7/1/2014

MSI

QlikView Extranet Deployments

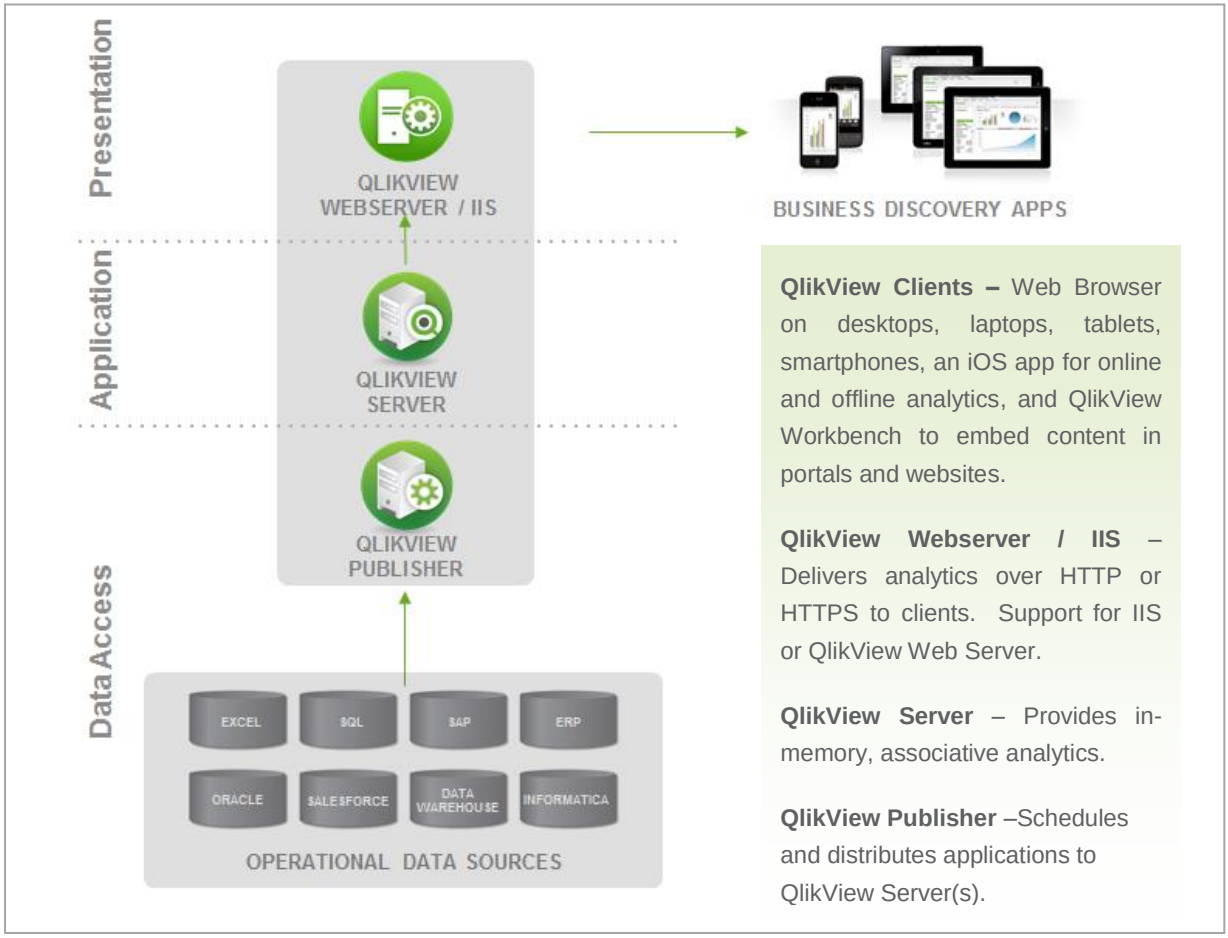
This document provides an overview of the capabilities of QlikView to deploy analytics to employees and non-employees outside of the corporate network. With QlikView, it is possible to deliver valuable analytics via many devices, and this document illustrates the technical considerations and capabilities commonly employed to deploy QlikView securely.

