Security & Compliance
Frequently Asked Questions

Date: June 2023

Version: 1.1

This document contains proprietary and confidential information and may not be shared with any 3rd party without the express written permission of Transvault.

IMPORTANT: The information in this document is to act as a guide only. Transvault shall not be liable for technical or editorial errors or omissions contained herein. No warranties or any kind are made, including the accuracy of the information contained herein, or whether this information reflects the latest capability of the technology referenced.

www.transvault.com

Contents

1. How do you ensure the security of your software?

We implement the GDPR best practice of "Secure By Design and By Default" to ensure that normal operation of our software in inherently secure. We rigorously test any changes for functional or security defects and automate industry best practice testing within our software build pipeline. To validate this, we regularly and independently Penetration Test our software and ensure that no security issues exist.

2. What security training does the Transvault Team receive?

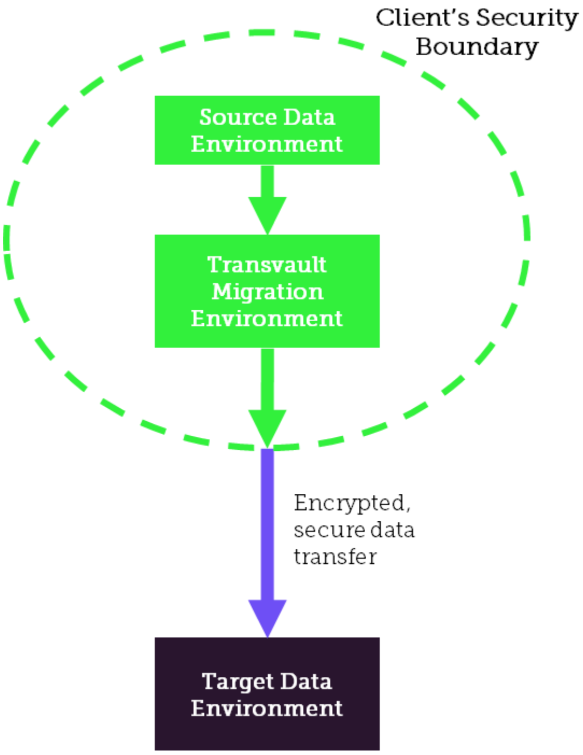
Every member of the Transvault team must undergo audited security training when joining the team to ensure that they are able to operate to our security standards. Any deviation is addressed, and the individuals are tested until they understand and pass. In addition to this, all team members have regular education and testing on the most prevalent security risks, with their understanding tested and their speed of response to the training graded. Where necessary, we also undergo formal and mandatory training for any changes to our security policies or stance to reflect the changing nature of IT security.

3. How does Transvault ensure data compliance when migrating?

Transvault migrations operate within the client's security boundary, thereby respecting the client's investment in security and leaving them in control of their data throughout the migration.

Clients have full access to Transvault's migration environment. A secure-by-design architecture for data transport enables complete transparency and governance.

This method of migration is viewed as the gold-standard for clients in regulated industries owing to its secure method of migration.


Client's Security Boundary
Source Data Environment
Transvault Migration Environment
Encrypted, secure data transfer
Target Data Environment

Our software is able to migrate data in one step. Where others may land data in a temporary location and intermediate format, we are able to do this in-line and therefore reduce the potential for data to be exposed. We encrypt data on-the-wire to ensure that data cannot be exposed in transport, and we have the ability to perform hash validation between the source and target message if a customer wishes to have that additional layer of validation. We leverage a chain of custody process, best practice in secure data transfer, to ensure that every message migrated is mapped and any data which cannot be migrated (source data corruption, etc.) is audited and remedied wherever possible.

4. What do you mean by ‘Chain of Custody’ and why is it important?

Chain of custody refers to the reliable recording of processes and procedures that occur while evidence (physical or electronic) is being captured, held, transferred or disposed of.

It is vital that the data in question has remained free from alteration and that secure handling has been provided at all stages. This is important since any later data investigation or discovery against migrated emails will seek to validate that the data has been handled correctly and that nothing was amended or missed out.

If possible, transferring your archives in one step, end-to-end, is the best way to preserve chain-of-custody. This approach avoids any chance of manual intervention or loss of tight control.

Other migration techniques that involve extraction to interim storage areas and file formats (such as PST or EML files) risk your data being inadvertently lost, maliciously tampered with, or indeed corrupted while they are waiting to be ingested into the target archive. It is therefore difficult to vouch for the security of your data ‘in transit’.

Transvault’s wide range of platform-specific connectors avoids the need to use interim storage, plus its optimized performance makes it viable to move directly across the network without making copies of your archive. Additionally, Transvault’s forensic message level auditing provides evidence that all of your source data has been successfully transferred to its final destination, and provides both a source ID and target ID.

5. How can I find out if Transvault has migrated all of our data?

Transvault includes comprehensive auditing that tracks the migration of each individual item. In the event of a future eDiscovery, the audit enables you to prove that you have not lost items during the move and that chain-of-custody has been maintained. Reporting is also available to highlight how much data has been migrated for each ‘mailbox‘ in the archive. As Transvault migrations are non-destructive, you have the option to validate any or all of the migrated data before you remove your original data.

6. What happens if an item fails to migrate?

As your data is migrated, Transvault carries out a series of integrity checks to ensure your email records will be viable post-migration. Any items that fail to migrate are automatically re-processed a specified number of times and/or at a different time of day. In the event of a permanent failure, a full log of the item(s) in question is produced and handled to our security standards to enable investigation.

'Permanent' failures tend to be low – typically 0.001% of the overall email quantity. They are usually attributable to pre-existing problems in the source archive such as data corruption (i.e. not caused by the migration process). As such, it is likely that these items would NOT have been picked up by any audit or eDiscovery exercise.

If your organization requires further investigative work to be carried out on failed items, data remediation services are available to help and where possible, address the problem to the satisfaction of your legal team.