www.vigience.com

QuiXilver Security

White Paper

Version 2.0.3

Dated: February 2014

Prepared By:

Vigience LTD

Contents

Executive Summary 3

Introduction 4

- Workspace Concept for Multi-tenancy 5
- QX Apps 5
- QuiXilver Architecture 5

Secure Data Storage 6

- Server-side Protection 6
- Encryption 7
- Client-side Protection 7
- Data Backup 7

Access Control 8

- Administrator Authorization 8
- Workspace Authorization 9
- Role-based Data Access Authorization 9
- Inviting Users 10
- User Authentication 10

Security in Transit 11

- Secure Communications 11
- Preventing Impersonation 11
- Encrypted E-Mail Notifications 11
- Disturbance of Data Transmission 12
- Access QuiXilver through a VNC Client 12

Secure Deployment & Operations 12

- Administrative Staff 12
- Response to Attacks 13
- Responsibility for Data Security 13
- On-Premise Deployment 13

Secure Software 13

- Signed Software Code 13
- Secure Development Processes 14
- Guards against Malicious Users 14

Audits 14

- Tracing of Data Access 14
- External Audits 15

Conclusion 15

Executive Summary

QuiXilver is a cloud-based application platform for collaboration and information sharing. As such, security is very important; security is designed into the solution and security policies are observed in the development process as well as in the daily operations. All these different aspects of security regarding the QuiXilver solution and Vigience as a vendor and operator of the solution are summarized in this white paper.

The main goal of security is to guard the confidentiality, integrity and availability of information. The prevention of unauthorized access and manipulation of data is key. The security of the QuiXilver solution is addressed on multiple levels:

- *Secure Data Storage*: The QuiXilver services including the database are run on a cloud infrastructure provided by secure certified providers that guarantee physical and infrastructure security and 24/7 availability. All data is regularly backed up in encrypted form to logically and administratively separate data centers. Optionally, customers can use encrypted workspaces for sensitive data.
- *Access Control*: QuiXilver offers fine-grained access control to the data. All users are authenticated, and have by default only access to data in their workspaces. The access can be further detailed by assigning the users to specific roles. The access rights of different types of administrators – at the customer but also at the infrastructure provider and Vigience staff – are also controlled and follow the principle of separation of concerns.
- *Security in Transit*: All data transmissions are secured using SSL/TLS, and necessary measures are in place to prevent data transmission disturbances as well as impersonation attacks.
- *Secure Deployment & Operations*: Operations are monitored by qualified staff to detect and respond to any attacks or malicious usage. Operational and security policies are followed both at Vigience as well as the infrastructure provider.
- *Secure Software*: The software is digitally signed to assure that the code has not been manipulated. To guard against security holes in the software, the development process follows industry best practices, including code and architecture reviews and thorough security testing.
- *Audits*: User activities are logged and can be traced back if malicious use is suspected. External audits of QuiXilver can be conducted upon customer request.

INTRODUCTION

QuiXilver (QX) is a secure PaaS[1] cloud service developed for teams of information workers. It is both a social collaboration platform to share files, communicate better, and manage projects as well as a platform to easily develop additional productivity and cloud database applications. Please see www.quixilver.com for more information about QuiXilver and its features.

Prof. Dr. Paulus

Especially for cloud services that primarily target business users like QuiXilver, security is of prime importance and is being addressed in the design of the solution, its deployment, and its operation. The security of QuiXilver has been thoroughly reviewed by Prof. Dr. Sachar Paulus, an internationally renowned expert on IT security, former Chief Security Officer of SAP and now Professor for Information Systems and Security Management at Brandenburg University of Applied Sciences.

This white paper demonstrates all major security aspects in relation to QuiXilver. QuiXilver offers different security features that are available in deployment and operations to adapt to the individual needs of each customer, as shown in the following table:

Default Security	Additional Security Features
• Secure 24/7 operations • All data transmission using SSL/TLS • Salted & hashed password storage • Multi-tenancy: data access limited to workspace members • Different access rights for different types of administrators • User activity logging • Authentication of software modules • Server-side file encryption	Role-based authorization concept for cloud database access • Encrypted e-mail notifications • Single Sign-On based on SAML

[1] Platform-as-a-Service

The information in this paper is based on release 2.0 of QuiXilver. After an introduction to the main concepts and the architecture of QuiXilver, this paper details in the following sections how security is achieved regarding storage, access control, data transmissions, deployment and operations, and the software itself. The last section finally deals with auditability.

