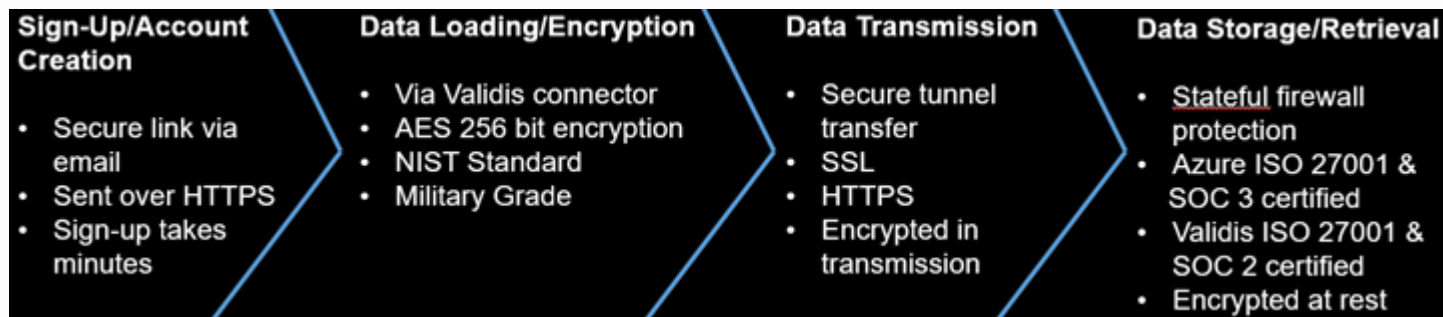# Security Overview

The below gives you a quick visual to help you understand how the tool protects your information through the signup, data upload, data transmission, and storage/retrieval process. At our company data security is our top priority. The tool is sourced from an ISO27001-certified organization. In conjunction with Microsoft Azure, the tool maintains the highest level of security.

Microsoft Azure is ISO/IEC27001 & SOC 2 certified which covers all the data uploaded to and used by Validis.

Sign-Up/Account Creation	Data Loading/Encryption	Data Transmission	Data Storage/Retrieval
• Secure link via email • Sent over HTTPS • Sign-up takes minutes	• Via Validis connector • AES 256 bit encryption • NIST Standard • Military Grade	• Secure tunnel transfer • SSL • HTTPS • Encrypted in transmission	• Stateful firewall protection • Azure ISO 27001 & SOC 3 certified • Validis ISO 27001 & SOC 2 certified • Encrypted at rest

Validis

Security FAQs

Data Transmission

How is data secure when uploading or downloading?

Data extracted from End Users accounting software is encrypted before transmission to the application.
All file uploads and downloads to/from the server happen over an encrypted channel encrypted channel using SSL.

Data Access

Who can access my client's data?

Access to all data is restricted to Client authorised users. All customer data and user management is completely controlled by the Customer.
Adaptive maintenance required to correct issues, or unexpected data elements sometimes requires access and is highly restricted to key members of the engineering team in the performance of their roles. All activity on the production servers is audited.

Platform Access

Who can access the platform client's data?

Environment Access Valdis administrator members have access to the production environment and is highly restricted to key members of the engineering team in the performance of their roles. All activity on the production servers is audited.

Encryption

Is my client data safe if a breach occurred?

All data written to Azure Storage is encrypted through 256-bit AES encryption, one of the strongest block ciphers available. Encryption at rest is provided by TDE on Database Encryption in transit is provided by TLSv1.2 throughout any external access to our service.
All external traffic between client and server is encrypted using SSL.

Process and protocols

Policies & process to manage and host data

Vaildis is ISO 27001 and SOC2 certified. Policies and procedures are independently audited every year.

Platform

Where is the Service hosted?

Vaildis is hosted on the Azure platform. Azure Architecture: availability sets are isolated locations within an Azure region and geographically separate data centres.

Penetration testing

Application vulnerability checks?

Vaildis performs penetration tests for every major release or annually using a trusted third party. The results can be shared in summary form.

Validis™

Knowledge Base Links

[How does Validis 'Connect' access my data? – Validis Support](#)

[How is my data protected? – Validis Support](#)

[What does Validis extract from my accounting package? – Validis Support](#)

[Will the Validis team have access to my data? – Validis Support](#)

[What are the risks to my systems and data? – Validis Support](#)

[Security Incident Response - Can I see your process? – Validis Support](#)

Validis™