Qwilt Cloud Security

Updated:
10 Dec 2018

Table of Contents

1. Preface

1.1 Abstract

This document describes the Qwilt Cloud Security processes, policies and activities, allowing Qwilt to provide a secure and private solution to its customers and partners.

1.2 Purpose of this document

This document provides Customers and Partners with insight into the Qwilt Cloud Security related processes and policies.

1.3 References

Table 1 lists documents and other references that are essential for understanding the topic of this document. Note that the Qwilt Cloud is been currently deployed on the AWS cloud and using selected best practice microservices.

Table 1 - References

No.	Designation	Title
1.	AWS Inspector	https://aws.amazon.com/documentation/inspector/
2.	Center of Internet Security	https://www.cisecurity.org/
3.	Common Vulnerability Scoring System	https://www.first.org/cvss/specification-document
4.	ISO 27001	http://www.27000.org/iso-27001.htm
5.	ISO 27017	https://www.iso.org/standard/43757.html

1.4 Abbreviations and Acronyms

Table 2 provides a glossary of acronyms and terms used in this document.

Table 2 - Terminology

Term	Definition
API	Application Programmatic Interface
AWS	Amazon Web Services
ATP	Acceptance Test Plan
BW	Bandwidth
CDN	Content Delivery Network
CP	Content Provider
HTTP/S	Hypertext Transport Protocol / Secure
HW	Hardware
ISP	Internet Service Provider
ISO	International Organization for Standardization
Qwilt Cloud	Open Cache Controller
OCN	Open Caching Node
OCS	Open Cache System
PT	Penetration Test
QC	Qwilt Cloud Service Suite
QID	Qwilt System Identifier
QN	Qwilt Node
SVA	Streaming Video Alliance
SW	Software
VOD	Video on Demand

2. Qwilt Cloud overview

2.1 Qwilt Open Edge Cloud and Cloud Offering

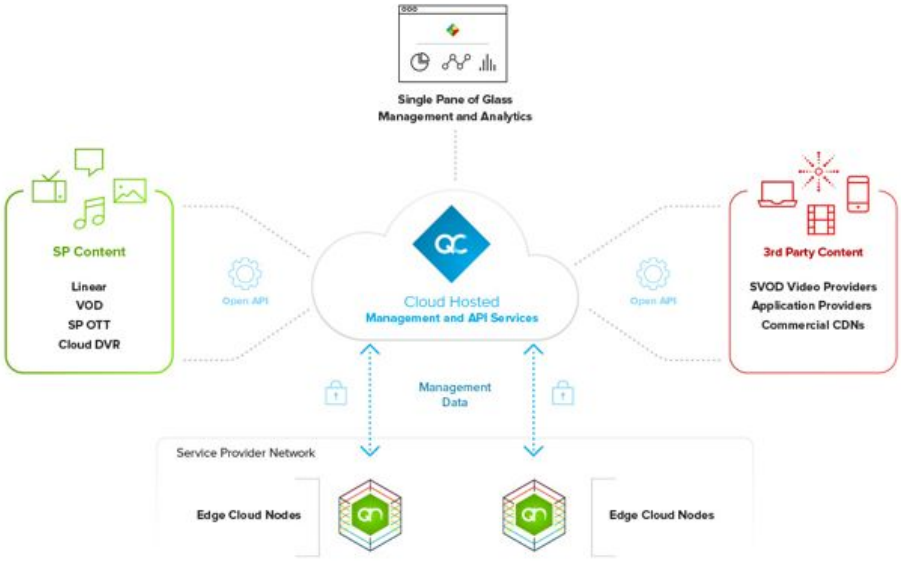

Figure 1 - Qwilt Open Edge Cloud

Today's applications are increasingly dependent on low latency and high bandwidth input, output and processing. New applications such as virtual and augmented reality as well as 4K and higher quality videos are increasingly being delivered over fixed and mobile networks. Internet of Things (IoT) sensors and autonomous vehicles are examples of applications that depend upon localized processing at the very edge of the network to facilitate low latency response to inputs. Due to these trends, fixed and mobile Internet Service Providers (ISP) are increasingly deploying their processing capabilities at the edge of their networks, typically by building new hardware platforms based upon common off-the-shelf (COTS) compute and storage and by supplying virtualized software infrastructure for running 3rd party as well as their own services.

