

Gale Analytics On Demand

Technical Security

Data protection is on the minds of anyone who reads the media. Headlines warn us to remain very selective when discussing our personal information and to be careful with whom we share it. *Gale Analytics on Demand* uses a variety of ways to keep your library's information secure and protects your data at every stage of its journey.

Cloud Storage and Security

Your reports are stored on a secure, encrypted, password-protected server, Amazon Web Services Australia (AWS), that is separate from any other system. AWS is used as the cloud computing service (Platform as a Service – PaaS) for the *Gale Analytics On Demand/Alteryx Analytics Gallery*. AWS has a number of certification and accreditations with respect to the security of their hardware and supporting services <http://aws.amazon.com/security>. *Gale Analytics On Demand* stores the output data file in a compressed, proprietary schema in a NoSQL data warehouse until such time as the user deletes the output file.

Your patrons' privacy is very important to us. The built-in data protection in *Gale Analytics On Demand* occurs automatically, and at all stages of access and storage, providing you with the information you need, while protecting your community's information every step of the way. If an attacker managed to obtain a copy or portion of the output report stored in the data warehouse, they would lack the proprietary code to decrypt and utilise the data. Also, the output report is a summary and lacks any detail information on any specific library patron.

Transfer

When a *Gale Analytics On Demand* application is executed (run), the file used is not permanently stored, but rather only used during 'run-time' and deleted immediately afterwards. The communication 'channel' used to deliver the file to the application in order to execute the application is an encrypted channel. The only output saved from executing the application is the report generated by the specific application, until such time as the user deletes it. All files and report outputs can only be viewed by the specific user that has logged in to *Gale Analytics On Demand* to execute the application.

Alteryx Analytics Gallery

While any data is stored in a shared NoSQL data warehouse, security firewalls and multiple permission levels prevent access to the *Gale Analytics On Demand* applications or their relevant data to anyone other than the specific library customer that has been authorised to use it. Neither Gale or Alteryx Gallery administrators have access to content/data that is used to generate a report within the gallery by a specific customer. Permission has to be explicitly granted to a Gale/Alteryx administrator or delivered to a Gale/Alteryx representative via some other electronic means such as FTP or email. The site was reviewed and security penetration tests were performed by a third party vendor.

Execution and Run Time

Gale Analytics On Demand applications and their associated data is secure even when being transferred amongst the horizontal array of execution servers in AWS. All communication is compressed and encrypted among all servers in the array to prevent against "man-in-the-middle" attacks. Execution is a transient operation and no residual data (temporary or otherwise) is persisted in any location other than the secure data warehouse.