ARGUS Developer

ARGUS Developer on Cloud: Hosting, Data Security, and Availability

ARGUS Developer 8.3.5

March 13, 2025

ARGUS Developer on Cloud: Hosting, Data Security, and Availability
www.altusgroup.com/argus
ARGUS Developer 8.3.5
March 13, 2025

Published by:
ARGUS Software, Inc.
11700 Katy Fwy Suite 260
Houston, Texas 77079
Telephone (713) 621-4343
Facsimile (713) 341-3648
www.altusgroup.com/argus

ARGUS Developer on Cloud: Hosting, Data Security, and Availability

Introduction

ARGUS Developer on Cloud is a hosted technology that consists of two parts:

- The application
- The database

ARGUS Developer on Cloud provides a way for users/customers to host their data and application on the cloud, thereby reducing their local footprint.

Hosting information

The ARGUS Developer on Cloud system consists of a dedicated database for each organization.

- Clients **choose how much of their data to store** in the cloud using their organization's database.
- Clients continue to **have access to models** stored on their local computers or networks**.**

Hosting

ARGUS Cloud leverages Amazon Web Services (AWS) as a secure infrastructure for hosting the Cloud components of the solution. AWS provides secure infrastructure for the world's biggest organizations in the private and public sectors and has a robust compliance program that includes regular SOC-1 and SOC-2 audits and compliance to a wide range of international security standards such as ISO/IEC 27017. Details of the AWS compliance program are available directly from Amazon at https://aws.amazon.com/compliance/programs/

ARGUS Cloud uses Amazon's EU-West region (Ireland) Availability Zone.

Segregation

ARGUS Cloud is deployed and operated in a completely segregated Virtual Private Cloud (VPC). This ensures access to the environment and any client data is strictly controlled and data cannot be moved to other systems or applications. Strict segregation between production and non-production environments prevents non-production resources accessing any production environment applications and data. Each customer gets their own database and thus their data is completely segregated from other customers' databases.

Secure communication

Industry standard Transport Layer Security (TLS) protocols and algorithms are used to fully encrypt and secure all communications with ARGUS Cloud. Additional cryptographic controls such as digitally signed certificates are used. Certificates are strongly signed with RSA keys in excess of 2,048 bits; never with the weaker SHA-1 hashing algorithm. Customers use ARGUS Developer on Cloud via Citrix virtual sessions using ICA protocol.

Data security

Data is encrypted in transit and at rest.

Only authorized users can access client data. Strict separation between different clients is enforced at the database level to ensure that clients can access data belonging only to their organization.

Operations

A dedicated operations team manages the ARGUS Cloud environment. Completely separate from all development functions, the operations team is solely responsible for all updates and changes to the production environment.

Management of the environment uses strong authentication, secure protocols, and is fully logged and audited. This reduces the risk of unauthorized access to the environment and protects client data and privacy.

Security testing and assurance

At Altus, it is a general practice to do penetration testing of our applications at least once annually through a third-party vendor.

Monitoring and alerting

Continuous monitoring of servers and infrastructure components notifies the operations team of any performance and security events using automated alerts.