TrustSphere

3 Phillip Street,
13-03 Royal Group Building,
Singapore 048693
www.trustsphere.com

Information Security Practices

Contents

TrustSphere Customers make use of TrustVault on cloud services for one of the following purposes:

- **Production TrustVault services for "Messaging Intelligence":** The relationship data held is derived from the customer's email and communication systems and can be made available through TrustView, a CRM plugin or directly through APIs.

- **Proof of Concept:** The cloud services are used on a temporary basis to upload data from the customers email and/or communications systems for the purpose of a trial of the TrustVault and client technologies

- **False Positive "Discovery":** The cloud services are used on a temporary basis to upload data, as for a PoC, but for the purpose of a False Positive report only (produced by TrustSphere analysts).

All these services require customer data to be uploaded and reside in TrustSphere's cloud services such that this data can be queried or made available to the customer or to TrustSphere.

This Appendix briefly describes the security of the TrustSphere cloud services:

- Physical security
- Network security
- Vulnerability and patch management
- Application security
- Data security
- Machine security
- Employee compliance

1 Physical security

The TrustVault cloud services are hosted with TrustSphere's hosting partner: Rackspace. Therefore, Rackspace control physical security for the cloud services. Rackspace provides comprehensive security as described in the following linked document. Rackspace complies with the following security standards:

- ISO/IEC 27001:2005
- PCI-DSS
- ISAE 3042

Full details can be found here: http://www.rackspace.co.uk/about-us/security

2 Network security

- All servers run firewall software, allowing access only to required applications
- Administration is via SSH (Secure shell), firewall controlled, restricted to clients originating on TrustSphere's corporate headquarters IP address range.
- Each server within the TrustSphere cloud has a separate access account and password.
- Each server also uses two factor authentication
- Control of two factor account access is based on a third party's server, including full audit logging, enabling easy provision and de-provision of accounts
- Access to the machine O/S is only allowed for trusted staff members; no access is allowed for customers

3 Vulnerability and patch management

The server O/S vulnerabilities are monitored using industry standard alert notifications. Any vulnerability that can be used to gain access to or affect the running of servers is applied as quickly as possible.

Vulnerabilities that affect applications, libraries or sub-systems that are installed, but UNUSED on the machines are not updated; a review is made of the sub-system containing the vulnerability to ensure that it cannot impact running services in any way. The sub-system is removed if possible, or otherwise completely disabled.

Upgrades to TrustSphere's own software happen three times a year, and patches are introduced as needed, should issues arise.

4 Application security

Access to the Administration console of the TrustVault application is available via an SSL web page.

Some customers are given their own username and password access to the console. Customers are encouraged to follow current recommendations for password strength including the use of mixed case, numbers and punctuation characters.

A breach of a customer's administration password will give access to that customer's relationship data.

TrustSphere uses passwords greater than 15 characters, with mixed case and character types. Passwords are changed on a regular basis.

5 Data security

TrustSphere runs a single, multi-tenant cloud service for most customers. In addition, a number of separate services are operated for customers requiring a greater degree of security.

In the multi-tenant system, data for different customers is held in the same database. Data is segregated by use of the customers 'id' or 'domain group', making it impossible for one customer to view or modify another customers data.

If a separate service is run for a customer, only their data is present on the server(s) that constitute that service.

5.1 Data upload security

Data is always pushed to the TrustVault cloud from a customer's network. The client 'connectors' that upload the data are all SSL capable and will be configured to use SSL by default. The connector might use the SFTP protocol or will use the 'query API', both of which require a username and password specific to that connector and customer.

The email connector for Google Apps send a copy of the original messages to the TrustVault systems. The customer is in control of the configuration rules that enable the copies to be sent, and these will be configured to use TLS (SSL) security where it is possible with the email service.

The email connectors for Office365 and IBM SmartCloud pulls the message trace/journal logs using an account for that purpose, which has limited access to the cloud system.

5.2 Data retention security

The data held consists of:

- relationship data: Details of connected senders and recipients along with counters and date fields
- message metadata: Limited details about each message; timestamp, sender, recipient, subject, size, id retained for a limited period. (No message body data is uploaded or retained).

Data is held in two NOSQL databases which use their own proprietary formats. At this point, data is not encrypted due to the performance requirements of the service. Security is assured by the other methods described in this document.

5.3 Data access security

Data is made available to client applications (e.g. TrustView, CRM plugins) by the Messaging Intelligence API. The API is available via SSL and requires a username and password to access data for specific customer domain groups.

5.4 Email copy security

When a copy of an email is received from a cloud email provider, the TrustVault email connector MTA creates a new process and receives the message into memory. All required metadata is collected and the message is then immediately deleted. Only under exceptional circumstances (e.g. heavy load) is the message be written to a queue on disk – should this happen, the disk copy is removed as soon as processing is complete.

6 Machine security

Should a customer terminate their TrustVault service, all data and accounts are removed from the service within 45 days of their termination.

Should a separate service be terminated, the data and accounts are removed and scrubbed before the server itself is decommissioned.

7 Staff and Contractor compliance

TrustSphere ensures all employees are aware of and periodically affirm their understanding of and compliance with the current Data Handling Policy (as amended).

This policy is specifically referred to in all employment contracts and contractor agreements.

During the orientation and staff on-boarding process, the importance of Data Handling is emphasized to all new team members.

TrustSphere has a formally nominated Data Protection Officer - currently Roland Turner.

TrustSphere is an active participant in various industry bodies and associations including the Online Trust Alliance www.otalliance.org and the Messaging Anti-Abuse Working Group www.maawg.org and regularly updates its policies and practices to ensure adopt the latest best industry best practice.