Workspace Concept for Multi-tenancy

Multi-tenancy is a necessary property of all cloud solutions used in a business context. It enables the separation of data from different customers, even though all customers are using the same system and infrastructure services. QuiXilver achieves multi-tenancy by using *workspaces*. A workspace groups a number of QX Apps, related data as well as any number of files. Usually a workspace is created for one specific activity, project or even program. Workspaces ensure that only members of that workspace – i.e., users that have been granted the right to participate in that workspace by the workspace's administrator – have access to these QX Apps and their data and files.

QX Apps

QuiXilver is an application platform that also allows developing, deploying and customizing QuiXilver Applications – QX Apps. QX Apps consist of html and JavaScript files and the same security handling applies as to other file types. The only exception is an additional security feature that only a workspace administrator can deploy QX Apps to other workspace members.

QuiXilver Architecture

In order to describe the security concepts around QuiXilver, it is necessary to first have a look at the overall architecture and describe the main components. The QX Server residing in the Cloud deals mainly with two types of data: files and database records. The database records are only stored on the server, while files are also replicated to the local file system of computers accessing QuiXilver through the QX Windows Client.

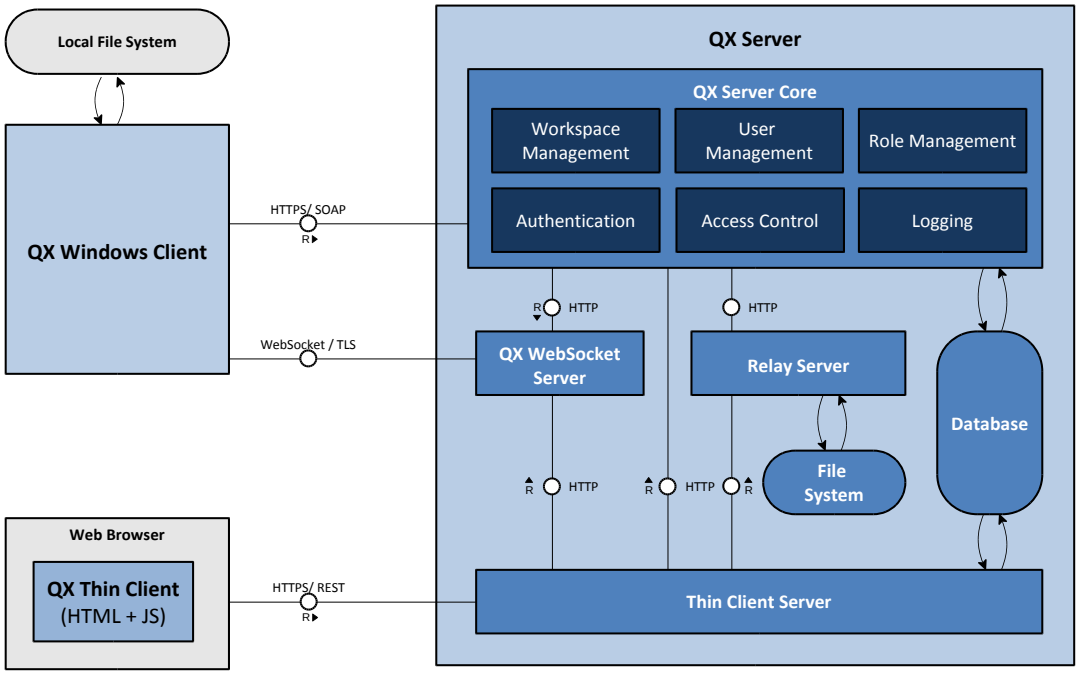

Figure 1: QuiXilver Architecture Overview

In addition the QX Windows Client, QuiXilver can also be accessed using a Thin Client running in any common Web Browser like Internet Explorer, Firefox, Chrome or Safari, also supporting access via mobile devices. In all cases the communication between client and server is secured using SSL/TLS.

Both the QX Windows Client as well as the QX Server are written in .NET and make use of Microsoft's WCF Security libraries.

Secure Data Storage

Server-side Protection

QuiXilver is relying on cloud infrastructure providers[1] to run its services. The infrastructure provider guarantees physical security, 24/7 availability, and firewall protection; Vigience is responsible for operating system patches and updates, virus scanning, and intrusion detection. The selection of infrastructure providers is important for the overall security and is based on proven track record and compliance to standards like SSAE16, SOC2, ISO 27001 or ISAE 3402.

