



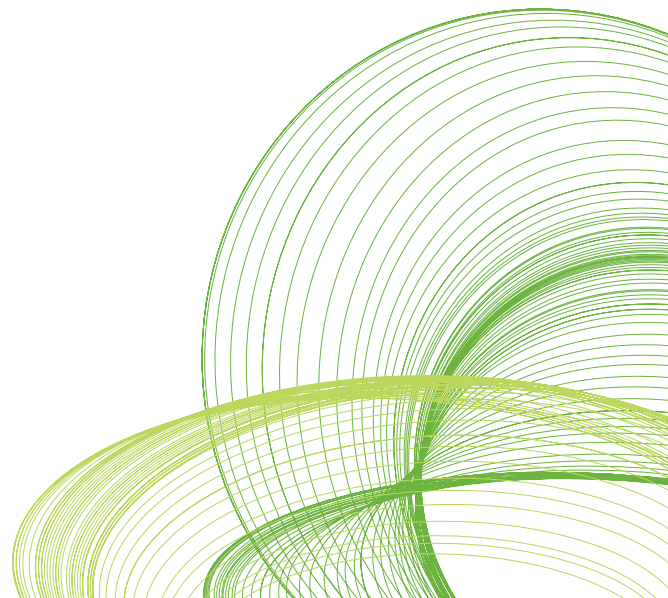
# QLIKVIEW DEPLOYMENT AT A LARGE INSURANCE COMPANY

---

A QlikView Technical Case Study

March 2012

[qlikview.com](http://qlikview.com)



## Introduction

---

This document describes the QlikView deployment for a large insurance company at a technical level. This large insurance firm has chosen QlikView to enable Business Discovery capabilities on insurance data for thirty thousand external users. To provide business-to-business collaboration and making insurance data available to their agents, they integrated QlikView into their extranet portals providing secure information access to their agents anytime from anywhere. This deployment serves the business discovery needs of thirty thousand potential external users.

This paper illustrates one of the real-life examples of a QlikView deployment providing secure access to internal data by external users. As with any extranet deployment, providing direct access to external parties without the proper safeguards increases the risk of divulging sensitive information to competitors or exposing the corporate computer infrastructure to malicious users. With Qlikview's robust security integration capabilities, this insurance firm made sure that only authorized agents' users can gain access to the relevant data. Please note that the technical specifications of an extranet QlikView deployment depend on a range of considerations such as extranet purpose, component models and security policies in place.

The technical deployment decisions explained in this paper are dependent on the considerations specific to this customer. In addition, this deployment is an example of a scaled case. The hardware specifications and the architecture details explained here were designed based on the current and the future needs of this specific customer. This is a referral paper and should not be used as a deployment guideline.

The remaining part of the paper talks about the technical solution, providing an understanding of the QlikView architecture, hardware specifications, and details on the QlikView Server deployment in the demilitarized zone (DMZ).

Before reading this paper, we recommend you review the QlikView Development and Deployment Architecture Technical Brief in order to get a fundamental understanding of the various QlikView components.

## **LARGE SCALE QLIKVIEW EXTRANET DEPLOYMENT AT A LARGE INSURANCE FIRM**

- 30,000 external users
- Streamlined Business Discovery on the insurance data
- Seamless QlikView integration to the existing portal and security systems

## Executive Summary

---

To remain competitive in today's information-driven, partner oriented marketplace, companies must be able to communicate and share mission-critical data with anyone, anywhere, in real-time easily and securely.

The IT department at this large insurance company has chosen QlikView because of the secure platform it provides that seamlessly and securely extended the insurance analytics to their thirty thousand agents. By using QlikView, they were also able to leverage their existing substantial IT investments on portals and security systems as QlikView provided seamless integration with these systems.

The QlikView environment serves the Business Discovery needs of thirty thousand agents analyzing the insurance data. With QlikView, each user can analyze the claim and policy data at the individual detail level. QlikView powered the existing portal system at this insurance firm providing streamlined analytics processes and strengthened the relationship with their agents.

