bit AES encryption in CBC mode.

With regard to monitoring and incident response, Fusion Sport has implemented SELinux enforcement and security tooling on all assets with centralised logging for continuous monitoring and rapid incident response times. Staff are on call 24/7.



OPEN PORTS

PORT	SERVICE	SECURITY METHOD
80	http	This port redirects to 443
443	SSL https	OpenSSL
22	ssh terminal	2048-bit Ed2551 advanced encryption / IP whitelisting

SECURITY FEATURES

AUTOMATIC BANNING TECHNOLOGY

SMARTABASE scans incoming traffic and pattern matches 'atypical' traffic and automatically bans the offending IP(s). SMARTABASE administrators have granular control over this behaviour and can unban or whitelist on request. The system also has a limit on failed password attempts. At the application level, as a security measure, users with multiple failed login attempts receive a temporary ban.

PENETRATION TESTING

SMARTABASE is tested using the latest and greatest automatic security-scanning software to date. If you would like to know more please contact our support team.

CLIENT-SIDE CONTENT SECURITY POLICY

To further mitigate any possible risk of cross-site script hacking, we have implemented a content-security-policy which restricts the source URL of all website resources and white-lists only a few trusted hosts. This policy is highly adaptable and can be set to suit your needs.

24HR ACTIVE MONITORING AND ALERTING

SMARTABASE utilizes software which actively monitors logs and in real-time can pattern match issues into specialised monitoring / alerting tools. This allows our system administrators to be notified instantly and respond quickly to a huge list of possible events.

DATA ENCRYPTION AND DATA INTEGRITY

User data is securely stored on fully encrypted cloud disk storage and compressed in unique block storage containers. Automatic data back-up procedures offer you four nines of data reliability (99.9999% reliability). Comparatively excellent in today's standards.

MOBILE APPLICATION SECURITY

As a basic security measure, we recommend cell phone data encryption and locking functions are set up for all users. SMARTABASE application data is also locked using 256 bit encryption in a local database. If these protections are not possible, or secure enough, you can direct users to use the SMARTABASE mobile website via the cell phone mobile browser.

SYSTEM ARCHITECTURE

The SMARTABASE system uses a client-server model with a number of options for both the client and server side. The server can be run virtually in the cloud or locally in the client premises data centre, depending on the IT requirements of the organisation. The server runs an instance of Linux which can be virtualised with VMWare 5.0 and utilises Java running on the Glassfish application framework. All data is stored in a PostgreSQL database on the hosting server.

The SMARTABASE system runs on Apache. This will be hosted by the SMARTABASE server from within the VM, so there will not be a requirement for the client to provide an Apache web server. The only requirement on the client side is the VMware itself and sufficient hardware to support the processing and storage needs of the application. SMARTABASE has no third-party licence implications.

The primary means for access on the client side is via a web browser on the local machine. This allows interoperability between all operating systems and web browser technologies. The client side runs through a monolithic JavaScript application and takes advantage of Google Web Toolkit. For this reason, the use of a modern browser such as Chrome, Firefox or Safari is recommended and the use of Internet Explorer is discouraged, due to its poor handling of JavaScript.

For organisations that use Internet Explorer as the primary or only browser, we simply recommend that users install the installed version of the application and use it instead of the browser. Some organisations choose to use this approach by default, irrespective of browser preference, as it ensures continuity for staff that are regularly using SMARTABASE offline.

An offline version is also available for PC, Mac OSX and Linux which uses Adobe AIR to create an installed version of the SMARTABASE client on the local machine. This local version includes an encrypted database with the required information from SMARTABASE and also stores any new data that is entered. When the user is next online any entered data is synchronised with the host server by choosing the login online option.

Mobile versions of the client are also available either via the web browser on the mobile device or via an installed application. Applications are currently available for Android and iOS (iPad and iPhone) devices. The installed applications include the ability to work offline via the use of a local database that can be synchronised when next online.

System deployment, management and monitoring is performed with Puppet Enterprise by Puppet Labs, giving scalability and flexibility to the installation.

BACKUP SOLUTIONS

SMARTABASE has a robust backup system with multiple simultaneous solutions to ensure maximum data redundancy. Data backups are compressed then encrypted using strong modern encryption to ensure they cannot be compromised. SMARTABASE backups cover everything with which a user interacts, including data, administrative framework, and built content such as event forms, profiles, dashboards and site architecture.

FREQUENCY

BACKUP TYPE	FREQUENCY	PURPOSE	LIFESPAN
Point-in-time	Continuous	We use a sophisticated time-based backup and recovery solution to create instantaneous snapshots of a SMARTABASE application.	21 days
Daily	Daily*	This is a scheduled backup of a SMARTABASE application, created at daily intervals.	21 days
Weekly	Weekly*	This is a scheduled backup of a SMARTABASE application, created at weekly intervals.	5 days
DB Volume	Bi-weekly*	This is a scheduled backup of the database volume, created at bi-weekly intervals.	1 year

*These backups occur in the agreed maintenance time window.

HOSTING OPTIONS

There are essentially three options for hosting SMARTABASE data. SMARTABASE can be either hosted by Fusion Sport on Amazon Web Services in EU, USA or Australian data centres (cloud-hosted) or on the client's server (self-hosted). Alternatively, SMARTABASE can use a combination: the SMARTABASE system and most data is cloud hosted, but some data (such as large video les) is hosted locally on the client's server. Over 90% of clients use Fusion Sport's cloud hosting service.

CLOUD HOSTING USING AMAZON WEB SERVICES

Fusion Sport uses the Amazon Web Services (AWS) EC2 infrastructure for all cloud hosted sites. Clients are allocated to either USA, EU or Australian servers based on client requirements and their local data storage legislature. AWS is backed by Amazon's service level agreement.

A comprehensive overview of the EC2 services, security and Service Levels can be found here.

SELF-HOSTING REQUIREMENTS

SERVER REQUIREMENTS

Should a customer elect to self-host their SMARTABASE application, the minimum server requirements are as follows:

1. Dedicated server or partition (minimum 8Gb ram) with large disks in a mirrored RAID configuration
2. Virtualization method, depending on your infrastructure
3. VPN between your network and ours (you can lock down the IP to our static IP)
4. Access to server via SSH or remote desktop, then we install a virtual machine image of our server to configure and manage it

Scalability of server storage and capacity is the responsibility of the customer. The above specifications are based on a standard application and should be seen as minimum requirements.

SECURITY AUDITING

Self-hosted SMARTABASE sites are able to conduct auditing within the SMARTABASE application itself using an audit trail module.