CONTENTSQUARE

Technical Security Measures

Cloud security infrastructure & architecture

CONTENTSQUARE

CLOUD HOSTING

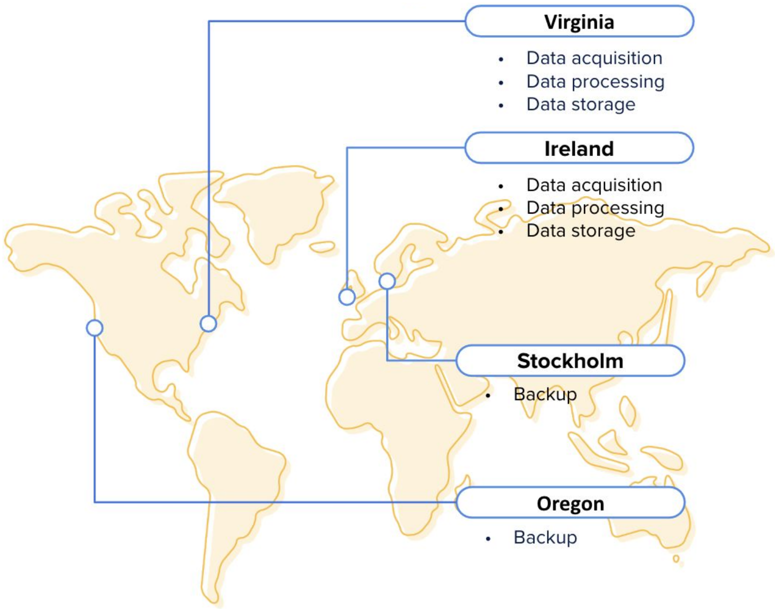
Contentsquare leverages AWS and Azure as its cloud providers.
The cloud provider manage the physical and environmental security of facilities and the logical security of high level services that Contentsquare relies on. Physical access is strictly controlled both at the perimeter and at building ingress points by professional security staff using video surveillance, state of the art intrusion detection systems, and other electronic means. Authorized staff must pass two-factor authentication a minimum of two times to access data center floors. All physical access by employees is logged and routinely audited.
Cloud computing environments are continuously audited, with certifications including ISO 27001, FedRAMP, DoD CSM, and PCI DSS (https://aws.amazon.com/compliance/, https://docs.microsoft.com/en-us/azure/compliance/)
They are also fully compliant with applicable EU data protection laws.
Physical and environmental security controls of cloud data centers are described here: https://aws.amazon.com/compliance/data-center/controls/, https://docs.microsoft.com/en-us/azure/security/fundamentals/physical-security

DEPLOYMENT MODEL

Contentsquare provides a multi-tenant SaaS service meaning that all customer share the same platform. As such, it's important that users only be able to access their own organization's information. That's why Contentsquare services use unique organization identifiers. These identifiers are assigned with each new session, so that your data is available only to those who are authorized to access it.
Contentsquare leverages a Virtual Private Cloud (VPC) which provides advanced security features, such as security groups and access control lists (ACLs), to enable inbound and outbound filtering at the instance and subnet level

REGIONS

EU pipeline: Production in AWS Ireland, Backup in AWS Stockholm
US pipeline: Production in AWS North Virginia, Backup in AWS Oregon



AVAILABILITY & SCALABILITY

Each region encompass 3 Availability Zones (AZ). Each zone in a region has redundant and separate power, networking and connectivity to reduce the likelihood of two zones failing simultaneously.
In each zone, participating data centers are connected to each other over redundant low-latency private network links. Likewise, all zones in a region communicate with each other over redundant private network links. These intra and inter-zone links are heavily used for data replication by a number of services including storage and database management.
This ability to leverage multiple zones is paramount for building a highly available, fault-tolerant service.
While the cloud third-party provides features for vertical scalability, the horizontal scalability of Contentsquare service is ensured by working with a "infrastructure as code" paradigm which is the process of managing and provisioning machines through machine-readable definition files, rather than physical hardware configuration or interactive configuration tools

