White Paper

Qlik Sense® Cloud Security

August, 2016

Table of Contents

Introduction

Qlik Sense® is used around the world by large and small organizations for data visualization and business intelligence, assisting. Many businesses make better decisions and allowing many users to create and share their insights using this next generation, self-service data visualization platform. Qlik Sense® Cloud provides access to the same core Qlik Sense experience as Qlik Sense® Enterprise and Qlik Sense Desktop but is engineered to ensure a high performance, highly available, secure, global environment through which Qlik delivers multi-tenant software-as-a-service (SaaS) based offerings. Given the significant role of security in a multi-tenant Cloud application, this paper describes the Qlik Sense Cloud security layers.

Security is an integral part of how Qlik develops software. Qlik Sense Cloud incorporates leading security technologies and modern open standards to provide users with the confidence their data and analysis is secure. Qlik Sense Cloud and its operating infrastructure provide security using a number of approaches and methods which include authentication, encryption, public and private sharing modes, virtual private cloud and subnets as well as real-time vulnerability monitoring. These approaches can be grouped in to the following categories:

- Foundational Security
- Information Security
- Qlik Software Design
- Secure Sharing and Collaboration

Foundational Security

In order to ensure a strong, secure foundation, Qlik shares security responsibilities with an industry leading cloud infrastructure vendor and valued partner, Amazon. Amazon's collection of cloud computing services, known as Amazon Web Services (AWS), is used by Qlik for internal purposes as well as Qlik's clients for Qlik Sense and QlikView cloud deployments. AWS security has been validated by independent 3rd parties and currently complies with the following security standards for infrastructure as a service:

- FEDRAMP
- ISO 27001
- PCI Data Security Standard
- Australian Signals Directorate Information Security Manual
- Singapore Multi-Tier Cloud Security Standard

Qlik Sense Cloud relies on AWS infrastructure for secure physical access, redundant (fault tolerant) infrastructure, and scalability.

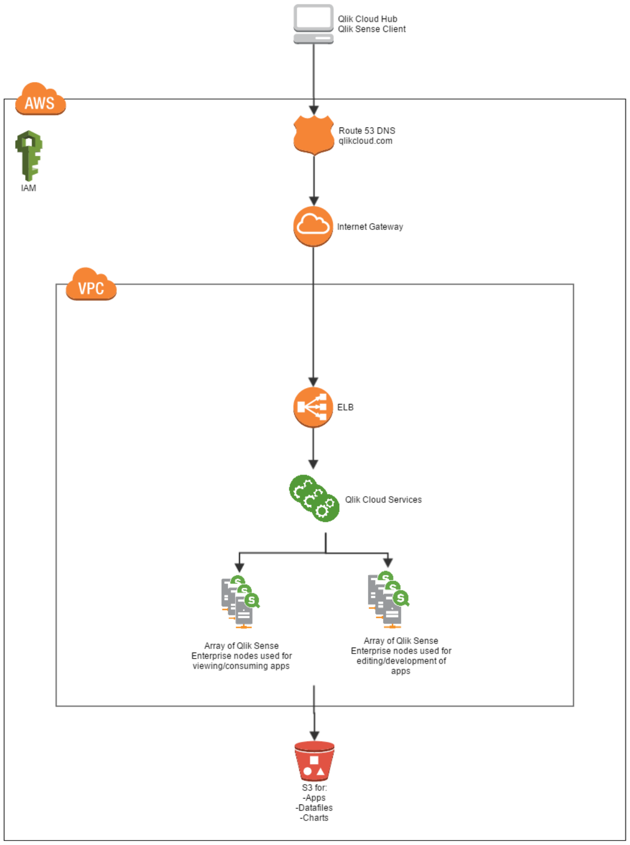
AWS' network design and monitoring mitigate the most common types of network security issues like Distributed Denial of Service (DDoS), Man in the Middle (MITM), IP Spoofing, Port Scanning, or packet sniffing.

Additional security for Qlik Sense® Cloud is implemented through the use of AWS services and third party solutions in a virtual private cloud (VPC).

Within the VPCs, Elastic Load Balancers (ELB) provide the capabilities of traditional load balancers with additional security features, to direct traffic to the different Elastic Compute Cloud (EC2) instances. These ELBs also enable all data moving between the end-user and Qlik Sense Cloud to be encrypted using Transport Layer Security (TLS) version 1.2.

The EC2 instances allow the rapid deployment and scaling of the Qlik Sense Cloud servers. Each of these EC2 instances enforces a further level of security by using security groups, which function as firewalls, allowing only predetermined traffic to flow between EC2 instances.

