

THE SOLVEXIA SECURITY PHILOSOPHY

Security is an integral part of our business, an essential foundation upon which all our services are delivered. Protection of client data is fundamental to SolveXia's existence as a business and, as such, we ensure that all client information is secured at all times. Security has to be a central tenet of the way we operate in order for our business to thrive as an IP solution, attracting clients in banking, insurance and the government sector.

The importance of security has meant that it features in every stage of our development plan. This emphasis continues through every release of our software and is evidenced throughout our company. For example:

- Our solution design does not allow client data to be co-mingled as is the case with most other software-as-a-service providers.
- Our infrastructure does not store client data on shared hardware as is the case with most other software-as-a-service providers.
- Our infrastructure employs multiple levels of firewalls, using different vendors and technologies at each level to avoid systemic weaknesses in any one provider's technology.
- Our infrastructure is periodically reviewed by professional “penetration testers”. These tests employ the latest and most aggressive techniques in an attempt to compromise our system.
- Our project managers and quality assurance personnel receive regular training on the development and delivery of secure software design.
- Our daily operations routine includes explicit tasks to review and refine security measures.

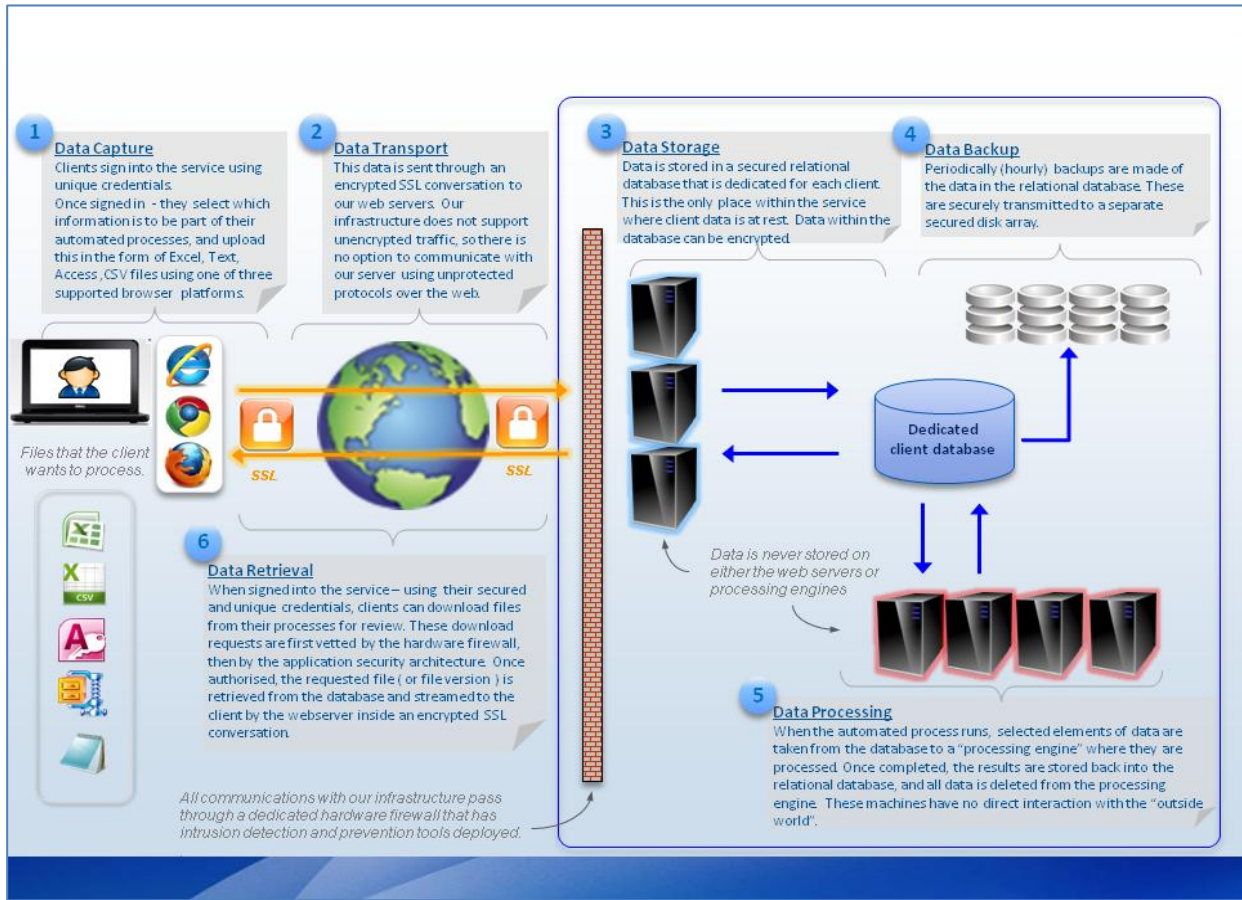
SolveXia's business plan recognises the central importance of security by allocating a significant amount of time and money to this area. We recognise that this is essential to both our survival and success.