Qwilt has developed the Open Edge Cloud platform to facilitate the deployment of content caching at the edge of the ISP network, at the closest possible location to the users of these services. Qwilt's Open Edge Cloud architecture leverages cloud management and connectivity,

open APIs and powerful small form-factor software nodes to deliver true edge content delivery capabilities built for tomorrow's application and content delivery demands. Qwilt builds the software that unlocks the potential of this ISP edge by deploying hundreds/thousands of software nodes at any point in an ISP network, from core, to metro and even to access networks. Qwilt software is simple to operate as it is 100% cloud managed. Qwilt software packs maximum performance into a small form factor that is elastic and resilient at the same time.

The Qwilt Open Edge Cloud connects applications to their edge services. Not only does the Qwilt Open Edge Cloud enable ISPs to manage all content delivery services from a single pane of glass, it also supports standardized Open Caching interfaces to enable the common delivery of managed partner content at the edge of their network.

Qwilt is a founding member of the Streaming Video Alliance (SVA) and is the leader of the Open Cache working group. SVA has developed an ecosystem where CDNs can work together with Internet Service Providers (ISP) to cost-effectively deliver content at the very edge of the ISP network, regionally maximizing end user bandwidth, without a corresponding increase of load on the ISPs central network or backbone. The Open Cache Ecosystem defines standard roles, responsibilities and interfaces by which content providers via their content delivery networks (CDNs) may delegate content caching responsibility to the ISP edge.

2.2 Qwilt Open Caching Architecture and Components

Qwilt Cloud (QC)

The Qwilt Cloud (QC) is the existing Cloud Connectivity Service Suite hosted by Qwilt in AWS. Qwilt will implement a Verizon specific ISP tenant in AWS, including secure and isolated databases.

QC™ cloud hosted connectivity services encompasses request routing, cache group and node monitoring, configuration and logging services within a single pane of glass web-based management console.

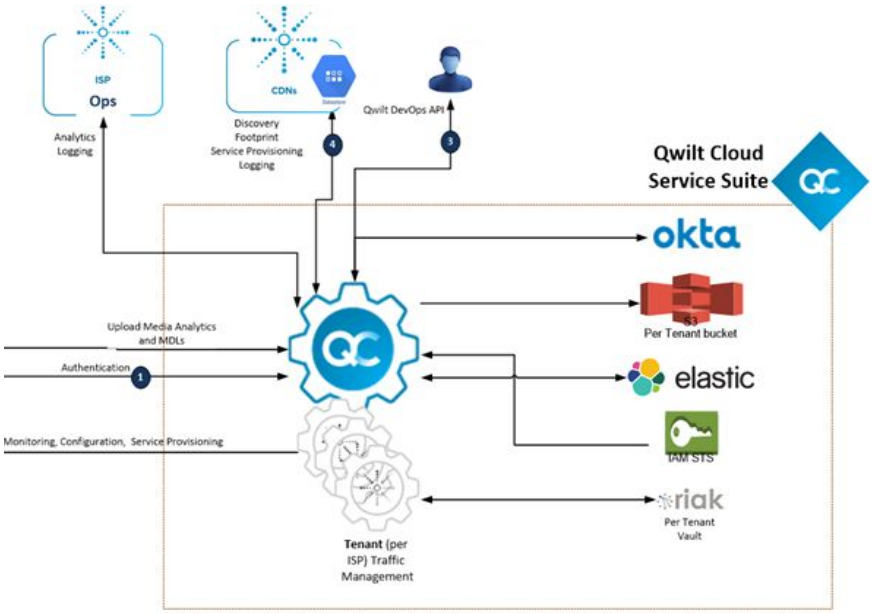

Figure 2 - Qwilt Cloud architecture

3. Certifications

The current landscape for information security standards specifically targeted for cloud computing environments is maturing. There are several cloud specific security standards initiatives that have recently been published, including ISO/IEC 27017 and ISO/IEC 27018, that provide more detailed guidance and recommendations for both cloud service customers and cloud service providers.

Current best practice for cloud service security assessments is a combination of **ISO 27001** and **ISO 27017** implementation and certification of ecosystem security requirements.

ISO 27001

The objective of the standard itself is to "provide requirements for establishing, implementing, maintaining and continuously improving an Information Security Management System (ISMS)". Further, "The design and implementation of an organization's information security management system is influenced by the organization's needs and objectives, security requirements, the organizational processes used and the size and structure of the organization".