## QLIKVIEW PRODUCTS COMPONENTS

- 2 QlikView Server Clusters with 8 QlikView Servers in total
- 1 QlikView Publisher providing ease of maintenance with loop and reduce capability
- QlikView Developer and zero-footprint Ajax clients

## Technical Solution

---

### 1. ARCHITECTURE OVERVIEW

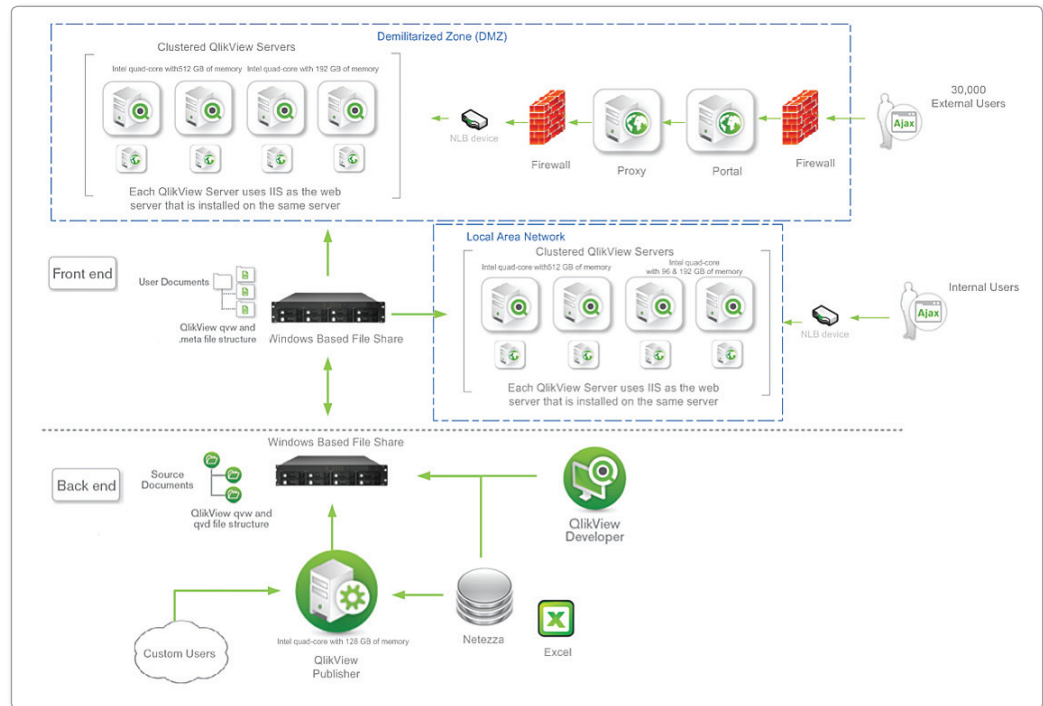
Figure 1 shows the architecture of the QlikView production environment. Three main infrastructure components are used in this deployment.

- QlikView Server (QVS) handles the communication between the clients and the QlikView applications. QlikView Server loads the QlikView applications into memory and calculates and presents user selections in real time. In this deployment, IIS web servers are used to provide the content to the users. There are four servers used to host the QlikView Server. These servers are clustered and located in the demilitarized zone (DMZ). They are used to serve the QlikView applications to the external users.

In addition to these, there are four other servers, which are located in the local area network (LAN). These servers are used to serve the QlikView applications to the internal users. These servers are also clustered.

- QlikView Publisher is used to load the data from Netezza. Publisher's loop and reduce capability is used to create several QlikView applications from seven master QlikView applications based on the sector information found in the data. The sizes of these seven master QlikView applications range from one to three gigabytes. Publisher's loop and reduce capability simplified the maintenance of the QlikView applications for the IT department as these are the only applications that they should maintain and make changes to. Publisher automatically creates the sector based versions of the applications after each data refresh.
- QlikView Developer is used to develop the data extraction and transformation as well as to develop the graphical user interface. As the business user access required no installations, AJAX Zero-Footprint Client is used for business users accessing QlikView applications on the QlikView Server from the extranet.

**Figure 1 – QlikView Production Environment Architecture**



© 2012 QlikTech

**2. DEMILITARIZED ZONE (DMZ) ARCHITECTURE AND EXTERNAL USERS QLIKVIEW ACCESS PROCESS**

Figure 2 shows the architecture of the Demilitarized Zone (DMZ) and the external users' access process to a QlikView application. The DMZ is used as the physical sub-network that contains QlikView Servers, the proxy server and the servers hosting the portal and the security system.

The DMZ adds an additional layer of security to the organization's local area network (LAN). QlikView Servers are hosted in the DMZ with limited connectivity to the local area network. This allows QlikView Servers to provide services to the external users without risking any vulnerable attacks to the internal systems. The deployment used two firewalls to control the traffic within the DMZ.

The following part of this section explains the external users' authentication method and the access process to open a QlikView application.