QlikView Business Discovery Platform

QlikView is an in-memory analytics platform that uses a Natural Analytics™ technology and design approach to deliver analytics to users via a QlikView application that resides in-memory. (In the remainder of this document, a "QlikView application" will be referred to as an "application.") From a user standpoint, an application is a predefined data model and presentation layer. Based on selections users make within an application, calculations are computed at runtime using data stored in RAM, and results are returned to users via a browser on a desktop, laptop, tablet, mobile device, a QlikView iOS application, or via embedded content. (You can see this in action at the QlikView demonstration site.) QlikView offers a highly interactive, associative experience in which users can freely navigate through applications with little to no constraint in their analysis path.

QlikView Architecture

The QlikView Business Discovery Platform is a three tiered architecture that scales vertically and horizontally to meet the demands of your organization.



For more information please reference the QlikView Architectural Overview whitepaper:

http://www.qlik.com/us/explore/resources/whitepapers/qlikview-architectural-overview

QlikView Clients

The QlikView Business Discovery platform delivers highly interactive, associative analytics to users through many clients. To experience the interactivity of the clients, please reference http://demo.qlik.com. For more information about supported versions of the clients listed below, please reference the QlikView 11 system requirements document titled QV11_System_Requirements.pdf.

QlikView AJAX Client

The QlikView AJAX client is a zero footprint AJAX and JavaScript based web client for desktops, laptops, notebooks and iOS, Android, and BlackBerry mobile devices. The QlikView AJAX client is supported in Internet Explorer, Firefox, Safari, Chrome, Good, and the native browsers of the mobile Operating Systems listed above.

QlikView for iOS

The QlikView iOS application provides online and offline (i.e. disconnected) analytics with no need to rebuild applications that are created for the AJAX client. Online analytics leverage a native Safari web browser embedded within QlkView for iOS application. Offline analytics provide users the ability to choose which applications and data to take offline provided it is permitted by your organization's security administrators.

QlikView Workbench

QlikView Workbench is an AJAX and JavaScript based API that allows granular, object level QlikView content to be embedded within websites and portals. QlikView Workbench allows content to be embedded in websites and portals utilizing HTML and JavaScript.

Customer Examples

The deployment scenarios, authentication, and authorization methods detailed in this document are leveraged to expose QlikView securely to external users. There are many possible permutations and common customer requirements, but given the modular, service oriented nature of QlikView and the ability to leverage many authentication providers and authorization sources, QlikView can be deployed simply and securely in corporate environments.

To illustrate some configurations, these examples describe actual QlikView customer deployments, but in no way exhaust the possibilities that are outlined in the remainder of this document.

- 30,000 employees at a large insurance firm leverage QlikView to view policy and claims data. By authenticating to an existing portal and using QlikView custom ticket exchange, users leverage their same sign-on to authenticate and are passed through a reverse proxy to the QlikView deployment on the corporate network.

- A senior executive at a large financial services company, while travelling, connects to QlikView via the QlikView for iOS application and views a dashboard. While connected, the executive authenticates via VPN to the corporate network and leverages Active Directory credentials to securely view QlikView content.

- 1500 healthcare analysts external to a large healthcare insurance company leverage QlikView to analyze claim reimbursement information. By authenticating to an existing portal, users leverage their same sign-on to authenticate and pass credentials to QlikView via SAML received by a web server in the DMZ. QlikView leverages authorization information stored in MS SQL Server to secure data to the row and column level.

- 3000 pharmaceutical sales reps leverage the QlikView for iOS application to review their account information while disconnected. By authenticating to a VPN provided by their Mobile Device Management (MDM) solution, sales reps connect to QlikView inside the corporate network to securely take their personal QlikView content offline, as permitted by an administrator.

- A government entity shares state spending information with the general public on their PHP based website using QlikView Workbench.

Deployment Scenarios

To the right is a categorization of different user types based on the relationship with your organization and from where those users access QlikView. For brevity and when the distinction is not relevant, this document will reference **External Employees**, **External Non Employees**, and **Anonymous Users** together as "**External Users"**.

Given the modular, service oriented nature of QlikView, it is possible to securely deploy in a variety of configurations commonly required by organizations. Depicted below are many common deployment scenarios, but not every possible scenario. Please contact Qlik with questions.