TECHNICAL ACCESS MANAGEMENT

Contentsquare is using RBAC for authentication and authorization of its technical administrators on its infrastructure. RBAC enables security best practices by allowing us to grant unique security credentials to users and groups to specify which service and resources administrators they can access. RBAC is secure by default; users have no access to resources until permissions are explicitly granted. Each user is belonging to groups with different authorisations. The scope of authorisations is limited in each case to the absolute minimum necessary for performing tasks or functions.
Two-factor authentication is enabled and mandatory for administrators.
Contentsquare technical administrators can also connect to production servers via a unique SSH gateway, which is the entry point the the VPC. Server accesses are performed via 4096 bits RSA keys (private key protected by a passphrase).
These accesses are only provided following an internal validation workflow that focuses on need-to-know and need-to-use principles. Furthermore, all accesses are reviewed every 6 months.

SECURITY TESTING OF THE INFRASTRUCTURE

An annual penetration test targeting our infrastructure and public facing services is conducted annually by external security specialists.
Monthly automated vulnerability scans and cloud compliance assessments (following the Foundations Benchmark) are also performed As well, a private bug bounty program is in place

ENCRYPTION

- **In-transit encryption**

Strong cryptography mechanisms are implemented to ensure data in-transit and at-rest security:

- Data in transit is encrypted and secured from the user's browser to the application via TLS (ranked A by Qualys SSL labs)
- VPN and SSH for technical administratives accesses

- **At-rest encryption**

We rely on industry-grade mechanisms to secure at-rest data:

- Applicative user passwords are secured using a dedicated hashing function (SHA-512) with salting
- Buckets storing data are encrypted with AES-256 (One key per object, key AES-256 encrypted with a masterkey managed with AWS KMS)

HTTPS/TLS STRENGTH

CS Digital application only negociates HTTPS/TLS session with TLSv1.2 which is the standard for in-transit encryption
Tag negotiates HTTP/TLS session with TLSv1.2, TLSv1.1 and TLSv1.0.
This depends only on users' browser : up-to-date browser will only negotiates session with TLSv1.2 whereas TLSv1.0 is maintained for compatibility with old browsers.
SSLv2 and SSLv3 cypher suites are all rejected are they are not considered secure anymore.

SERVER SECURITY

Systems configuration are managed as code with Ansible. Weekly, systems are monitored with OpenSCAP and CIS benchmark to ensure compliance with security best-practices and that systems are free of vulnerabilities.
Contentsquare leverages "unattended-upgrade" to perform daily check for new security patch and ensure that our systems are always up-to-date.
An Host-based Intrusion Detection System (Wazuh - OSSEC fork) is implemented on all sensitive systems in order to monitor all aspects of system activity with file integrity monitoring, log monitoring, rootcheck, and process monitoring. All security events are then pushed to a dedicated stack (ELK - ElasticSearch / Logstash / Kibana) that acts as a SIEM and correlates all security logs to detect potential intrusions or malicious activities.

BACKUP & DISASTER RECOVERY

The infrastructure is designed for resilience or restoration in case of service-impacting events. Contentsquare provides disaster recovery and business continuity through multiple means :

- Use of several Availability Zones in the region
- Use of an "infrastructure as code" paradigm which allows rebuilding a full platform from scratch
- Replication of data in a backup region

Contentsquare main data are replicated into another region that is fully segregated from the Ireland production region. This backup region is part of our Disaster Recovery Plan and comes with the following security feature:

- Backup data are located in an isolated region that is not the same geographical location as the production one
- The Disaster Recovery Plan is tested at least annually and RTO / RPO are compared with designed objectives.
- All data kept in the backup region are stored within **encrypted (AES-256) blob storage.**
- Only key employees have access to this backup infrastructure. Furthermore these employees do not have access to the Ireland production infrastructure.
- Access to this region follows strong security requirements :
    - Strong password policy
    - Mandatory 2 factors authentication

CHANGE MANAGEMENT

Infrastructure changes including configuration changes are managed as code modification and follow the SDLC workflow (peer-review, traceability,...)