Customers using QuiXilver can choose between two secure infrastructure providers, depending on their security and legal requirements as well as internal policies and preferences regarding the location where data is stored: a regular data center based in the US (AICPA SOC2 and US-EU Safe Harbor-certified), and a highly secure Swiss data center (ISO 27001 and ISAE 3402-certified).

[1] Also known as IaaS – Infrastructure-as-a-Service

Free trial and regular users use the US-based service; the high-security data center in Switzerland is subject to separate licensing.

Encryption

User passwords are not stored on the server in clear text. Rather, they are salted and hashed using SHA1 algorithm; only the salts and hashes are stored, making practically impossible for any attacker or even Vigience to get access to the plain text passwords.

All user files stored on the QuiXilver servers are automatically encrypted; database and server administrators thus cannot open them.

Client-side Protection

When using QuiXilver through the QX Thin Client, no data is stored on the local machine. The QX Thin Client is just using one cookie to identify the session. The session ID expires if the user hasn't been active for more than 15 minutes. No other cookies are stored in the browser, so the QX Thin Client can be safely used also from unprotected locations like an Internet Café. The QX Windows Client on the other hand stores all sensitive information like username, password and encryption keys using the Windows Protected Storage service, a standard Windows component to securely store sensitive data.

Security however is only as strong as its weakest link. Therefore users are advised to follow common best practices in securely handling their local PCs and the devices they use. If a hacker is able to gain access to the user account on the PC, he would also be able to access QuiXilver – for example by installing a key stroke recorder he could retrieve username and password.

Data Backup

The QX Servers are regularly backed up to prevent data loss. The data is backed up using AES encryption to physically and administratively separate data centers.

In addition, users have the possibility to back up their data individually as well.

Access Control

QuiXilver offers fine-grained control over who has what access to the system. As shown in Figure 2, there are 3 levels of access control in QuiXilver: Administrator access, workspace access, and role-based data access.

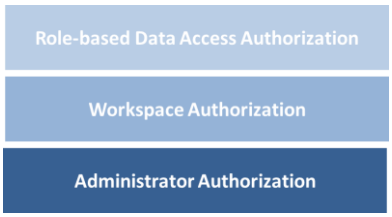

Figure 2: Levels Of Access Control

These different levels of access are described in the following sections.

Administrator Authorization

QuiXilver makes a distinction between several types of administrators. While this may sound complicated at first, it increases the security of the system as it allows the separation of concerns and prohibits one single administrator to have all power. QuiXilver distinguishes between the following types of administrators and their respective management rights:

Scope / Admin Type	Description	Management Rights		
		Files[1]	Database	Organization & User Information
Organization Administrator	Manages the users within an organization.	No	No	Yes
Workspace Administrator	Manages a specific workspace.	Yes	Yes	No
Database Administrator	Manages the database server, including patches and upgrades to the DB software.	No	Yes	Yes
OS-level Administrator	Manages the underlying operating system, including system patches and backups.	Only files from workspaces not using local file encryption.	No	No

Note that the first two types are managed and assigned to individuals by the QX customer, while the latter two are system-level and consists of staff at Vigience as well as the infrastructure provider.

[1] Includes the files for the installed QX applications.

Workspace Authorization

As a part of QuiXilver's multi-tenancy concept, the storage of all data and of all files is segregated according to the workspace. Only properly authenticated users get access to the workspace data. Based in the spirit of open, collaborating teams, all workspace members get by default full access to all data and files of the workspace.

There are three different types of workspaces: Workspaces open only to an explicitly defined list of users, workspaces open to all users in an organization, and workspaces that have (invited) guest users. The workspace administrator makes these configurations and decides who gets access. To guard against sharing a document inadvertently, in the UI it is visible to all users what type of workspace it is and who is a member.

In a workspace, users have the option to declare files as private. These files are not shared and not uploaded to the QX Server, but they are visible and can be accessed within the QX Windows Client as any other, public file in the folder structure of QuiXilver.

Manipulating data about the workspace (like name, user membership and other configurations) is restricted to workspace administrators. A workspace administrator must explicitly manage the membership of users in the workspace, be it including or excluding individuals of the organization, or be it the invitation of additional external users.

Role-based Data Access Authorization

In addition to just defining access rights based on workspace membership, a fine-granular access authorization based on roles can optionally be employed. As shown in Figure 3, individual users are assigned to one or more roles that were defined by the QX application developer. Hence there are different roles for different applications. A role consists of all rights necessary to perform a certain business function. Technically speaking, a role is a bundle of authorization objects, each of which defines access rights (create, read, update, delete) for individual rows or fields (columns) of a specific table.