SolveXia's development plan has, at any given point in time, at least one activity dedicated to improving the security of the solution. This reflects our belief that security is never “finished” but is a process of continuous review and improvement.

SolveXia's CIO, James Simpson, has many years of experience developing large scale, secure systems for Microsoft and its clients. James and the team work consistently with our banking clients who employ well-trained IT security specialists to understand and address any specific concerns as they arise. This practice has been in place since SolveXia commenced operations with its first client, Westpac Bank.

DATA FLOWS

The following diagram illustrates the data flows within the SolveXia solution:



DATA PROTECTION - ENCRYPTION

For data "in motion" SolveXia uses two levels of protection. First, all communication between our clients and our infrastructure takes place using SSL. This means all traffic is encrypted. Our infrastructure does not support unencrypted traffic preventing the possibility of unsecured connections being used accidentally. Within these encrypted conversations, we further encrypt highly sensitive data items such as user credentials with 256-bit AES encryption. SolveXia therefore provides two levels of encryption for data "in motion".

For data "at rest" everything is encrypted using 256-bit AES encryption. This applies to all "live" client data and backups of client data. The keys used for this encryption are not stored with the client databases. They are held by SolveXia in a secured offsite location and are themselves encrypted. This means that, should the database files or even the whole disks be stolen, it will not be possible to access stored client data.

SolveXia's Security Summary

DATA PROTECTION - FIRE WALLS

SolveXia uses a combination of hardware and software firewall technologies to provide multiple layers of defence. The outer hardware firewall layer (dedicated CISCO hardware) has both IDS (Intrusion Detection System) and IPS (Intrusion Prevention System) modules installed and operational. These IDS and IPS modules provide both “heartbeat” reporting to SolveXia staff to confirm their continued operation as well as immediate alerting in the event of suspicious activity. The IPS module is configured to automatically terminate and block connections that register any form of suspicious activity, without waiting for human intervention.

Each server within our infrastructure is also protected by a dedicated software firewall. This makes it possible to establish for each server a profile that determines what connection types are allowed and from which specific locations. As a consequence, each machine has a firewall configuration that provides the smallest possible attack surface.

DATA PROTECTION - BACKUPS

The SolveXia backup schedule provides for data recovery points every hour. This means that in the event of a service outage, on average, only 30 minutes of transactions will be lost. The worst case is 59 minutes of transactions being lost. The system has also been designed so that it is straight forward to re-run processes under such circumstances to replace any lost transactions.

SolveXia also has the ability to perform more frequent backups for clients as required. This allows the client data stored within the SolveXia platform to match any existing data protection profiles and policies that clients have in place for other systems.

The backups created in the above schedule are stored on a dedicated and secured RAID 5 disk array attached to the local database server and encrypted. This allows for extremely quick data recovery times when the root cause of the service outage does not destroy or invalidate the database server. These backup data sets are also copied to a physically separate backup drive array every hour to protect against the risk of data loss due to destruction of the database server itself.

In addition, clients typically store on their local systems copies of input data (which is uploaded or transferred to the SolveXia system) and the outputs resulting from processes that have been run. It is quite straight forward to supplement this data with the transmission back to the client of other intermediate or key files on a regular basis.

DATA PROTECTION – EXTERNAL COMMUNICATIONS

The SolveXia service provides clients with the ability to configure processes to send email and SMS messages. It is entirely at the client's discretion as to how these are used. Most commonly we see the email capability used to send summary information to stakeholders of a process and

SolveXia's Security Summary

SMS messages sent to indicate interim progress, error scenarios or process completion. In all cases, clients use these facilities in accordance with the same rules and policies that apply to email and SMS messages within their own organisations.

Additional security can be provided when using these channels but we ask clients to note:

- We can support email TLS where it is supported by the client email servers. This provides email server to email server security.
- We can support sender-to-recipient email protection using asymmetric encryption technologies such as PGP. This requires additional setup, co-ordination and training of client personnel on how to use this sort of email security technology. It does, however, provide a much stricter level of security and control than TLS.
- SMS unfortunately is not a form of communication that can have modern data protections applied. Consequently we advise clients only to send information via SMS that is consistent with their corporate policies regarding the general use of SMS.

SOLVEXIA'S XIAN DATA STRUCTURE

SolveXia has developed a propriety mechanism for organising data within its environment. This has been branded as its "Xian" structure. Whilst this provides a very flexible mechanism for arranging and accessing data, it also means that it is difficult for any unauthorised person to gain access to meaningful information without understanding how the data is organised.

There are three primary benefits to the Xian data structure:

- It allows the functionality of our service to rapidly adapt to ever-changing client requirements,
- It increases the level of consistency with which data is stored and organised thereby improving data integrity, and
- It obfuscates the structure of any particular client's processes or data therefore improving security.

Please note that this is a data format and organisation; not database technology. We use proven enterprise level database technology (SQL Server 2008 R2) for all RDBMS operations. The Xian structure refers to the schemas and mechanisms implemented on top of SQL Server 2008 R2.