DATA DELETION

All our blob storage are encrypted and there is one encryption key per object.
When data is deleted, the encryption key associated to that data is deleted and content can't be retrieved
On top of that, as storage is virtual storage, the associated block space related to that object is freed and available only for write operations.
Those controls ensure that deleted data can't be retrieved.

Product Security

CONTENTSQUARE

SDLC

Before deployment, new developments are qualified, reviewed and automatically tested through our code quality pipeline which validates that the version conforms with our standards in terms of functionality, performance and security :

- Code is peer-reviewed before being committed to the master code branch
- Functional and unit tests are performed using automated tools
- Code is reviewed with SonarQube and Guardrails.io (SAST - static code analysis tools) to detect potential vulnerabilities like injection flaws, input validation before shipping code to production
- Dynamic Application Security testing (DAST) is performed with Cypress framework
- Clair is used for the static analysis of vulnerabilities in docker application containers
- Developers are regularly trained on secure coding practices following OWASP security best practices

Development and production environment are associated with a dedicated VPC that ensure a full segregation between these two environments.

APPLICATION AUTHENTICATION

End-user authentication to Contentsquare's SaaS application uses a login / password scheme with the following security requirements :

- 8 characters minimum length
- Complexity enforced (numeric, special and upper characters)
- To protect against dictionary-based, brute-force attacks, user accounts are prompted with a CAPTCHA mechanism after several failed login attempts
- 8 hour JWT token expiration
- End-users passwords are stored securely (SHA-512 hash with salt)

Single sign-on is available. Supported protocol is SAML 2.0.

WEB-APPLICATION FIREWALL

Contentsquare leverages Sqreen.io service that acts as a web-application firewall and provides the following security features :

- Detect and block application-level attacks and vulnerabilities (injection, LFI, XSS ...)
- Incident response automation

DATA SEGMENTATION / SEGREGATION

Contentsquare provides a multi-tenants service that means that customers share the same infrastructure.
The segmentation of customer data is logical : all data collected is linked to a customer ID that is required by the application to fetch back the data.
This principle of segmentation of data is also automatically tested before release with End-to-end tests and during our penetration tests.

PRODUCT PENETRATION TESTS & SECURITY TESTING

A yearly third-party penetration test is performed to detect potential vulnerabilities and ensures that our applications are in compliance with industry standards. The tests cover :

- Tag
- Data acquisition pipeline
- Web applications

The report can be provided to customers upon request and with a Non-Disclosure Agreement (NDA).
Contentsquare welcomes customers and potential customers to independently verify our product security by conducting their own vulnerability assessments and penetration tests. **These tests can be performed yearly and can come with a cost. Contentsquare must formally authorize each test.** Customer can reach security@contentsquare.com to request a pentest authorization (SEC07 - Penetration test protocol.docx)
The preparation of those pentests can take some time on our end (having the protocol signed by the customer, IP address whitelisting) so please anticipate those when possible.
To be noted that we don't authorize automated vulnerability scans as they generate a lot of noises and a lot of false positives.

TAG SECURITY

We are completely aware that the main risk about our solution is the hijacking of the javascript that is used as third-party libraries.
To protect against that we have the following layer of controls :

- SDLC process with peer-review, static code analysis and dynamic analysis of every change, this process is audited by external party is it is in the scope of our ISO 27001 certification
- External penetration tests of our tag (report can be provided on demand)
- Compatible CSP : https://docs.contentsquare.com/uxa-en/#content-security-policy-csp-compatibility

While we acknowledge that SRI (sub-ressources integrity) is a way to protect against these type of attacks, we have chosen an other implementation for our default deployment for the following reasons :

- We change the TAG very often
- SRI are not supported by all browsers and need to be activated by customers
- In case of Tag hijacking, we would have to wait for customers to give us feedback about SRI errors so we would loose a lot of time.

