# SolveXia's Security Summary

## 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 employs multiple levels of protection, 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.
- Our staff do not access client data without permission from the client.

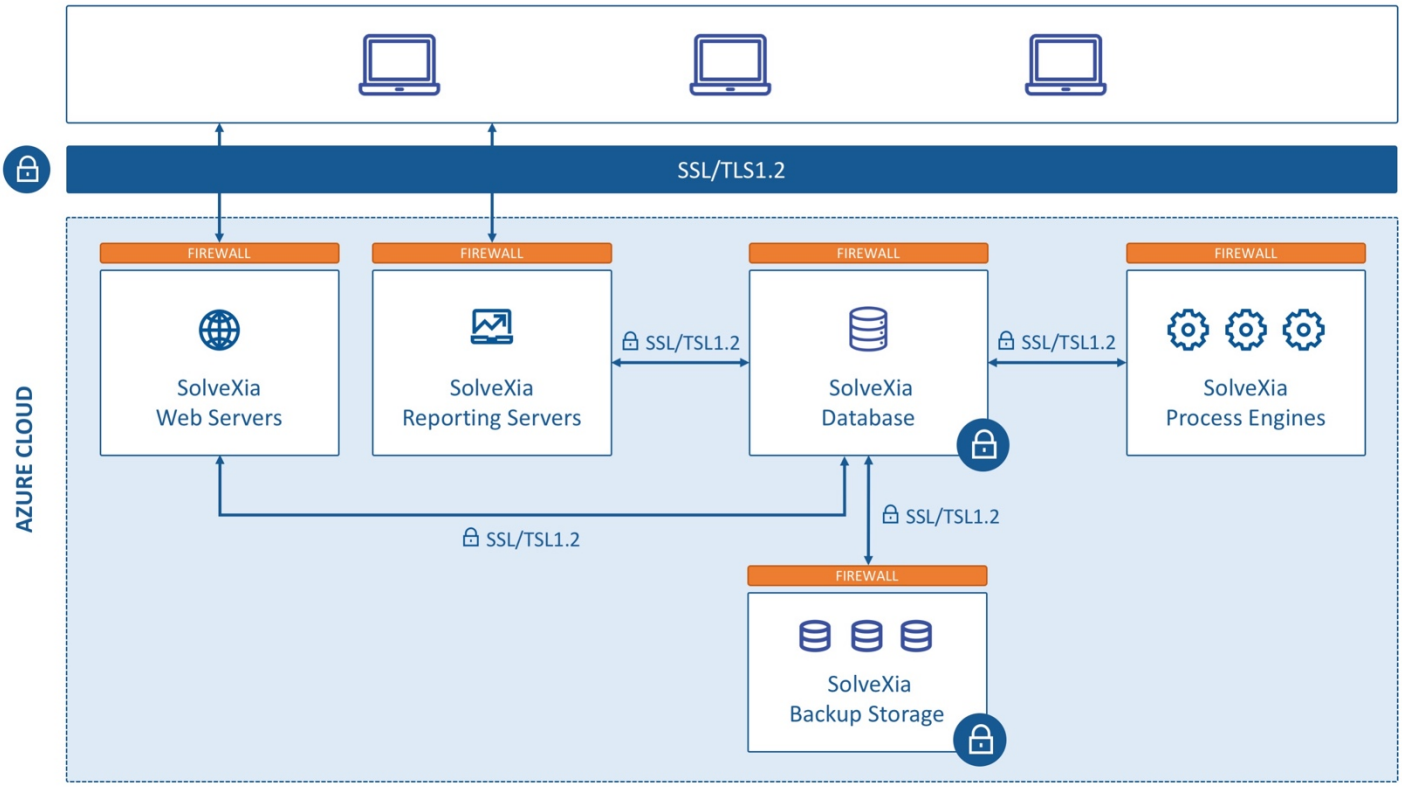
SolveXia's business plan recognises the central importance of security by allocating a significant amount of time and money to this area. We recognise that this is essential to both our survival and success.

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 CTO, Paul Cartwright, has many years of experience developing large scale, secure systems. Paul 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.

## SOLVEXIA INFRASTRUCTURE

SolveXia's production systems are hosted at Microsoft Azure cloud service data centres located in Australia and Northern Europe. Microsoft is responsible for the physical, environmental and operational security controls for the SolveXia infrastructure. SolveXia manages and controls the logical, network and application security of our software and infrastructure.




The SolveXia infrastructure consists of the following components:

### SolveXia Web Servers

SolveXia web servers serve the main SolveXia application for users and process user requests. Traffic to the web servers passes through the load balancer to ensure all web servers maintain stable production performance. SolveXia web servers write all changes in user data to SolveXia databases.

Communication sessions between SolveXia web servers and SolveXia databases are encrypted using Secure Sockets Layer (SSL)/Transport Layer Security (TLS) 1.2.

### SolveXia Databases

SolveXia stores all clients' data in SolveXia Enterprise Edition SQL Server databases. Each client database is encrypted, isolated and secured. SolveXia database infrastructure has no direct path to the Internet.

### SolveXia Processing Engines

SolveXia processing engines handle data processing and manipulation while running processes in the SolveXia application. The results of the processing are being stored in the SolveXia databases mentioned above. SolveXia processing engine infrastructure has no direct path to the Internet.

Communication sessions between SolveXia processing and SolveXia databases are encrypted using SSL / TLS 1.2.

### SolveXia Reporting Servers

SolveXia reporting servers process user requests and provide business intelligence (BI) reporting integrated with the SolveXia core application. SolveXia reporting servers link to clients' data in SolveXia databases.

Communication sessions between SolveXia reporting servers and SolveXia databases are encrypted using SSL / TLS 1.2.

