› Service Overview

SAS® Results Customer DATA Security

Whether this involves profiling and segmentation, retention, response modelling, visualization, fraud or forecasting – SAS can develop a system that adds competitive advantage to your organization.

Data Handling and management for SAS Results on AWS

SAS Results leverages the expertise of SAS to develop analytical models and insight that help organizations generate quick ROI with their data. Whether this involves profiling and segmentation, retention, response modelling, visualization, fraud or forecasting – SAS can develop a system that adds competitive advantage to your organization.

Environmental Security

The SAS Results environment is a cloud environment on AWS (Amazon Web Services), where each customer is provided with a unique and secure environment into which the customer data is transferred for SAS to provide analytical services. The data is managed and stored for the duration of the project, and then destroyed by the date agreed on by the customer and SAS.

There are security policies in place by AWS to ensure the environment is secure and only accessible by the account holder (in this case SAS), and users specified by the account holder. (Please refer to http://aws.amazon.com/security/).

The only touch point the customer has to the system is through the Secure FTP server. The customer's public IP address will be white listed, and as such only the customer will have access to the Secure FTP server. The customer will also be provided with their own unique username and password. Data is then moved and stored on a SAS Platform Server that is dedicated purely to processing the customer's data.

The Customer's dedicated SAS Server is only accessible by SAS Staff who are connected to SAS' corporate network. The server where the data is actually stored is not visible or accessible via the public internet therefore adding an additional level of security.

The machine built to do the analytical work is stored on AWS (in the customer's local region) and is maintained by SAS Solutions on Demand. There are individual SAS logins assigned to SAS staff to ensure enhanced security.

Delivered by

sas Solutions OnDemand

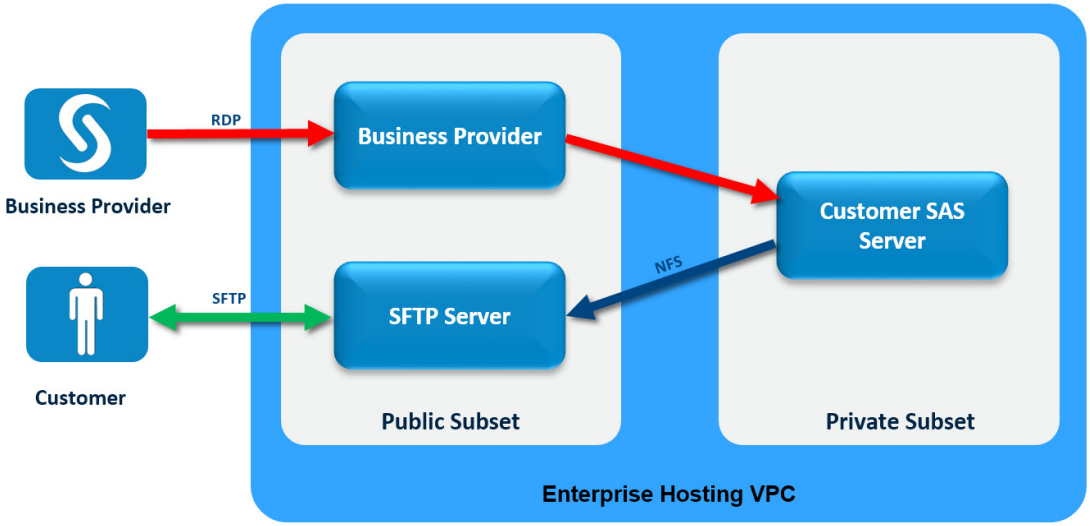

Figure 1: SAS Results Environment

The Customer's dedicated SAS Server

To ensure the privacy and security of the customer data received, SAS Results has processes in place to minimise exposure of any customer data to all external environments and people.

SAS Results achieve this by:

- The customer has the option to encrypt their data at the customer site before being transferred. This can be achieved with freeware such as 7zip.
- All data is transferred directly from customer site to the SAS Results Secure FTP server minimizing the chance of touching other networks.
- All data is moved from the Secure FTP site to the Customer's dedicated SAS instance within SAS' private AWS subnet.
- Data that was encrypted by the customer is decrypted only when within the SAS secure environment.
- All data is stored persistent on storage and is encrypted at rest with 256bit file encryption.
- Access to the platform and data is limited to named individuals, i.e. authorized SAS employees, contractors or consultants who have gone through formal SAS Solutions OnDemand training and approval processes, and who have acknowledged their responsibilities to ensure ongoing information security.
- Any data returned follows the same process as when first received by SAS.
- Upon completion of the project the data and environment is dissolved by SAS (please refer to the Data Deletion process below).