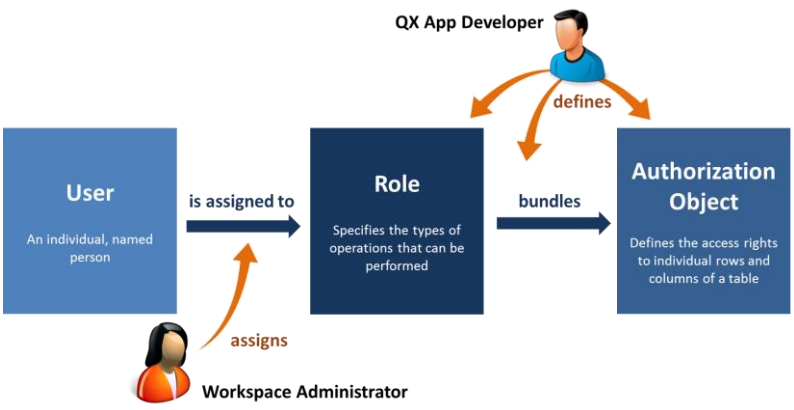

Figure 3: QX Role-based Data Access

With role-based authorization, it becomes possible that only certain users can edit all data, others can just read it, and again others can just change individual fields. For example in the task management application, only a manager can create new tasks, while the team members can read all task information, but only change the status or add comments to a task.

Inviting Users

Workspace administrators can directly invite external users to a workspace, for example in order to collaborate with an external company in a specific project. For additional security though, invitation of external users is only possible after re-authentication of the workspace administrator. So even if a hacker were able to capture a web session of an administrator, he would not be able to invite other – likely malicious – users.

User Authentication

Username and password is used as the main means of identifying the user. In the subsequent communications between client and server however, OAuth 2.0 and OpenID Connect is used.

Single Sign-On and integration with external identity management solutions (e.g., Active Directory) is possible based on the WS-Federation standard; please contact us for further information if such integration is needed.

Security in Transit

Secure Communications

All data transmissions are secured using SSL/TLS with certificates issued by a well-known certificate authority, GeoTrust. Programmatic access to QuiXilver is secured through the use of the encrypted WS-Security stack.

To ensure that the QuiXilver servers can only be accessed through such secure channels, the HTTP Strict Transport Security (HSTS) policy is employed.

Preventing Impersonation

All users are properly authenticated with username and password. When using the QX Windows Client, these data are stored within Windows Protected Storage, to enable the login to QuiXilver without reentering username and password all the time. Hence an attacker would need to get the access credentials to the Windows account if he wanted to impersonate a proper QX user.

When using the QX Thin Client, the initial authentication is done with username and password, and in subsequent communications OAuth is used. QuiXilver applications make use of a few cookies, but in a secure way. All have the "secure" attribute set so that cookies are only transmitted over a secure HTTPS channel, and the session cookie further makes use of the "httpOnly" attribute to guard against XSS (Cross-Site Scripting) attacks.

Sessions are timed out after 15 minutes of idleness to mitigate the danger of being hijacked, e.g., when a user in an Internet café forgets to close the browser window.

In addition, for auditing purposes the IP addresses from which QuiXilver is being accessed, are logged.

Encrypted E-Mail Notifications

By default, QuiXilver is sending out notifications to its users via e-mail, for example about overdue tasks or important changes in tasks. These e-mails are normally not encrypted, but as an optional feature, users can configure that all e-mail notifications that are sent to them are encrypted via S/MIME. All they need to provide is a valid X.509 certificate.

Alternatively, e-mail notifications can also be turned off completely.

Disturbance of Data Transmission

The infrastructure on which the QX Servers are deployed is protected by services of the infrastructure provider. Concretely, this includes the blocking of DDoS (Distributed Denial of Service) attacks on the firewall as well as intrusion detection among other basic security services. Vigience staff is regularly executing vulnerability scans on its servers and is monitoring the reports from industry-standard intrusion detection software.

In addition, customers are advised to take the usual precautions that their network infrastructure – in particular DNS – is not compromised, as a failure in the basic networking would obviously also impact the data transmission to and from the QX Server.

Access QuiXilver through a VNC Client

Both the QX Windows client and the QX Thin Client are a secure way to use QuiXilver. For customers that do not want to install the QX Windows Client on their employees' machines but still want them to have access to the full QuiXilver functionality, there is a third deployment option: Install the QX Windows Client on a (virtual) machine in the company network, and have employees access this machine through VNC[1] or RDP[2] using SSL. Such a setup is commonly used in high security environments such as at NEC Systems Technology.