To get authenticated, external business users login to the portal (step 1 on figure 2.) This portal is written in .NET and it is hosted on an IIS web server in the DMZ. This server is located behind a reverse proxy layer (step 2 on figure 2.) The authentication is done with a web form over Secure Sockets Layer (SSL). The portal uses a backend security system to validate the credentials (step 2a on figure 2) and this is addressed by the portal via SOAP\* (Simple Object Access Protocol) web services.

To pass the authenticated user name to the QlikView Server, the Custom Ticket Exchange (CTE) method is used. Custom Ticket Exchange is a process offered by QlikView that is most applicable to embedding QlikView content in third-party applications and portals. Please refer to the QlikView Security Technology White Paper to learn more about the Custom Ticket Exchange process.

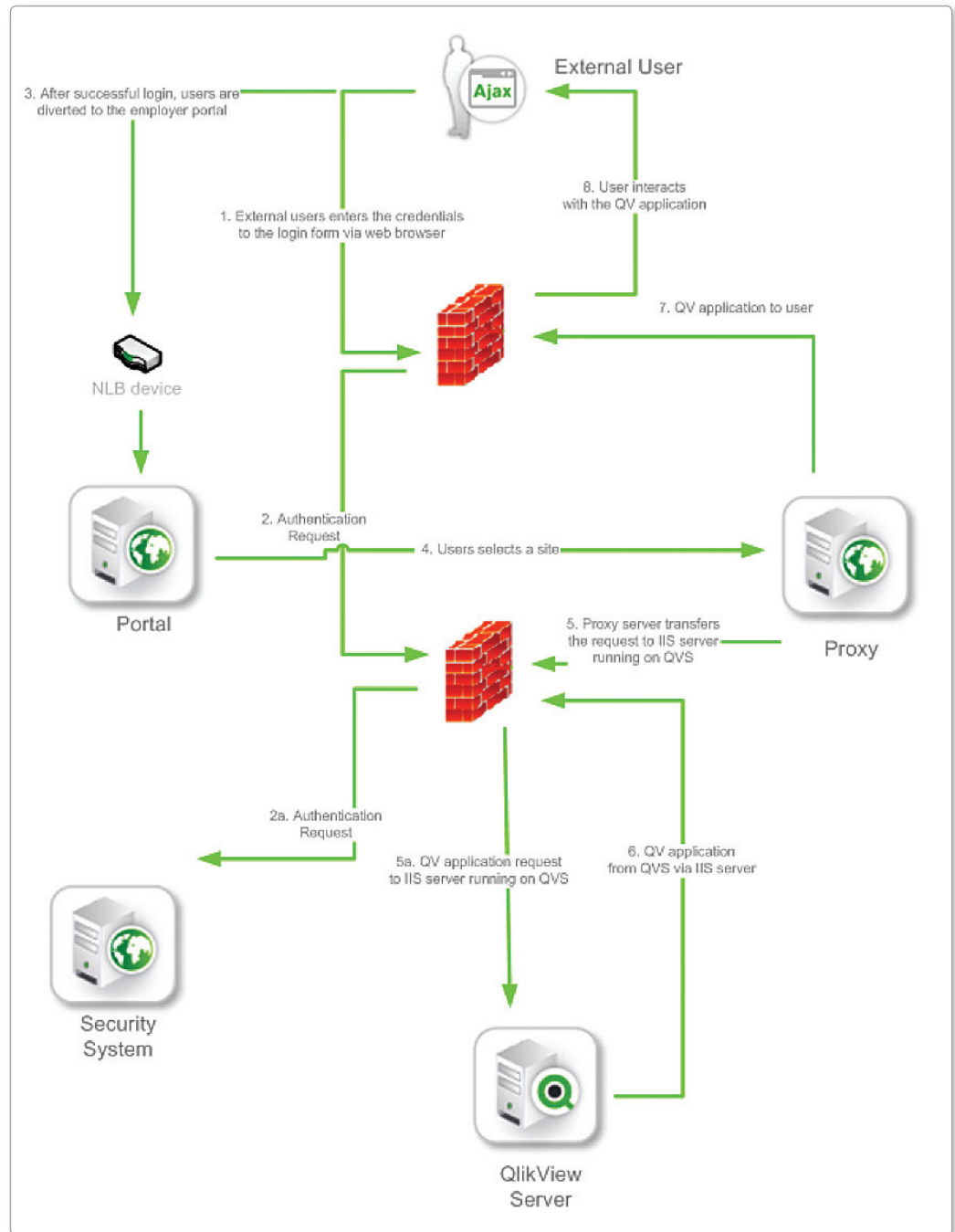
After the business users are authenticated, the list of sites they can access are displayed on the portal (steps 3 and 4 on figure 2.) Once they chose a site, the site makes a SOAP call to another backend system (step 5 on figure 2) asking for a QlikView Server ticket for the user's identity. This SOAP call is secured via SSL. The SOAP endpoint then makes a web request to the IIS web server used for the QlikView Server to request a ticket for the user. Please note that SOAP is not a pre-requisite to be able to use QlikView ticketing process. In this deployment it is used as a way to allow communication between different applications with different technologies.

