CAST

CAST Imaging Express

Security summary

Rev 2 | Jan 2026

CAST provides secure -based products and services used by companies with strict security requirements (Gov / BFSI / Utilities)

Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
MINISTÈRE DES ARMÉES

CA

WELLS FARGO

BMW

NEW YORK LIFE

Home Office

GRDF
GAZ RÉSEAU DISTRIBUTION FRANCE

UNITED STATES AIR FORCE

First Data is now fiserv.

FannieMae.

Broadridge

MarshMcLennan

NORTHERN TRUST

XL

AXA

BNP PARIBAS
PERSONAL FINANCE

And many others…

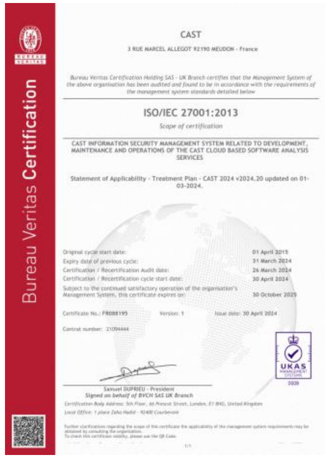
ISO 27001, 27017 and 27018 Certifications

Since 2015, CAST is ISO 27001 certified for the following activities:

- Executive and Product Management
- Development and Quality Assurance
- Release management
- Operating and Facilities management
  - Latest certificate date: April 30th, 2024 by Bureau Veritas

Since then, the certification has been extended:

- ISO 27017: Information security controls for services
  - Since 2019. Latest certificate date: March 19th, 2025 by Bureau Veritas
- ISO 27018: Protection of personally identifiable information (PII) in public s
  - Since 2019. Latest certificate date: March 19th, 2025 by Bureau Veritas
- ISO 27701: Privacy Information Management requirements and guideline
  - Since 2023. Latest certificate date: April 5th, 2023 by Bureau Veritas



Bureau Veritas Certification

CAST

3 RUE MARCEL ALLEGOT 92190 MEUDON - France

Bureau Veritas Certification Holding SAS - UK Branch certifies that the Management System of the above organisation has been audited and found to be in accordance with the requirements of the management system standards detailed below

ISO/IEC 27001:2013

Scope of certification

CAST INFORMATION SECURITY MANAGEMENT SYSTEM RELATED TO DEVELOPMENT, MAINTENANCE AND OPERATIONS OF THE CAST CLOUD BASED SOFTWARE ANALYSIS SERVICES

Statement of Applicability - Treatment Plan - CAST 2024 v2024.20 updated on 01-03-2024.

Original cycle start date:	01 April 2015
Expiry date of previous cycle:	31 March 2024
Certification / Recertification Audit date:	26 March 2024
Certification / Recertification cycle start date:	30 April 2024
Subject to the continued satisfactory operation of the organisation's Management System, this certificate expires on:	30 October 2025

Certificate No.: FR088195 Version: 1 Issue date: 30 April 2024

Contrat number: 21094444

UKAS MANAGEMENT SYSTEMS 0008

Samuel DUPRIEU - President

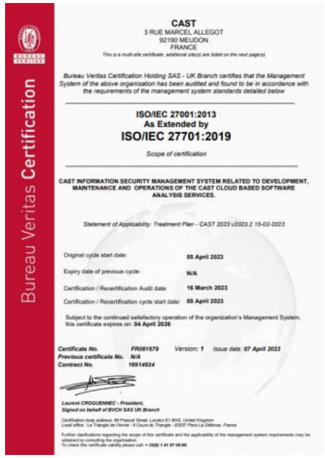
Signed on behalf of BVCH SAS UK Branch

Certification Body Address: 5th Floor, 66 Prescot Street, London, E1 8HG, United Kingdom

Local Office: 1 place Zaha Hadid - 92400 Courbevoie

Further clarifications regarding the scope of this certificate the applicability of the management system requirements may be obtained by consulting the organization.
To check this certificate validity, please use the QR Code.