Secure Deployment & Operations

Administrative Staff

Regarding the administrative staff of the infrastructure providers, Vigience is only working together with companies that have a good reputation and appropriate certifications. In addition, Vigience is giving its customers the choice between two providers, thus they can choose which one they prefer and trust more.

The staff at Vigience itself follows strict security policies, and when hiring new staff care is taken to only hire people with a good track record. Furthermore, new people are not hired directly into positions related to the security and confidentiality of customer data.

---

[1] Virtual Network Computing

[2] Remote Desktop Protocol

Response to Attacks

We need to discern between two types of attacks. For network-level attacks, it is mainly the responsibility of the infrastructure provider to first of all guard against such attacks, but also to detect and immediately respond to any attacks.

For application-level attacks, i.e., by an authenticated QuiXilver user, Vigience has its own monitoring in place. User activity is monitored for suspicious patterns like the size and type of uploaded files, number of workspaces used, location of requests, creation of a user followed shortly by its deletion, etc. When such patterns are detected, the behavior is analyzed more deeply by Vigience staff and appropriate action is taken. The responses taken range from informing the organization administrator about the issue to blocking the user in question altogether.

Responsibility for Data Security

As stated in the Master Service Agreement, Vigience is maintaining appropriate administrative, physical, and technical safeguards for protection of the availability, confidentiality and integrity of all customer data. All data is regularly encrypted and backed up to a physically and administratively separate data storage provider.

In addition, customers can also backup their data using their own tools.

On-Premise Deployment

Customers wishing to do have full control over their QX system also have the option to deploy a QX Server on premise, i.e., within their network. In this case, Vigience offers consulting services regarding deployment options, sizing, monitoring and upgrading.

Secure Software

Signed Software Code

The code of the QX Windows client is digitally signed in order to assure that the downloaded software has not been manipulated. The distribution of QX Apps is controlled and managed by the workspace administrator. Without approval from the workspace administrator, no changes to existing QX Apps nor newly developed QX Apps will be distributed.

Secure Development Processes

The security of the QuiXilver is ensured already in the software development process. This process is based on industry best practices like they are described in the OWASP[1] guides and addresses all phases of the development process: Threat analysis workshops, code and architecture reviews, as well as security testing. All development staff is trained and aware of security issues and how to avoid them.

In addition to code review done by developers and architects, automated code analysis tools are employed to eliminate coding mistakes. Regarding testing, standard tools like OWASP ZAP are used to guard against potential vulnerabilities that could be exploited by an attacker.

Guards against Malicious Users

The fine granular authorization concept described above makes sure that a user can only manipulate data he is allowed to change. Furthermore, all changes a user makes are logged and would therefore be traceable.

All potentially unsafe data a user enters directly through fields in the user interface or is included in an API call to QuiXilver is checked and if necessary encoded to protect the system against common known attacks such as code injection or cross-site scripting (XSS). These guards also make impersonation difficult as it is practically impossible to capture the session of another user as long as common security practices on the users' computers are followed.

Audits

Tracing of Data Access

User activities on QuiXilver are logged, thus an audit and trace back of any malicious use would be possible. Create, delete, and update operations on any table data are written to specific, non-editable change log tables. For confidentiality reasons, these change log tables are by default organization-specific, so only members of the same organization can view them. Access rights can even be further restricted, e.g., to organization administrators only.

File uploads and deletions are tracked as well. The file handling includes versioning so that older versions of a file can be restored if necessary.

---

[1] Opern Web Application Security Project, see https://www.owasp.org

External Audits

External audits of QuiXilver can be conducted upon customer request.

Conclusion

As has been outlined above, QuiXilver is a secure platform for applications, collaboration and information sharing. Security measures are in place and have been reviewed to guard the confidentiality, integrity and availability of information. Security is addressed on all levels: Secure data storage, access control, security in transit, deployment and operations as well as the software itself. Audits are also possible.

The QuiXilver platform is therefore well suited also to be used in enterprise environments. Its advantages and features make it an ideal tool for collaboration and increased productivity, and companies can trust that their data will not be compromised.

Contact:

For further information, please contact us at

contact@vigience.com

Vigience LTD

Seestrasse 227

CH-8810 Horgen

Switzerland

Vigience Co. Ltd.

Vigience Building 2

7-3-8 Nishi-Gotanda,
Shinagawa-ku, Tokyo 141-0031

Japan