The final step in the ticketing process is the IIS web server makes a call to the QlikView Server (step 5a on figure 2) to get a ticket and then responds back to the portal. The portal embeds the ticket in a web redirect to a URL through a Reverse Proxy layer to the IIS web server associated with the QlikView Server (steps 6 and 7 on figure 2.)

At this point the business user's browser connects to the IIS web server of the QlikView Server with the ticket (step 8 on figure 2) and his QlikView application session is established for them.

*\* SOAP is an XML-based messaging protocol. It defines a set of rules for structuring messages that can be used for simple one-way messaging but is particularly useful for performing RPC-style (Remote Procedure Call) request-response dialogues.*

**Figure 2. External user authentication and QlikView application access process in the DMZ**



© 2012 QlikTech

### **3. HARDWARE SPECIFICATIONS**

There are four servers used in the Demilitarized Zone (DMZ) serving the QlikView applications to the external users. Two of these servers are Intel quad-core with 512 GB of memory. The other two servers are Intel quad-core with 192 GB of memory.

Four QlikView Servers are located in the local area network serving QlikView applications to the internal users. These servers are Intel quad-core servers with memory ranging from 192GB to 256GB.

There is one publisher server used at the back end and both the external and internal deployments have two QA and one development environments. These servers are Intel quad-core with memory ranging from 96GB to 192GB.

One of the main considerations on determining the server size was to retain performance levels as the data, the number of users and QlikView applications grow in the future. The plan is to open the portal to the individual members and provide them access to their claims information.

### **4. CLUSTERING DETAILS**

QlikView Server clustering is used to support load sharing of QlikView applications across the servers. There are two QlikView Server clusters. The first one is located in the DMZ with four servers. The second one is in the local area network with the other four servers. With QlikView clustering, the user requesting the QlikView application is directed to that server which has the most RAM and CPU available.

### **5. NUMBER OF USERS AND LICENSE TYPES**

The deployment supports thirty thousand external users. Different Client Access License (CAL) types are used to accommodate the Business Discovery needs of these users.

Named User CALs are used for users that need dedicated access to QlikView applications. Session CALs are used to share a pool of licenses to accommodate less frequent QlikView users (users that will access QlikView applications couple times per week). And Usage CALs are used to accommodate additional users during peak times.

### **6. SECURITY DETAILS**

The security model in this deployment is based on the following elements:

- Authentication and Custom Ticket Exchange (CTE)
- Loop and Reduce
- Section Access

The following section explains each of these in more detail.



### **Authentication and Custom Ticket Exchange (CTE)**

In the QlikView environments, the authentication of a user is always done against an external entity. QlikView relies on the authentication to be performed prior to accessing QlikView, and some token of identity is transmitted to QlikView.