To protect against that, we have chosen to check ourselves the integrity of the javascript Tag. Every 10 minutes, we are comparing the integrity of the Tag from multiple endpoints (after CDN from multiple location, before CDN in S3 buckets) with a trusted value that is generated when we build the Tag. In case of mismatch an alerts is directly sent to our on-call security team. We believe this is a better solution as we can actively monitor this scenario of attack and because we are not relying on client implementation / controls.
If your security policy requires to use Sub-resource Integrity to integrate the Contentsquare tracking tag on your application, you can deploy our tag using the SRI method we have developed : https://docs.contentsquare.com/sri/
Please note that the use of SRI will change the deployment of the tag and its updates.

Corporate Security

CONTENTSQUARE

SECURITY ORGANIZATION & GOUVERNANCE

Led by the Chief Information Security Officer (CISO), Contentsquare has an established function responsible for security and data compliance across the organization. A critical part of any Information Security Management System (ISMS) and Privacy Information Management System (PIMS) is the continual improvement of security, privacy and compliance programs, systems, and controls. Contentsquare is committed to soliciting feedback from different internal teams, customers, internal and external auditors, and improving our security, privacy and compliance processes and controls over time.

Contentsquare security governance, ISMS and PIMS closely follow the ISO/IEC 27001 and ISO/IEC 27701 standards:

- Annual risk analysis
- Key Performance Indicators are issued monthly to ensure that the ISMS is running efficiently
- Dedicated security policies and procedures:
    - **ISMS & PIMS Policy**
    - **Risk management policy and Risk analysis**
    - **Asset Management Policy**
    - **HR Security Policy**
    - **IT Security Policy**
    - **Access Management Policy**
    - **Engineering Security Policy**
    - **Physical and Environmental Security Policy**
    - **Supplier Security Policy**
    - **Incident Management Policy and Incident response guides**
    - **Business Continuity Policy**
    - **Global Privacy Network**
    - **Privacy by Design & By Default Policy**
    - **DPIA Policy**
- Annual ISMS & PIMS internal audit

All security policies and procedures are reviewed annually.

RISK MANAGEMENT

Contentsquare has implemented risk management processes to identify and manage risks that may affect the system's security, availability, and confidentiality. At least annually, Security & Privacy leadership performs a risk assessment to identify and evaluate potential threats to the effectiveness of the control environment.
Additionally, a risk register is continually maintained and updated by the Security & Privacy teams to ensure risks are continually identified, tracked, and mitigated based on magnitude and frequency.

HUMAN RESOURCES SECURITY

Security starts with the people Contentsquare employs. Contentsquare also invests in properly vetting and training staff to ensure that there is an organization-wide appreciation for data security. Before hire, limited background checks (identity, education) are performed by the Human Resources team. New employees must sign confidentiality agreements as part of their work contract and must complete a Security Awareness and Data Privacy training as part of the onboarding into the organization. All employees are also reminded of best practices through internal communications.

SUPPLIER MANAGEMENT

The Security, Privacy and Legal teams perform a review of third-parties, vendors and suppliers subservice providers during onboarding to ensure agreements meet Contentsquare's security, availability, confidentiality and privacy requirements.
On an annual basis, subservice provider risks are evaluated and applicable third-party attestation reports (i.e. SOC 1, SOC 2, ISO 27001, etc.) are obtained and reviewed for issues that might impact security, availability, confidentiality and privacy of Contentsquare services.

CORPORATE IT SECURITY

Contentsquare IT corporate resources are not used to store or process customer's data. However, they support processes related to the delivered services (SDLC, administration, monitoring). Due to this, these systems also require an appropriate level of safeguards:

- Corporate networks are fully segregated from production networks
- Corporate networks are monitored by an Intrusion Detection System
- Corporate networks and devices are analysed monthly with a vulnerability scanner
- Laptops are pre-configured with an endpoint protection and antivirus software
- Laptops hard-drives are encrypted at-rest
- Clean desk policy

SECURITY INCIDENT

A security incident management process is established to timely respond incidents. Contentsquare's Security Incident Response Plan is made available on the intranet. Employees are made aware of how to report a potential security incident. Specifically, the incident response plan defines and documents types of incidents that need to be managed, tracked and reported, and includes the following:

- Procedures for the identification, management, and resolution of security incidents
- List of relevant authorities' contact information
- Process for notifying customers (48 hours commitment for security incidents impacting customers)
- Process for learning from the incidents
- Process for safeguarding evidence

Contentsquare has contracted a cybersecurity insurance (CyberEdge by AIG) that would cover response, investigation and notification costs in case of major incidents.