Qlik Sense Cloud also leverages AWS' Simple Storage Service (S3), where a user's data (data files and QVFs[1]) is stored at rest. This service uses the 256-bit Advanced Encryption Standard (AES-256) cipher to encrypt the data.


Qlik Cloud Hub
Qlik Sense Client
AWS
IAM
Route 53 DNS
qlikcloud.com
Internet Gateway
VPC
ELB
Qlik Cloud Services
Array of Qlik Sense Enterprise nodes used for viewing/consuming apps
Array of Qlik Sense Enterprise nodes used for editing/development of apps
S3 for:
-Apps
-Datafiles
-Charts

Qlik Sense Cloud Architecture

[1] Qlik Files (QVFs) are comprised of data, a data model and presentation layer. These applications are persistently stored on a file system and are loaded into memory by the Qlik Sense Engine as users request them.

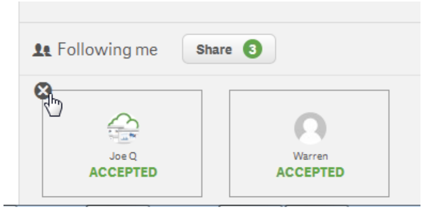
Secure Sharing and Collaboration

Sharing and collaboration is key in today's modern data visualization and business intelligence software. Qlik Sense® Cloud enables private or public sharing with whomever the user chooses. The personalized Hub is where all work is created, shared and organized. Private and public sharing options[2] puts the user in control of who has access and what they have access too.

Private Sharing

Users have complete control over who can access their content. This is achieved using Qlik's sharing and collaboration model. As a content administrator for its own content, a User may choose what content is viewable by others, inviting those others ("invitees") to interact with their shared content. Each User is also able to control when he or she chooses to stop sharing specific content, and/or remove invitee access from its shared content. Users can re-establish sharing at any time.

Users share content through a personal, active email invitation initiated by engaging with a "Share" feature. The invitee will receive an email and also see the invitation and content in their environment the next time the invitee logs in (or refreshes). The invitee may choose to accept or decline the invitation.



Invitation and Sharing Process:

1. **Invite:** The User enters the email address of the invitee to be granted access.
2. **Send Invitation:** An email from the Qlik Sense Cloud service is sent to the invitee and the invitation appears in the invitee's environment the next time such invitee logs into/refreshes its Hub.
3. **Receipt Invitation:** Invitee receives the email or logs in and sees the invitation
4. **Accept Invitation:** Invitee clicks on the unique link in the email and is taken to Qlik Sense Cloud or accepts within the Hub environment.
5. **Authentication:** The invitee registers or logs-in to its Qlik Sense Cloud account, which must be registered to the same email the User specified.
6. **Access to Content:** Invitee now accesses the shared content in Qlik Sense Cloud, until the User chooses to revoke access or unpublish the content.

Invitees who have had content shared with them are not able to copy, download, or export data through Qlik Sense features. Invitees are able to view, interact, and gain insights from the shared content, in the secure application environment.

[2] With public sharing you have the ability to share aggregation level of your choice. Others are not able to 'drill to detail'.

Public Sharing

Sometimes it is preferable to share a visualization with a broad public audience or in a more public manner. Qlik Sense® Charts allows a user to extract a component of a visualization app and share that data view through a number of different social and public channels.

Users may choose to publically or semi-publically share an unlimited number of data visualization charts. Qlik Sense Charts are semi-interactive visualizations that contain only the aggregated data needed to generate the visualization (drill to detail data is not possible; this capability is only accessed through actively sharing the entire app). Shared charts may be easily exposed and shared on social platforms such as Facebook, LinkedIn and Twitter or can be embedded in a web page (or blog, etc.) by using a public link or <iframe> embed code. These charts can be incorporated into public sites and applications, or placed into web pages or applications that require authenticated access.

Only those charts or visualizations defined by the User and shared through specific channels can be accessed by others. Qlik Sense Charts may be administered from within the Hub interface as well. Deleting the chart removes all public ability to view the chart going forward.

Unless you explicitly share the content of your Qlik Sense Cloud apps with someone at Qlik, Qlik personnel cannot access your content that you choose to upload to Qlik Sense Cloud.

Information Security

Qlik Sense Cloud adheres to the data security policies, programs, and procedures designed by Qlik's Security & Governance Team.

Qlik's Information Security Program takes its guidance from the security framework developed by the National Institute of Standards and Technology (NIST) using the moderate security baseline from Special Publication 800-53 (revision 4). In order to implement the NIST moderate security baseline, Qlik is updating policies, procedures and uses tools necessary to design, deliver and operate security controls. A select view of the NIST control families include:

- **Access Control** – All access to the Qlik Sense Cloud infrastructure is through an established access control processes and is limited to system administrators who are responsible for the infrastructure.