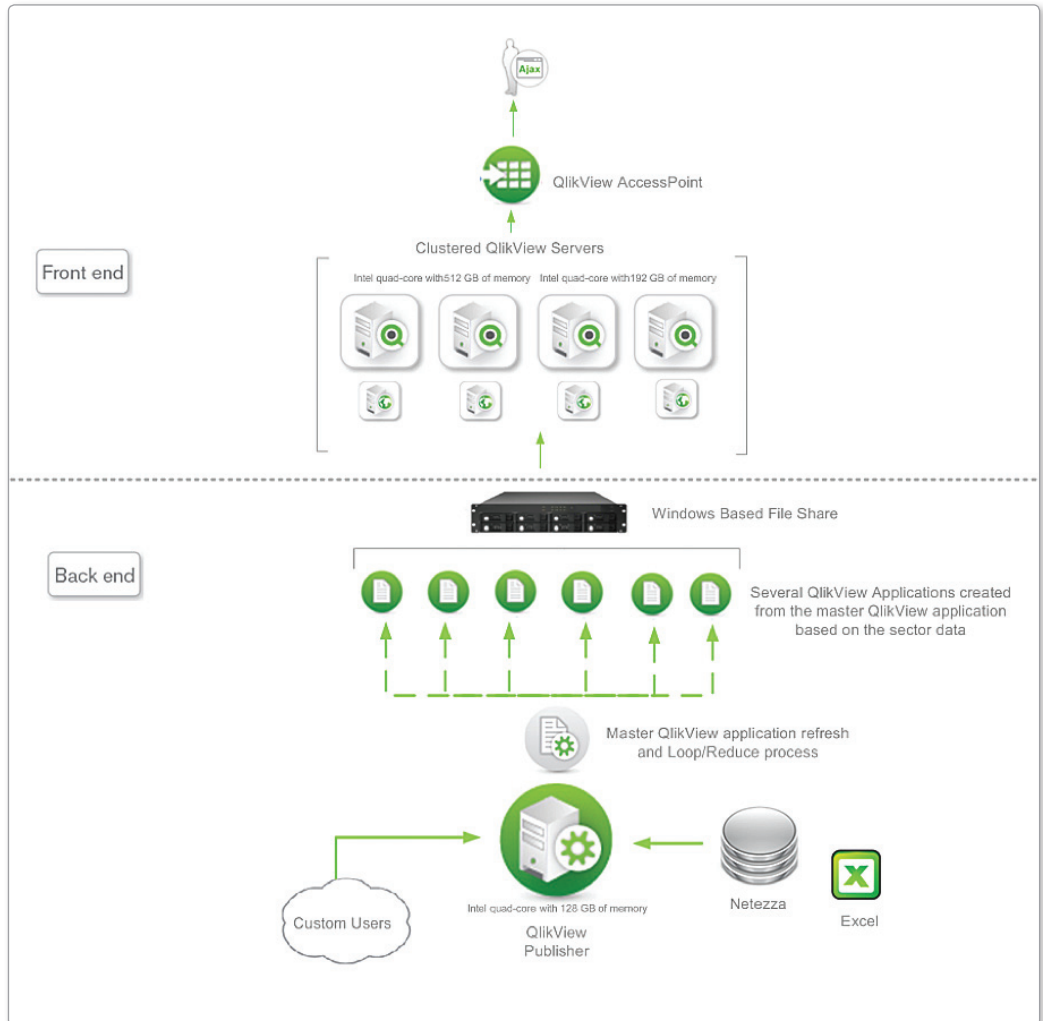
In this deployment, the portal's login page is used to authenticate the user against a custom security system. Once the user is authenticated, the site makes a web request to the IIS server used for the QlikView Server to get a ticket for the authenticated user. In this deployment, the web call is protected by NTLM authentication which means that the origin of the call uses an Active Directory service account known to the QlikView installation's IIS web server and that this account is a member of the local QlikView Administrators group on the IIS server. Once the IIS server gets the web request, it makes a call to the QlikView Server to get a ticket and finally passes the ticket back to the site.

At this point the business user's browser connects to the IIS server of the QlikView Server with the ticket and his QlikView application session is established for him. Please refer to the second section of this paper (the DMZ architecture and external user access process) to get an understanding of custom ticket exchange process with the DMZ architecture components.

### **Loop and Reduce**

In this deployment, QlikView Publisher's "Loop and Reduce" capability is used to create smaller versions of the master QlikView applications based on the sector information. With loop and reduce, the master QlikView application is split up into several smaller QlikView applications after each refresh. This provides a good security mechanism because each external user is only authorized to see the insurance data related with their sector. The external users would never have access to the master QlikView application as it is being secured at the back end of the QlikView environment. Only QlikView Publisher and the allowed QlikView developers can have access to it.