ISO 27017
ISO/IEC 27017:2015 gives guidelines for information security controls applicable to the provision and use of cloud services by providing:

- additional implementation guidance for relevant controls specified in ISO/IEC 27002;
- additional controls with implementation guidance that specifically relate to cloud services.

This Recommendation - International Standard - provides controls and implementation guidance for both cloud service providers and cloud service customers.

Qwilt has been ISO 27001 certified and recently has completed the ISO 27017 assessment with success. Qwilt is expecting the formal certification by end of April 2018.

CERTIFICATE

This is to certify that the Security Techniques Cloud Services of

QWILT INC.

275 Shoreline Drive, Suite 510, Redwood City, CA 94065, United States

Has been assessed and complies with the requirements of :

ISO 27001:2013 And ISO 27017:2015 Best Practices

This Certificate is Applicable to

Delivers solutions for storing and streaming of video for network operators in order to increase network capacity and improve subscriber's quality of experience. Developing, training, consulting, monitoring, support and management of communication networks.

THE STANDARDS INSTITUTION OF ISRAEL

Certificate No.:	97664	**Certificate Issue Date:**	23/05/2018
Initial Certification Date:	23/05/2018	**Certification Expiry Date:**	22/05/2021

SII-QCD assumes no liability to any party other than the client, and then only in accordance with the agreed upon Certification Agreement.
This certificate's validity is subject to the organization maintaining their system in accordance with SII-QCD requirements for system certification. The continued validity may be verified via scanning the code with a smartphone, or via website www.sii.org.il. This certificate remains the property of SII-QCD.

Ilan Carmit
Acting Director General

R.N 514438761

Eli Cohen-Kagan
Director, Quality & Certification Division

The Standards Institution of Israel

Page 1 of 1

Our Vision: To Enhance Both Global Competitiveness of our Services, with our Uncompromised Quality and Integrity

Figure 6 - Qwilt ISO 27001 and 27017 certification

4. Cloud Information Security Measures

The following activities and policies are performed by Qwilt personnel in order to ensure the security of the solution and privacy of the users and data:

4.1 Secure Development

Information security is integrated into Qwilt's agile development process and tools. It is part of our user-stories and planning processes. Qwilt maintains a secure version control system to track of all changes to ensure that the code will remain consistent and manageable.
Security is part of our on-going testing efforts: in the QA, code-reviews, automated regression suites, vulnerability assessments and penetration testing.

4.2 DevSecOps - Qwilt Cloud Security Production Process

How does Qwilt ensure that our applications are secure and stay secure? How can we find and fix security issues early in the process?

Qwilt practices what is commonly referred to as "DevSecOps". DevSecOps incorporates the security team and their capabilities into Qwilt's DevOps delivery practices to ensure that security is incorporated into all production releases.

Figure 3 - DevSecOps

Continuous security validation is added at each step - from development through production - to ensure that the application is always secure. The outline of the process is as follows.

From Dev to DevOps:
Once the quality of new code is verified, the application is deployed to a new environment also known as Staging. The Staging process verifies that there are no security vulnerabilities in the running application. This verification is accomplished by executing automated penetration test against the running application to scan for vulnerabilities.

The Amazon Inspector (https://aws.amazon.com/inspector/) is utilized for all existing Qwilt Cloud services that have been implemented using AWS resources. The Amazon Inspector has been optimized for AWS resource security assessments.

Amazon Inspector is an automated security assessment service that automatically assesses applications for vulnerabilities or deviations from best practices. After performing an assessment, Amazon Inspector produces a detailed list of security findings prioritized by level of severity.

Amazon Inspector incorporates a built-in library of rules and reports. **These include checks for best practices, common compliance standards and vulnerabilities.** These checks include detailed recommended steps for resolving potential security issues.

The two leading compliance standards are:

- Common Vulnerability Scoring System (CVSS) see https://www.first.org/cvss/.
- Center of Internet Security (CIS) see https://www.cisecurity.org/.

The assessment is targeted at AWS resources working together as a unit. The monitored resources include network, file system and process activity. During the assessment a wide set of activity and configuration data is collected. This data includes:

1. Details of communication with AWS services
2. Use of secure channels
3. Details of the running process
4. Network traffic among the running processes
5. More....

4.3 Penetration Test

Qwilt regularly contracts security experts to perform multiple external penetration tests in order to identify and flag security issues with our target processes.