ENTERPRISE GRADE INFRASTRUCTURE

SolveXia's servers are housed at GoGrid's data centre in San Francisco. The building also houses "super-nodes" for Verizon and AT&T local phone services in San Francisco and it is considered an "essential" facility because 911 emergency calls are routed here. SolveXia, through GoGrid, shares generators, power, cooling and fire suppression infrastructure with

Verizon, including dual 2 Megawatt generators that support the critical power requirements and operations of the building. Our dedicated servers are secured, managed and monitored in a state-of-the-art facility. GoGrid also operates a similar facility on the East Coast of the USA, which SolveXia utilises for disaster recovery purposes.

ACTIVE MONITORING AND COMMUNICATION PROCEDURES

SolveXia has monitoring and reporting tools that are constantly checking the state and status of our database infrastructure. These tools provide both alerts and “heartbeat” style information to inform our support team that everything is OK (and that the monitoring tools are functioning). Alerts result in email and SMS messages being sent to the development team within SolveXia advising them to take corrective action.

SolveXia's system has been constructed to provide constant feedback on client activity. Development and support teams monitor a range of events, including errors in client processes and problems with the software. These teams are often aware of a faulty configuration or application of a client process before the client appreciates the inconsistency. Upon discovery, the client support group within SolveXia is informed and the client in question is called directly to advise on the corrective action to be taken. Clients are usually informed within minutes of the discovery of an error, omission or inconsistency.

The monitoring system has been designed with flexibility in mind and can easily be adapted to monitor specific client requirements such as excessive data transfers or to notify issues to a client's support team via text messages.

As a last resort, the extensive process documentation automatically generated by use of SolveXia's software provides a ready reference to manually complete automated tasks. In fact, some of SolveXia's clients encourage their staff to manually perform the processes of the business once a year, not so much as a backup procedure but more to keep the knowledge of its subject matter experts up-to-date.

MONITORING BY GOGRID

SolveXia's monitoring and reporting tools run independently of those operated by GoGrid and, as such, provide separate, additional monitoring of our infrastructure. In the event that a server encountered a problem or became unresponsive and this was detected by GoGrid personnel ahead of SolveXia personnel, our reporting agents at GoGrid would immediately notify SolveXia by phone/SMS and email.

ONLINE THREATS – REGULAR PENETRATION TESTING

SolveXia employs the services of an independent, specialist security firm to ensure that the highest levels of security are being adopted by the business. Sense of Security (SoS) provide

enterprise consulting services to organisations that need to protect information and remain abreast of current and emerging threats in the online world.

SolveXia engages SoS to:

- (a) Review our security stance in the context of real world threats and recommend how we can further tighten our security. We currently arrange for an 'arm's length' review to be conducted at least 3 times a year, and
- (b) Provide technical and awareness training to our R&D team, including both project management and quality assurance personnel, so that secure application development practices can be embedded into the foundation levels of a solution.

Our motivation for using SoS in this way are:

- We believe that having an independent, reputable outside agency to conduct the review will always be more effective than internal reviews alone,
- We believe that threats are evolving and emerging so quickly that the lifespan of any particular review and action plan is never more than 5-6 months, so we are targeting updates every 4 months, and
- We believe that we will deliver a more secure service if all our staff are fully aware of the current and emerging issues in online security and how to manage them.

CONTINUOUS VERIFICATION OF KEY PROCEDURES

An important part of providing a highly reliable service is to constantly test the procedures that are used to provide protection. The table below summarises the procedures that are tested regularly by SolveXia.

Process	Notes
UNINTERRUPTABLE POWER TESTING	<p>This is tested at least monthly and whenever a change is made to the power infrastructure. This test ensures that the real time (battery-based) UPS power supplies automatically engage with adequate charge when required.</p> <p>GoGrid contacts all customers (including SolveXia) prior to these tests and they are conducted with no interruption of service.</p>
BACKUP GENERATOR TESTING	<p>This is tested at least monthly and whenever a change is made to the power infrastructure. This test ensures that the backup diesel generators used to supply power in a sustained power failure are in good working order and can deliver the required power to the data centre.</p>

SolveXia's Security Summary



Process	Notes
CONFIRMATION THAT BACKUPS HAVE COMPLETED SUCCESSFULLY	GoGrid contacts all customers (including SolveXia) prior to these tests and they are conducted with no interruption to the service.
CONFIRMATION THAT THE DATA BACKUPS ARE OF VALID FORMAT	SolveXia is notified daily with the status of the backup processes. These reports include details that confirm each client database has been backed up. Every month SolveXia operations staff use sample client backup data to run through a trial restore process. This verifies that the format of the backup is being maintained in a manner that lends itself to recovery.

ADDITIONAL INFORMATION

If you need any additional information, please call SolveXia's CIO, James Simpson on +61-2-9386-0202 or by email at james.simpson@solvexia.com.

SolveXia
August 2011