INTERNAL USERS

Internal Employees – Employees who access QlikView from inside the corporate network – *e.g., Executives, Analysts*

EXTERNAL USERS

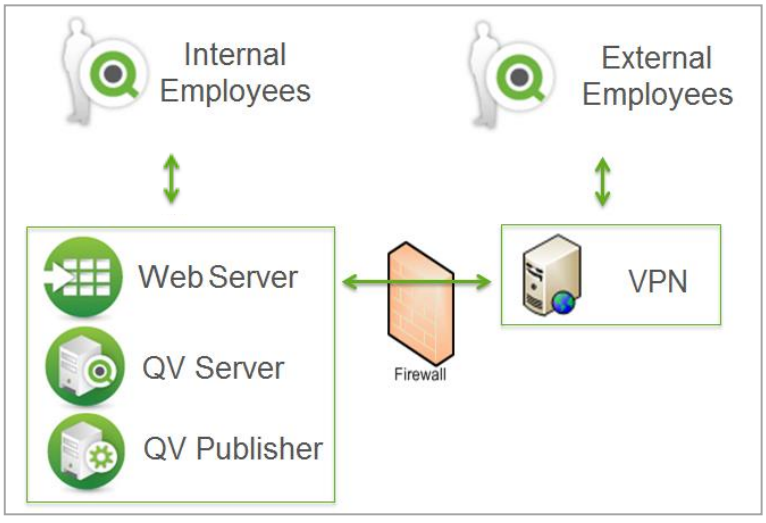
External Employees – Employees who access QlikView from outside the corporate network – *e.g., Field Sales*

External Non Employees – Identifiable Non-Employees who access QlikView from outside the corporate network – *e.g., B2B relationships, customers*

Anonymous Users – Unidentified users who access QlikView from outside the corporate network – *e.g., the public*

VPN Access

Leveraging a VPN is a possible deployment scenario for

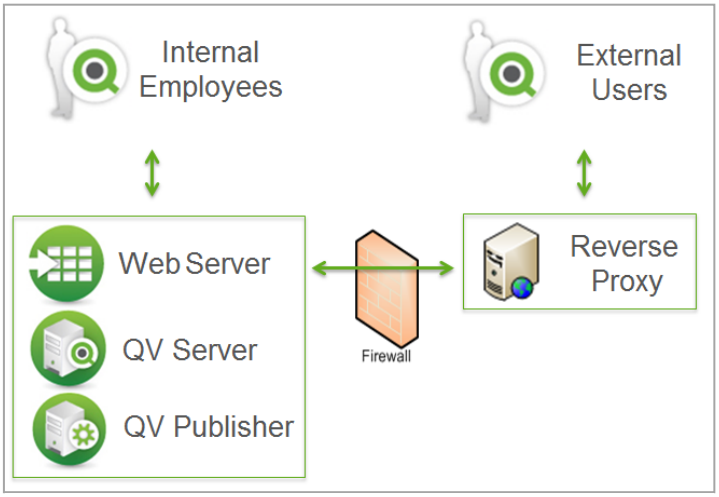


VPN Access

External Employees to access QlikView. In this scenario, all components of QlikView reside inside the corporate network, and after having authenticated to the VPN, External Employees are able to access QlikView via a URL as though they were an Internal Employee.

Reverse Proxy

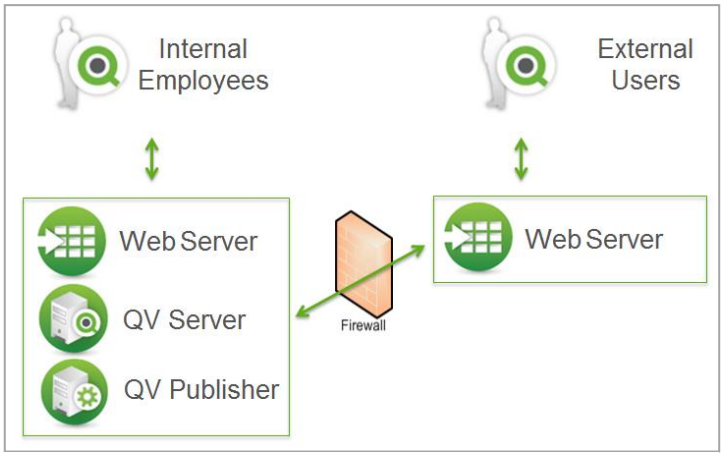
Leveraging a Reverse Proxy is a possible deployment scenario for External Users to access QlikView. In this scenario, all components of QlikView reside inside the corporate network, and after having navigated to the externally facing URL, user traffic is reverse proxied to QlikView. Authentication is often accomplished at the reverse proxy itself (e.g. SiteMinder) or at the QlikView Web tier. Please see the section entitled *Authentication* below for more information.