Figure 3 – QlikView Publisher Loop and Reduce Process



© 2012 QlikTech

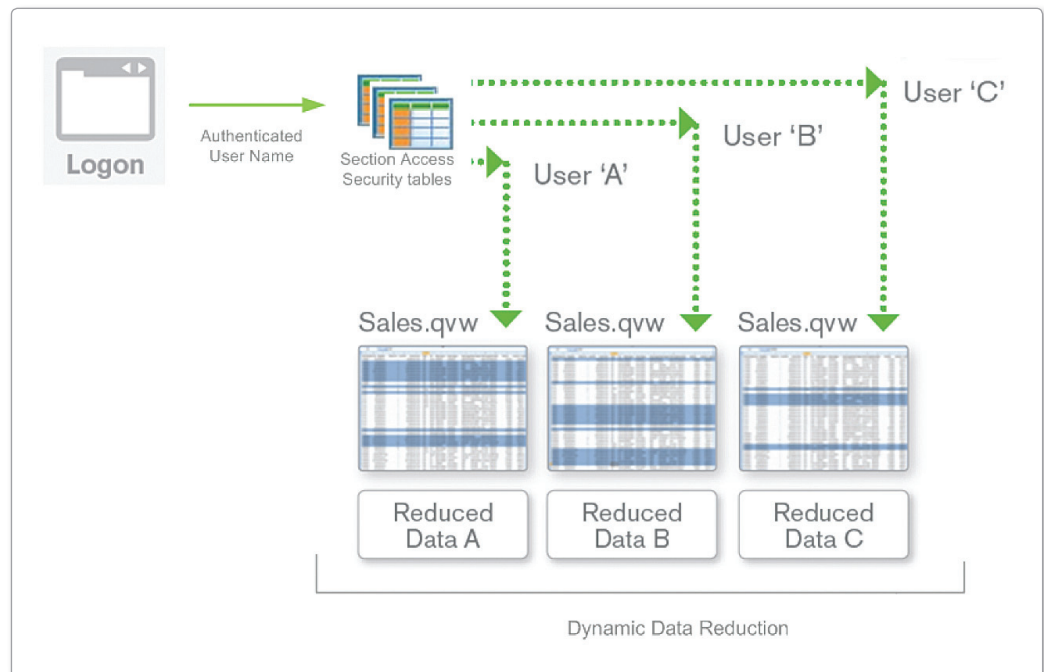
## Section Access

One of the security requirements in this deployment was to provide data level authorization. Although sector specific applications were automatically generated through Publisher's loop and reduce capability, the requirement was to provide additional data level security in the QlikView application so that external users can see and analyze only the relevant data to their role.

QlikView provides data-level security using Section Access within the QlikView document. 'Section Access' is a QlikView technology that allows QlikView to control which users have access to specific data (or sections of data) in a QlikView application. Section Access uses a security table to determine what data users can access to, and applies security based on an association between users and data. In this deployment, the security table is created by using the information in the custom security system. The authenticated user name is passed to Section Access security table by using a QlikView system field. Then QlikView dynamically reduces the data for that authenticated user based on the security information found in the Section Access.

By using QlikView's Section Access feature, IT department was able to extract and leverage the security information stored in the existing custom security system. This provided ease of maintenance and reusability of the security data.

**Figure 4 – QlikView Section Access Data Level Security**



© 2012 QlikTech

## Conclusion

---

This paper has outlined the technical QlikView deployment details taken at a large insurance firm to handle the Business Discovery needs of a large external user community. This insurance firm has chosen QlikView because of its seamless integration capabilities with their existing portal system and the robust security it provides. With QlikView, the IT department was able to leverage the existing investments on the portal and on the custom security system. This deployment is just one example of many large QlikView deployments proving QlikView's security and scalability to handle many thousands of external users.

At this insurance firm, the QlikView environment serves the Business Discovery needs of thirty thousand agents analyzing the insurance data at the individual detail level. With QlikView, each agent can self analyze the claim and policy data. QlikView powered the existing portal system at this insurance firm providing streamlined analytics processes and helped strengthen the relationship with their agents. With the Business Discovery environment, they provide superior operational service and differentiate themselves from the competition in a cost effective way.

## References

---

QlikView Development and Deployment Architecture Technical Brief

[www.qlikview.com/.../global-us/direct/datasheets/DS-Technical-Brief-Dev-and-Deploy-EN.ashx](http://www.qlikview.com/.../global-us/direct/datasheets/DS-Technical-Brief-Dev-and-Deploy-EN.ashx)

QlikView Architecture and System Resource Usage Technical Brief

[www.qlikview.com/.../DS-Technical-Brief-QlikView-Architecture-and-System-Resource-Usage-EN.ashx](http://www.qlikview.com/.../DS-Technical-Brief-QlikView-Architecture-and-System-Resource-Usage-EN.ashx)

QlikView Scalability Overview Technology White Paper

<http://www.qlikview.com/us/explore/resources/whitepapers/qlikview-scalability-overview>

QlikView Security Overview Technology White Paper

<http://www.qlikview.com/us/explore/resources/whitepapers/qlikview-security-overview>