Compliance

CONTENTSQUARE

CERTIFICATION

Contentsquare is **ISO/IEC 27001** and **ISO/IEC 27701** certified.
The scope of Contentsquare certification includes the design, development, implementation, monitoring, administration, and support of Contentsquare's Software As a service as centrally managed out of the Contentsquare Headquarters in Paris - France, New-York – United States, London – United Kingdom.

Our ISO 27001 certification also covers all of the 133 security measures described in the ISO 27001 Annex A.
Our ISO 27701 certification's scope encompasses both of our controller and processor role.

These certification audits will be followed by an annual surveillance audit and certification audit every 3 years.

SECURITY REPORTS

Contentsquare holds a **SOC 2 Type 2 Report**, available for review upon request (under NDA). This report testifies of our level of maturity over the course of 12 months and presents our commitment in terms of security standards.

This report is aligned with the requirements stated in our client contracts and thus, demonstrates the truthful implementation of these requirements at Contentsquare.

REGULATORY COMPLIANCE

Companies are responsible for complying with all applicable laws, including those related to data privacy and transmission of personal data, even when a service provider holds and processes a company's data on its behalf.
Contentsquare Legal Department is in charge of compliance with European and national privacy laws and regulations.

DATA RETENTION & DISPOSAL

Following CNIL's recommendations, acquired data is stored for 13 months and then erased from our servers for all clients.

PRIVACY

Contentsquare privacy policy is publicly available : https://contentsquare.com/privacy-center/privacy-policy/
Customers remain owner of the collected data and Contentsquare acts as a sub-processor.
A Data Protection Officer has been appointed to lead Contentsquare privacy strategy and can be reached at **dpo@contentsquare.com**

DATA COLLECTION

To prevent the collection, saving or display of PII through our products, we have developed a number of implementation tools, including:
Client-side keystroke block - By default, Contentsquare’s client-side keystroke block ensures that our product only keeps track of when keys are clicked, without keeping track of which keys are clicked. This helps customers ensure that no keystrokes are logged or recorded by our products, nor sent via the network.
PII exclude block - Customers may also tag sensitive data in the HTML with HTML comments, in order to ensure that any PII in data is removed by the Contentsquare parser before being stored on to Contentsquare’s servers.
When a visitor session is complete, Contentsquare determines and saves the geographical location of the visitor based on the IP address. Contentsquare delete the IP address after this process.

ISO/IEC 27001 & ISO/IEC 27701 Certifications

CONTENTSQUARE

WHAT IS ISO 27001 AND ISO 27701?

ISO/IEC 27001:2013 is a widely recognized and internationally accepted information security standard that establishes requirements related to Information Security Management Systems (ISMS), a systematic approach to keeping manage and improve continuously the security of an organisation.
An ISMS is a framework and related set of policies and procedures designed to manage an organization's risk, confidential information, and security approach.