Reverse Proxy

Web Server in DMZ

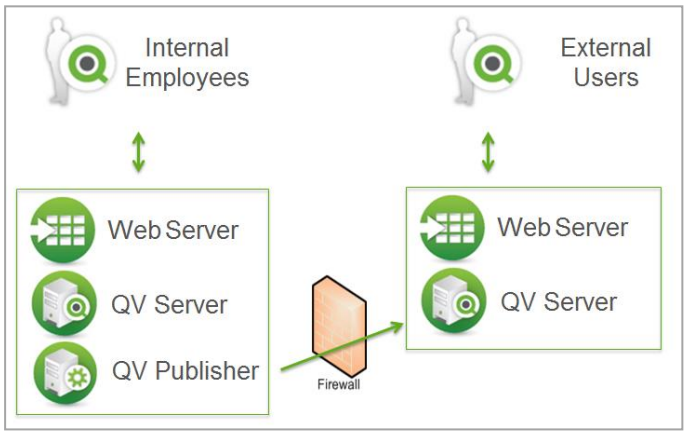
Leveraging a Web Server in the DMZ is a possible deployment scenario for External Users to access QlikView. In this scenario a web server is placed in the DMZ and allowed to communicate back to the QlikView Server via firewall rules. The diagram below illustrates that it is possible to deploy multiple web servers with QlikView, though it is not strictly required. The internal web server optionally serves internal users, which may or may not be related to the extranet deployment. Authentication is often accomplished with a single sign-on solution or a ticketing solution available in QlikView. Please see the section entitled *Authentication* below for more information.



Web Server in DMZ

QlikView Server in DMZ

Leveraging a QlikView Server in the DMZ is a possible deployment scenario for External Users to access QlikView. In this scenario, the Web Server and QlikView Server are deployed in the DMZ and no communication back to the corporate network is required. The diagram below illustrates that it is possible for QlikView Publisher to publish to multiple QlikView Servers, though it is not strictly required. It is possible to dedicate a QlikView Publisher to an extranet deployment, as well. Authentication is often accomplished with a single sign on solution or a ticketing solution available in QlikView. Please see the section entitled *Authentication* below for more information.



QlikView Server in DMZ

Security

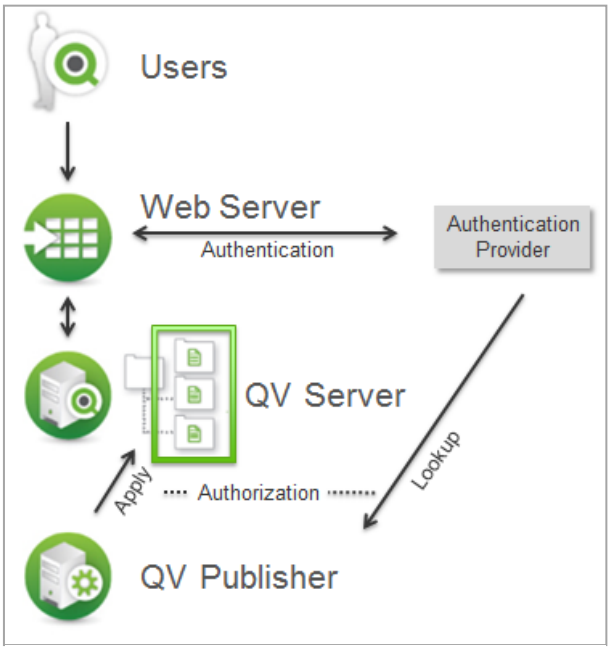
The QlikView security model allows administrators to secure applications and data with flexibility and granularity. QlikView addresses authentication, authorization, and secure communications as described below to deliver specific content to users.

Leverage Existing Investments

QlikView is able to leverage existing security infrastructure to seamlessly integrate into your corporate network. Users and groups defined in authentication providers are leveraged to secure access to applications and data. User definitions do not need to be maintained in QlikView, which reduces maintenance overhead.

Component Overview

At a component level, the web server tier is responsible for authentication, after which QlikView will resolve the groups to which the user belongs. Next, a session is created on the QlikView Server for the user. The QlikView Server grants the user access to those applications for which one is permissioned based on the attributes determined during the authentication process. Administration of application access is a function of QlikView Publisher, and applications are permissioned at a user and/or group level. Finally, within the applications, data is secured at a row and column level such that users are only able to see the data they are permitted to see.