- **Auditability and Risk Management** – Qlik manages security through the auditing and retracement of actions when troubleshooting or addressing an incident response. This also allows for the evaluation, identification and remediation of threats and risk to the environment on an ongoing basis.

- **Security and Awareness Training** - Qlik provides annual privacy training to all employees globally and has policies and procedures in place to ensure best practice. We utilize online mediums in multiple languages to ensure a consistent, yet tailored, approach by region. Our

Security and Awareness programs provide staff and contractors with security training specific to their positions.

- **Security Assessment** - Our security assessment program provides the foundation to proactively identify and remediate vulnerabilities on an ongoing basis. Testing also provides critical operational feedback enabling our operations team to spot and address operational issues before they become user problems. The security assessment program goes beyond simply scanning for issues and involves active component testing of the software, network, operational procedures and processes.

- **Configuration management -** A foundational element to our program is establishing and managing the configuration of all devices within our environment consistently and always with a focus on reducing or eliminating vulnerabilities as quickly as possible. The configuration management program, in conjunction with a variety of threat intelligence and remediation programs, allows Qlik Sense® Cloud to establish a secure baseline and continuously improve the program based upon testing and operational data.

- **Incident Response -** We define a security incident as "the potential failure of a control that supports the confidentiality, integrity or availability of data". As soon as a potential failure condition is identified an investigation begins to identify the issue, contain the issue and begin remediation as quickly as possible. All of these efforts are designed to minimize the likelihood of an actual disruption that our clients experience with our cloud products.

- **System and Services Acquisition –** In a modern computing environment, establishing rules and requirements that exist for the computing assets in only your organization is not adequate. In order to manage supply chain security risk, Qlik works with all of our vendors to understand their security programs and how those programs meet Qlik's security requirements.

- **Privacy Law Compliance/Consumer Choice** – Qlik's privacy policies are available for viewing on our website. AWS also has privacy policies published on their website. AWS has protections in place to handle large scale outages by having multiple availability zones in each region. Qlik consistently monitors regulatory changes globally, and it is our policy to make applicable changes as soon as possible.

Qlik Software Design

Qlik incorporates security during the software development life cycle by adhering to the Qlik Security Model, developed by the Software Security Office. The Qlik Security Model is an internal process that guarantees that all software development is done with a security focus. The model is a result of sourcing best practices from several existing well renowned secure software development processes, and molding them to fit the needs of Qlik. The model has five phases that span the entire lifecycle of software development:

- **Analysis & Design**: This phase of the processes includes System and Feature Level Threat Modeling. When a product is designed, the team considers each feature and determines the possible threats for this feature. Countermeasures are put in place to mitigate each threat.
- **Develop**: Qlik uses an industry-leading static code analysis tool and manually reviews every issue reported by the tool. Static code analysis is run on both the code specific to new features and the end-to-end code incorporating the new features. After deployment, the static code analysis tool runs the report on a regular basis. The automated reports are supplemented with manual security testing processes. If manual verification confirms that it is a security issue, then it is fixed prior to deployment.
- **Assemble:** Test cases are created from a security perspective and executed during the development process. Testing includes system level, feature level, penetration level and fuzzing. Test cases consider the end-to-end new product release to identify any security issues within the new product. Specific tests are conducted on code that contains the new features within the product. For each major release of the software by Qlik R&D, an unbiased third party security company will audit the product through penetration testing.
- **Deploy:** The Software Security Office is involved in the deployment phase through its vulnerability management process. Working with external security companies, customers, and partners to identify vulnerabilities within the deployed code, the team will assess any reported vulnerability and determine appropriate action.
- **Evolve:** All results from the activities that are a part of the security model are reviewed by the Software Security Office. The goal is to identify areas of improvements, making the model an evolving entity that is updated on a regular basis.

Conclusion

Qlik's approach to security begins with design and continues through development and deployment. Qlik shares security responsibilities with AWS by leveraging AWS cloud infrastructure. This provides our users with a proven and industry-leading infrastructure. Applying data storage, security and monitoring and infrastructure management, Qlik manages the security of its client's data within Qlik Sense® Cloud. Qlik provides a secure and safe environment that allows one to see the whole story that lives within their data.

150 N. Radnor Chester Road
Suite E120
Radnor, PA 19087
Phone: +1 (888) 828-9768
Fax: +1 (610) 975-5987

qlik.com