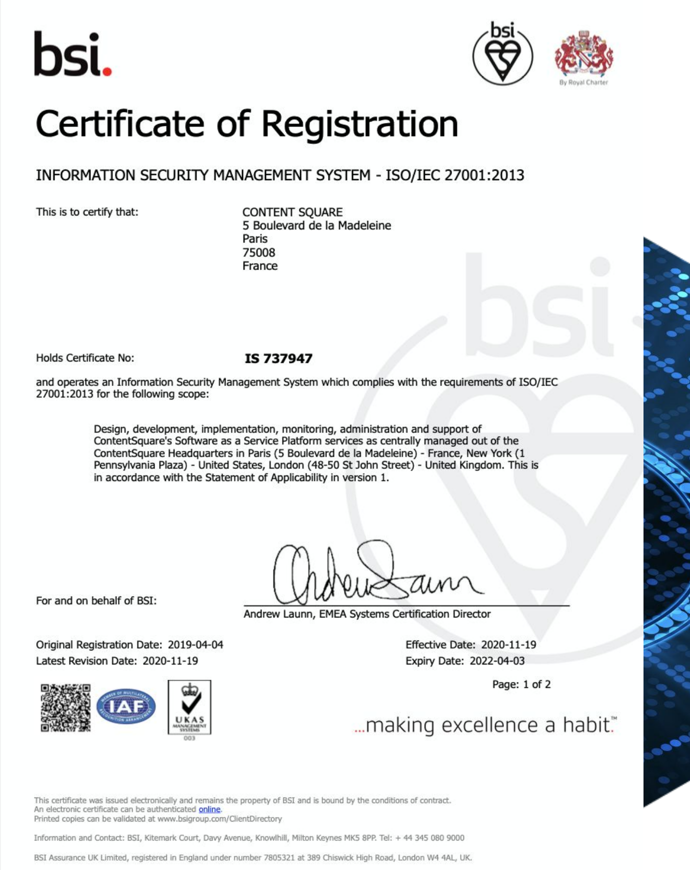
ISO/IEC 27701:2019 is a privacy extension to ISO/IEC 27001. The design goal is to enhance the existing ISMS with additional requirements in order to establish, implement, maintain, and continually improve a Privacy Information Management System (PIMS).

These certification audits will be followed by an annual surveillance and certification audit every 3 years.

SCOPE OF THE CERTIFICATIONS

The scope of our certifications includes the design, development, implementation, monitoring, administration, and support of Contentsquare's Software As A Service as centrally managed out of the Contentsquare Headquarters in Paris - France, New-York – United States, London – United Kingdom and Ramat Gan - Israel.
Our ISO/IEC 27001 and ISO/IEC 27701 certifications also cover all of the 133 security measures described in the ISO 27001 Annex A, and encompasses both of our controller and processor role.

- ISMS & PIMS Policy
- Organization of Information Security
- Human Resource Security
- Asset Management
- Access Control
- Cryptography
- Physical and Environmental Security
- Operation Security
- Communication Security
- System Acquisition, Development & Maintenance
- Supplier Relationships
- Business Continuity
- Compliance



bsi.

Certificate of Registration

INFORMATION SECURITY MANAGEMENT SYSTEM - ISO/IEC 27001:2013

This is to certify that:

CONTENT SQUARE
5 Boulevard de la Madeleine
Paris
75008
France

Holds Certificate No: **IS 737947**

and operates an Information Security Management System which complies with the requirements of ISO/IEC 27001:2013 for the following scope:

Design, development, implementation, monitoring, administration and support of ContentSquare's Software as a Service Platform services as centrally managed out of the ContentSquare Headquarters in Paris (5 Boulevard de la Madeleine) - France, New York (1 Pennsylvania Plaza) - United States, London (48-50 St John Street) - United Kingdom. This is in accordance with the Statement of Applicability in version 1.

For and on behalf of BSI:

Andrew Launn, EMEA Systems Certification Director

Original Registration Date: 2019-04-04
Latest Revision Date: 2020-11-19

Effective Date: 2020-11-19
Expiry Date: 2022-04-03

Page: 1 of 2

...making excellence a habit.™

This certificate was issued electronically and remains the property of BSI and is bound by the conditions of contract.
An electronic certificate can be authenticated online.
Printed copies can be validated at www.bsigroup.com/ClientDirectory

Information and Contact: BSI, Kitemark Court, Davy Avenue, Knowlhill, Milton Keynes MK5 8PP. Tel: + 44 345 080 9000

BSI Assurance UK Limited, registered in England under number 7805321 at 389 Chiswick High Road, London W4 4AL, UK.

CONTENTSQUARE

Thanks