QlikView Security Model – Component Overview

For more information, please reference the QlikView Security Overview whitepaper: http://www.qlik.com/us/explore/resources/whitepapers/qlikview-security-overview

Authentication

As above, the web server tier is responsible for authentication. QlikView will leverage existing security providers to accomplish authentication. Authentication integration methods are categorized as follows:

- Windows Integrated Authentication – Leverage Active Directory using NTLM, Kerberos, Basic authentication protocols. Note that while Kerberos is a supported authentication protocol for QlikView AJAX client and QlikView Workbench in general, it is not commonly utilized in extranet deployments.

- HTTP Header Authentication – Leverage Single Sign-on providers by accepting HTTP headers. (e.g. SiteMinder, Web Seal).

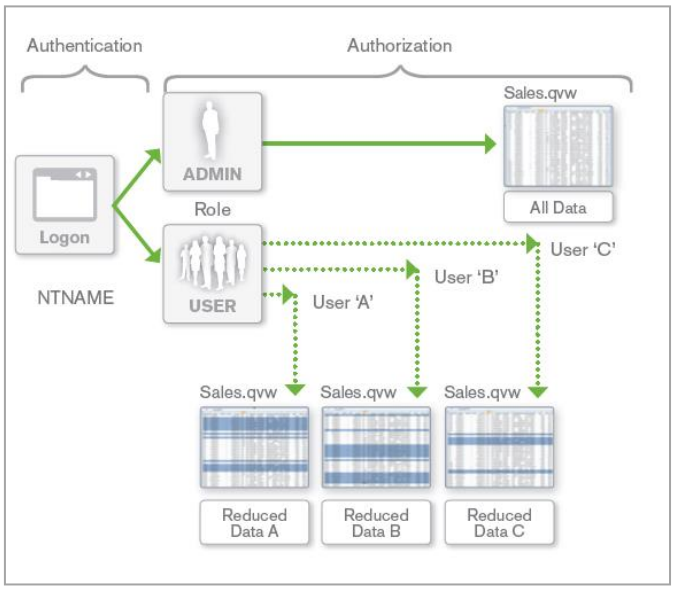
- Custom Ticket Exchange – Also known as GetWebTicket. This token based API allows QlikView to trust other websites and portals to request a session on behalf of a user. A small amount of code is placed in the website or portal to request a ticket on behalf of a user and redirect that user into QlikView.

- SAML – Leverage SAML providers by accepting a SAML token and resolve user and group attributes. Note that this requires a small amount of custom development using Custom Ticket Exchange described above and is deployed on the QlikView web server tier.

- Anonymous – Some use cases dictate anonymous access to applications. In this scenario, no authentication provider is leveraged.

Authorization

Authorization works at two levels of granularity. As mentioned above, administration of application level access is a function of QlikView Publisher and is permissioned at a user and/or group level. Next, Section Access is a capability by which entitlements – the relationship of users to the data they can view – are leveraged to drive data visibility at a row and column level.



QlikView Security Model – Section Access

As with authentication, QlikView will leverage existing security definitions to enforce authorization. Users and groups in Active Directory, LDAP, and/or ODBC compliant databases drive application and data visibility. Alternatively, define these visibility rules directly in QlikView.

Communication

For all QlikView clients, communication between the client and web server is delivered over HTTP or HTTPS, ensuring secure communication. Communication from the QlikView web server tier to the QlikView Server tier is delivered via 128 bit RSA encryption. Optionally, intra-component communication may be secured and encrypted via SSL certificates.

QlikView for iOS

In addition to the security capabilities described above, the QlikView for iOS application includes an offline caching capability that allows users to take applications offline at the discretion of an administrator.

Device Security

With the QlikView for iOS application, some data is cached when users take applications offline. The QlikView for iOS application leverages iOS security mechanisms to encrypt the data using AES-256 bit encryption, enforce password entry even while not connected, enforce strong passwords, and leverage over-the-air wipe capabilities.

Transmission Security

In addition to HTTPS, X.509 certificates may be used at the device level to seamlessly authenticate to VPN solutions.

Server Editions

The QlikView Server component of the QlikView Business Discovery Platform is delivered in one of three server editions to accommodate the user population to which QlikView should be deployed.