### SolveXia Backups

SolveXia performs regular database backups and stores them in the isolated SolveXia backup storage. All backups are encrypted, geo-replicated and secured using a strong cipher. Communication sessions between SolveXia processing and SolveXia databases are encrypted using SSL / TLS 1.2.

Each component is isolated and protected by a multi-tiered network topology and security devices.

## DATA PROTECTION - ENCRYPTION

SolveXia data at rest is encrypted using 256-bit Advanced Encryption Standard (AES). For data protection in transit between SolveXia web application and our servers, SolveXia uses SSL / TLS 1.2 for data transfer, creating a secure tunnel protected by 256-bit Advanced Encryption Standard (AES) encryption

SolveXia's key management infrastructure is designed with technical and procedural security controls with very limited direct access to keys. Encryption key generation, exchange and storage is held and processed by SolveXia in a secure offsite location.

## DATA PROTECTION - FIREWALLS

SolveXia uses a combination of hardware and software firewall technologies to provide multiple layers of defence. The outer hardware firewall layer 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. The logs produced by these firewalls are routinely analysed for any deviations from normal client activity.

Each server within our infrastructure is also protected by a dedicated software firewall. This makes it possible to establish a profile for each server that determines which 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.

Our current architecture provides us with a multitude of protection and mitigation strategies when it comes to securing our application. Amongst these are a comprehensive DDoS protection layer and multi-tiered network topology, providing traffic isolation between multiple production machines. This architecture provides no direct path from the internet to core infrastructure, all traffic to the core infrastructure must traverse through a series of security devices.

## DATA PROTECTION - BACKUPS

The SolveXia backup schedule provides for daily data recovery at the primary site. 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 utilises Microsoft Azure's triple replication and geo-replication of client databases. It utilises Microsoft's highly secure, state-of-the-art data centres in Sydney and Melbourne or Dublin and Amsterdam in Europe. The backups are also encrypted. This allows for rapid data recovery times.

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 – ACCESS CONTROL

SolveXia's employee access to our environment is protected and authenticated by using strong passwords, SSH keys and two-factor authentication. Remote access to our production and

corporate environments requires the compulsory use of a VPN. Our security team vets and monitors team all logins and access to our software and infrastructure.
We strive towards a Zero Trust security model, where we do not automatically trust anything inside and outside the SolveXia environment. Instead everything attempting to connect to the system must be verified and before access can be granted.

In addition, we approach staff access controls using a least privilege model. Providing access to systems and infrastructure on a time limited basis and only to parts of the system that the staff member will be working on.

## 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 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 proprietary 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 2014 Enterprise Edition). The Xian structure refers to the schemas and mechanisms implemented on top of SQL Server 2014.

## 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.

This procedure currently operates mainly in Sydney business hours to reflect the current location of SolveXia's clients, but out-of-hours support is also available from our staff in India and the UK. 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 MICROSOFT

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

## ESCALATION AND NOTIFICATION PROCEDURES

Even with all of the built-in protection, it is important to have a well-defined set of escalation procedures in place in the event of an incident. The notes below summarise our default process, although, if requested, we have the ability to customise these procedures for each client.

1. Each member of the SolveXia management team is informed of the breach by phone in the following order:
    - Chief Technology Officer
    - Head of Technical Sales
    - Managing Director
2. The client technical contact is immediately informed of the breach by phone by SolveXia personnel with the following order of preference:
    - Chief Technology Officer
    - Head of Technical Sales
    - Managing Director
    - Deputy Head of Development Team
3. Any other client appointed contacts are informed by SolveXia' s account management team in accordance with the agreed arrangement.
4. All client appointed contacts receive a follow up email from SolveXia's CTO, Head of Technical Sales or Deputy Head of Development to inform them of (a) the breach, (b) the nature of the problem, (c) a description of the verbal communication that has occurred between SolveXia and client personnel, and (d) the corrective action being taken.
5. At the very least, hourly communication is maintained between SolveXia's development team and the designated client technical contact unless a different update schedule is agreed in writing between SolveXia's CTO or Head of Technical Sales and the client designated technical contact.
6. This communication continues until full resolution of the breach has been confirmed in writing by SolveXia and agreed in writing by the client's designated technical contact.

In the event of a breach of security, SolveXia will work cooperatively with all relevant client personnel to describe which, if any, data was accessed and the action being taken to prevent a recurrence.

## 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 | 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. Microsoft Azure contacts all customers (including SolveXia) prior to these tests and they are conducted with no interruption of service. |
| BACKUP GENERATOR TESTING | 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. |
| CONFIRMATION THAT BACKUPS HAVE COMPLETED SUCCESSFULLY | SolveXia is notified daily with the status of the backup processes. These reports include details that confirm each client database has been backed up. |

| Process | Notes |
| --- | --- |
| CONFIRMATION THAT THE DATA BACKUPS ARE OF VALID FORMAT | 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 CTO, Paul Cartwright, on +61-2-9386-0202 or by email at paul.cartwright@solvexia.com.

**SolveXia**
August 2018

**Reviews**

| Date | Amended / Reviewed by | Reviewed / Approved by | Reviewed / Approved by |
| --- | --- | --- | --- |
| 28Feb16 | Paul Cartwright | Mark Schneider | Jonathan Glass |
| 21Sep16 | Paul Cartwright | Mark Schneider | Jonathan Glass |
| 19May17 | Paul Cartwright | Mark Schneider | Jonathan Glass |
| 28Nov17 | Paul Cartwright | Mark Schneider | Jonathan Glass |
| 08Aug18 | Alexandra Mourzina | Mark Schneider | Jonathan Glass |