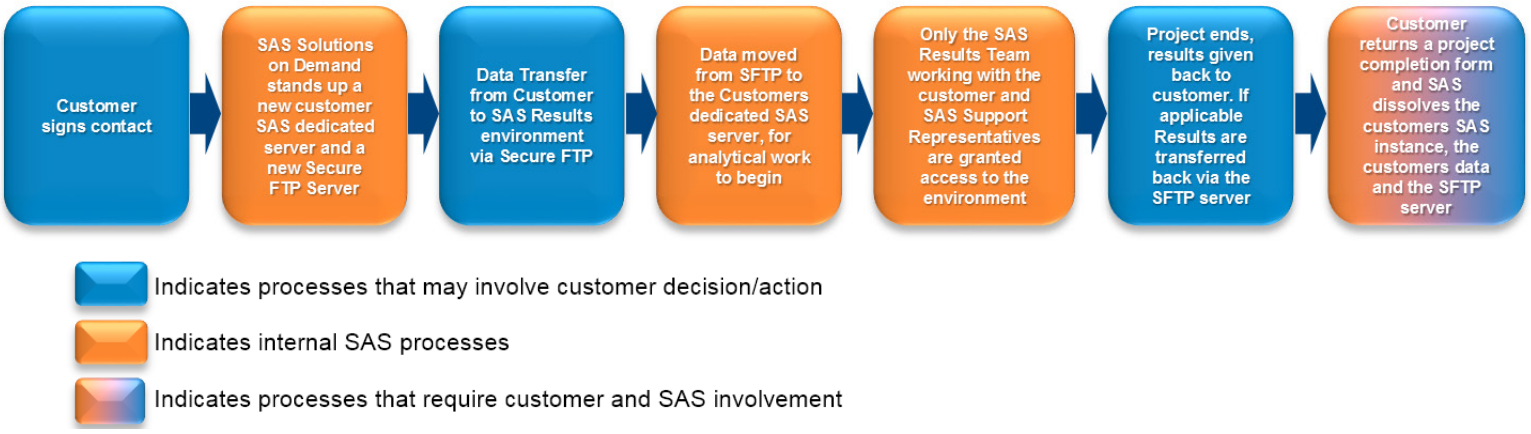

Figure 2: How SAS Manages and Handles Customer Data

Data Privacy Handling and Management - Overview

Each country has their own data privacy laws. A comprehensive list can be accessed here https://informationshield.com/policy-tools/international-data-privacy-laws/. SAS works with our customer's to understand the individual privacy laws in place and provide advice on how to ensure the data being passed is compliant with the privacy act as a part of the data handling process.

Data Transfer Process - How does the transfer process work?

SFTP (stands for SSH File Transfer Protocol, but also known as Secure FTP) is a computing network protocol for accessing and managing files on remote file systems. SFTP also allows file transfers between hosts. Unlike standard File Transfer Protocol (FTP), SFTP encrypt commands and data both, preventing passwords and sensitive information from being transmitted in a clear form over the public internet.

By transferring encrypted data via an SFTP method, there is extra security, as SFTP as a process encrypts the transfer command to prevent sensitive information being shared over a network.

If a customer encrypts their data before transmission, the decryption of the data only happens once the data is moved from the secure FTP environment and is on the Customer's dedicated SAS Server.

The server address of the secure FTP environment is unique to the customer and will be shared with the customer to perform the transfer process behind the security of their firewall.

The AWS security group will only permit transfers from the customer's network meaning access will be denied from anywhere else in the world. Customer's will also be given a unique username and password as an additional layer of security.

Once SAS is notified that the data transfer is complete the data will be moved internally within AWS from the SFTP server to the customer's dedicated SAS Server. The SAS server is only accessible by assigned SAS staff.