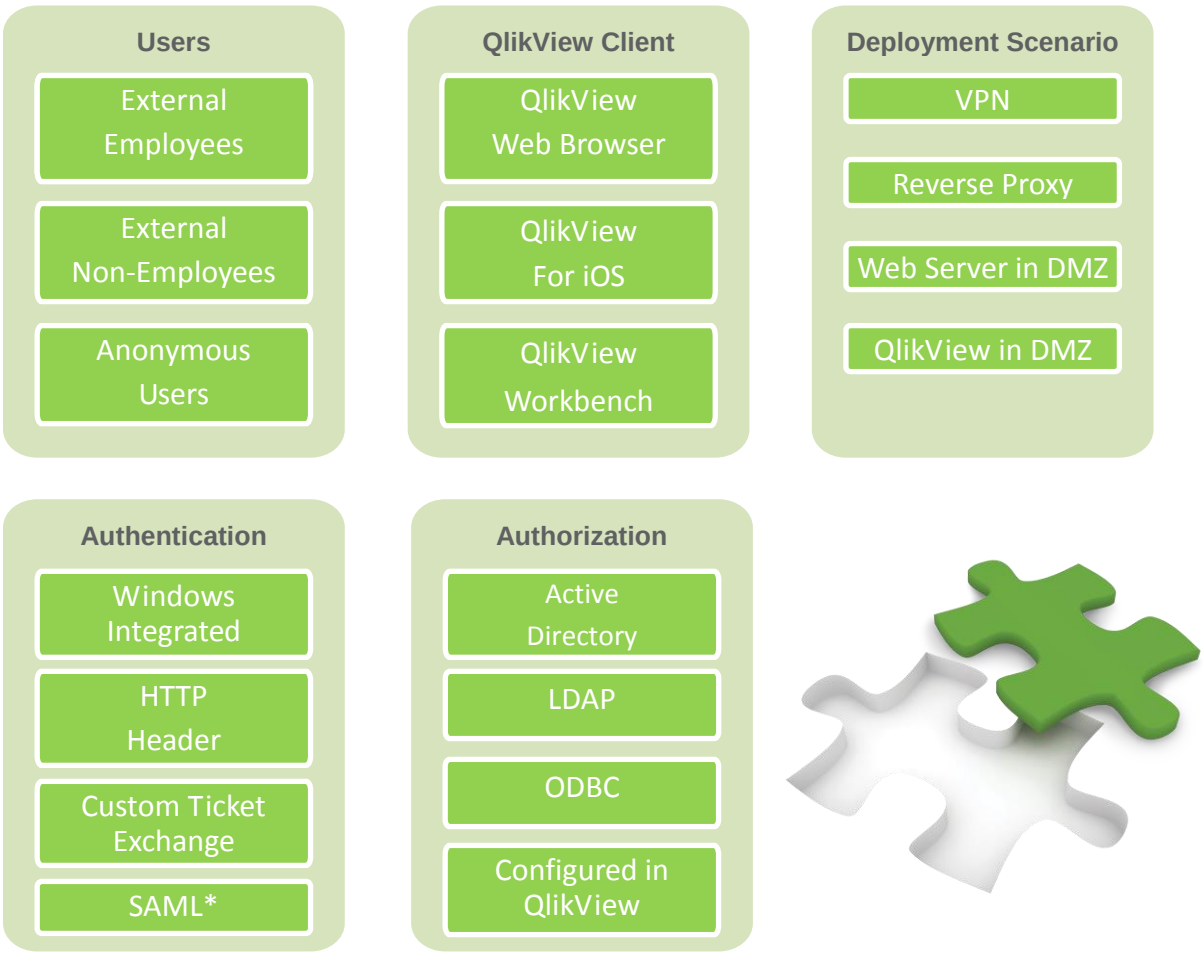
Server Edition	Users
Enterprise Edition	Internal and External Employees
Extranet Server	Non-Employees
Information Access Server	Anonymous Users

Please contact your Qlik representative for more information.

Putting it all Together

While the value in delivering QlikView externally to your organization may be high, the difficulty in doing so need not be. This document has outlined the most common deployment scenarios, clients, and authentication and authorization models used to deliver highly interactive, associative analytics to a variety of user groups.

Consider bringing business, security, and networking teams together to align on the key points summarized below, and contact your Qlik representative for more information.



**Requires a small amount of custom configuration*