4.4 Use of Encryption

As a rule any API exposed by QC and between QC elements utilizes TLS in order to encrypt all data in transit.
Data at rest is classified and is encrypted as needed.
We use TLSv1.2 with AES_128_GCM_SHA256 cipher.

4.5 Obfuscation of Personal Identity Information

As a rule the QC does not handle any Personal Identity Information of the ISP subscribers.
PII such as subscriber IP address in MDLs is obfuscated by performing, on the QN, a SHA-256 Cryptographic Hash Algorithm using a different secret per QN.

4.6 QC User Account and Authentication

Users of QC API's can be one of two types: humans or machines, and belong to one of the following three logical groups (organizations): Service Providers, CDNs or Qwilt DevOps team: In no case, can a user be of both types simultaneously, nor belong to more than one logical group.

User Statuses

A user (any kind of user) can be in one of the following statuses:

- **Active** - User may login to QC and perform permitted operations
- **Inactive** - User is registered in QC, but cannot login not perform any operations
- **Blocked** - A status of an Active user becoming temporarily inactive (due to recurrent login attempts, license enforcement, etc.). This case cannot be set manually (change to block), only unset manually (change to active or inactive)

NOTE: A user cannot change its own status. Such an operation requires a different user with higher privileges

QC UAA system is based on Stormpath/Okta identity management product for user authentication purposes. This includes:

- HTTPS only protocol
- OAuth 2.0 compliant API
- Encryption, salting and hashing of passwords
- JWT Token based authentication, including:
    - SHA-256 signing algorithm
    - Short lived access tokens
- Protection against web site attacks (SQL injections, CSRF, XSS)
- Cross Origin Request Sharing (CORS) limits JavaScript access to whitelisted QC endpoints
- Secured cookie management (no JavaScript access, sent only on secured connections)
- QC user management:
    - Private platform - no automated "signup" functionality;
    - New users are created by Qwilt Customer Care personnel and assigned to appropriate tenants following human validation of identity
    - The customer is required to formally update Qwilt's Customer Care on the need to remove users from this customer's tenat.
    - Tenants and all of their users are removed soon after the expiration of the business agreement with the tenant entity.

- Account initial registration and recovery (forgot password) is done via the user's email address
- Self-service user credentials management - password are never stored in plain text, nor are ever visible to any Qwilt personnel

QC credential types

- Human credentials are username and password
- Machine credentials are an API key and secret (currently not self-serviced)

Data Isolation

The QC API provides tenant (ISPs, CDNs, CPs) data isolation in the application layer and in data store layer either physically (e.g. different S3 buckets per tenant) or logically (e.g. different tables on SQL database).

4.7 Data Life Cycle management

QC is a multi-tenant environment and as such data handling is engineered to allow access of each tenant to their data and only to their data.
For example MDL logs are kept in per device per customer S3 bucket and the authorization is managed so the access of the customer is only to logs within their buckets, and the old MDLs are removed after a pre-agreed time.
Similarly to users, tenant's data is removed soon after the expiration of the business agreement with the tenant entity.

4.8 Qwilt Cloud Key Vault

QC is using Basho Riak KV data store for securing SSL credentials and private keys, key that will be used for HTTPS delivery by the ISP open caches (QNs).

QC holds a dedicated data store for each tenant (i.e. ISP or CDN) where:

- Data store is configured with SSL key and certificates.
- Qwilt DevOps admin are the only ones granted with administrator privileges.
- The admin user is provided full administrative privileges.
- Customers and partners can perform ADD operation of certificates and keys and only via an API

And per new Open Caching service:

- Credentials and private keys are being configured by the DevOps admin users.

5. Change Management

Qwilt constantly improves the solution's information security capabilities and updates the solution infrastructure from time to time in order to incorporate security vulnerability fixes. Updates to Qwilt's solution are communicated over:

1. Customer push notes
2. RN in our website- Qwilt.com
3. Qwilt Cloud UI

6. Handling Information Security Incidents

Qwilt handles information security incidents similarly to handling of any other customer impactive service oriented incidents. All relevant incidents are documented in the CRM and are maintained by Qwilt's customer care and DevOps engineers.

Customers and partners will be notified by Qwilt's customer-care engineer on Information Security Incidents that impact their services, data or network soon after they are identified and will receive updates on the scope and severity of the incident.

Customers and partners that identify information security incidents related to Qwilt service or that might impact Qwilt's service, are obliged to notify Qwilt's Customer-care as soon as they are aware of the incident and provide all relevant information.