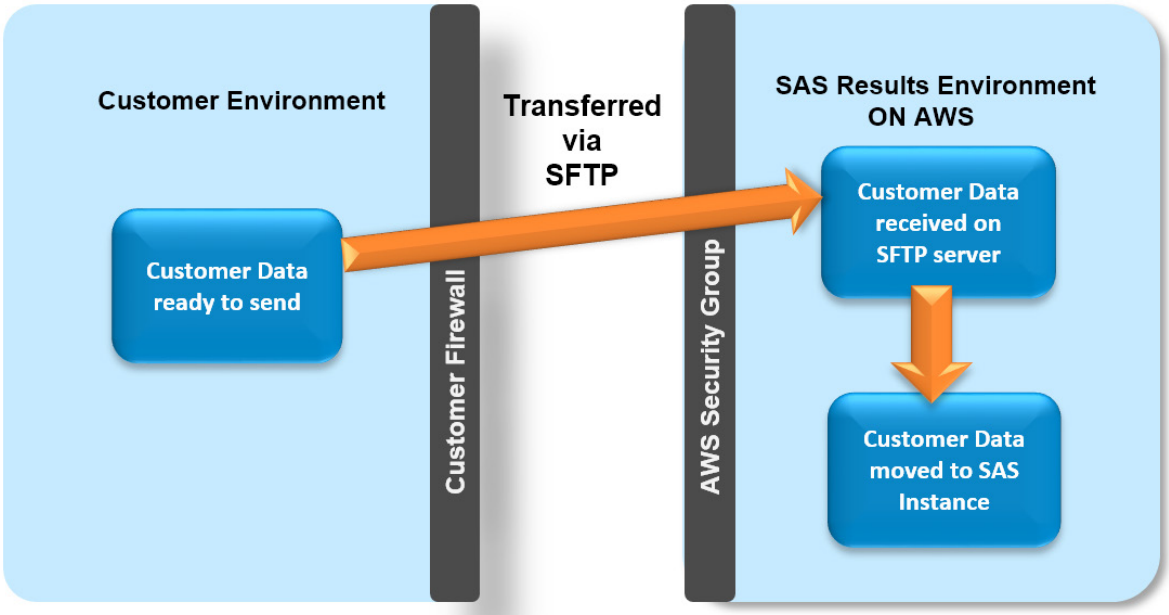

Figure 3: How the Transfer process works

Data Deletion Process - How can I be sure the data has been deleted?

Upon completion of all project(s) the data and environment is dissolved by a date agreed on by the customer and SAS.

What this process involves:

- Customer will be notified of the availability of the results from the SAS Results project and those Results will be shared.
- After the sharing of the results, the customer will be asked to confirm the completion of the project.
- Once there is written confirmation from the customer that the project is complete and the agreed deliverables are received, SAS will start the process to dissolve the environment.
- AWS wipes all storage volumes before they are reused; however at the customer's request, SAS can also run a secure wipe application called bcwipe which writes over every disk sector making data unrecoverable.
- SAS Solutions on Demand will then dissolve the dedicated environment created for the customer.
- Confirmation will be sent to the customer.

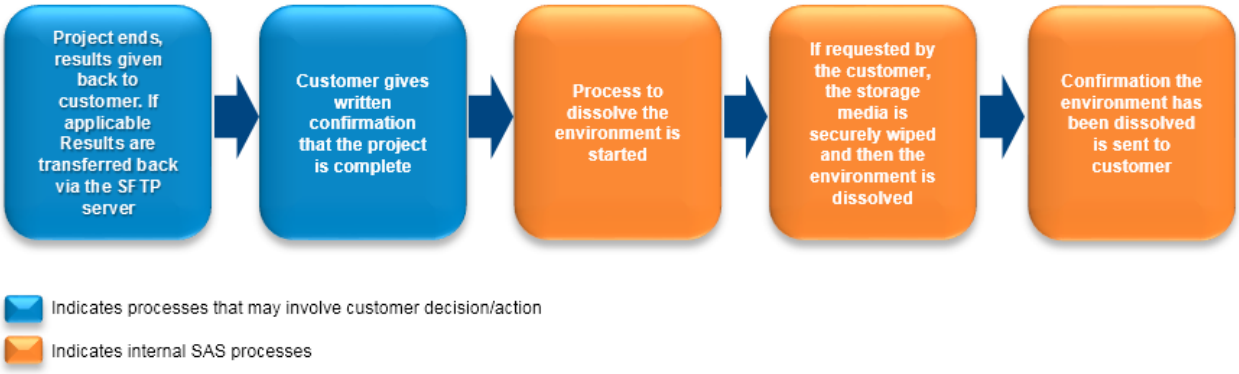

Figure 4: How can I be sure my data has been deleted?

AWS System Policies

AWS Risk and Compliance Policy:

http://d0.awsstatic.com/whitepapers/compliance/AWS_Risk_and_Compliance_Whitepaper.pdf

AWS Environment Security Overview:

http://aws.amazon.com/security/

AWS Security Policy:

http://d0.awsstatic.com/whitepapers/Security/AWS_Security_Whitepaper.pdf

SAS and all other SAS Institute Inc. product or service names are registered trademarks or trademarks of SAS Institute Inc. in the USA and other countries. ® indicates USA registration. Other brand and product names are trademarks of their respective companies. Copyright © 2016, SAS Institute Inc. All rights reserved.