1/1



Bureau Veritas Certification

CAST
3 RUE MARCEL ALLEGOT
92190 MEUDON
FRANCE

This is a multi-site certificate, additional site(s) are listed on the next page(s)

Bureau Veritas Certification Holding SAS - UK Branch certifies that the Management System of the above organisation has been audited and found to be in accordance with the requirements of the management system standards detailed below

ISO/IEC 27001:2013
As Extended by
ISO/IEC 27701:2019

Scope of certification

CAST INFORMATION SECURITY MANAGEMENT SYSTEM RELATED TO DEVELOPMENT, MAINTENANCE AND OPERATIONS OF THE CAST CLOUD BASED SOFTWARE ANALYSIS SERVICES.

Statement of Applicability: Treatment Plan - CAST 2023 v2023.2 15-02-2023

Original cycle start date:	05 April 2023
Expiry date of previous cycle:	N/A
Certification / Recertification Audit date:	16 March 2023
Certification / Recertification cycle start date:	05 April 2023

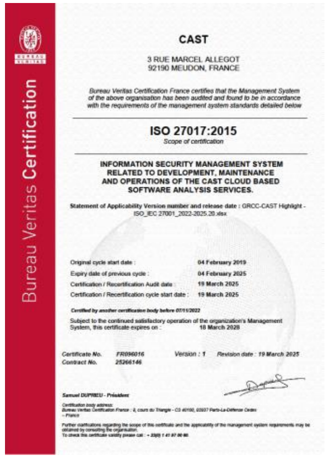
Subject to the continued satisfactory operation of the organization's Management System, this certificate expires on: **04 April 2026**

Certificate No. *FR081679* Version: 1 *Issue date: 07 April 2023*
Previous certificate No. *N/A*
Contract No. *16914924*

Laurent CROGUENNEC - President,
Signed on behalf of BVCH SAS UK Branch

Certification body address: 66 Prescot Street, London E1 8HG, United Kingdom
Local office : Le Triangle de l'Arche - 9 Cours du Triangle - 92937 Paris La Défense, France

Further clarifications regarding the scope of this certificate and the applicability of the management system requirements may be obtained by consulting the organisation.
To check this certificate validity please call: + 33(0) 1 41 97 00 60



Bureau Veritas Certification

CAST

3 RUE MARCEL ALLEGOT
92190 MEUDON, FRANCE

Bureau Veritas Certification France certifies that the Management System of the above organisation has been audited and found to be in accordance with the requirements of the management system standards detailed below

ISO 27017:2015

Scope of certification

INFORMATION SECURITY MANAGEMENT SYSTEM RELATED TO DEVELOPMENT, MAINTENANCE AND OPERATIONS OF THE CAST CLOUD BASED SOFTWARE ANALYSIS SERVICES.

Statement of Applicability Version number and release date : GRCC-CAST Highlight - ISO_IEC 27001_2022-2025.20.xlsx

Original cycle start date :	04 February 2019
Expiry date of previous cycle :	04 February 2025
Certification / Recertification Audit date :	19 March 2025
Certification / Recertification cycle start date :	19 March 2025

Certified by another certification body before 07/11/2022

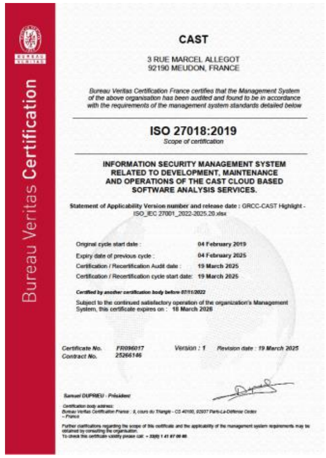
Subject to the continued satisfactory operation of the organization's Management System, this certificate expires on : **18 March 2028**

Certificate No. *FR096016* Version : 1 *Revision date : 19 March 2025*
Contract No. *25266146*

Samuel DUPRIEU - Président

Certification body address:
Bureau Veritas Certification France : 9, cours du Triangle - CS 40100, 92937 Paris-La-Défense Cedex - France

Further clarifications regarding the scope of this certificate and the applicability of the management system requirements may be obtained by consulting the organisation.
To check this certificate validity please call : + 33(0) 1 41 97 00 60



Bureau Veritas Certification

CAST

3 RUE MARCEL ALLEGOT
92190 MEUDON, FRANCE

Bureau Veritas Certification France certifies that the Management System of the above organisation has been audited and found to be in accordance with the requirements of the management system standards detailed below

ISO 27018:2019

Scope of certification

INFORMATION SECURITY MANAGEMENT SYSTEM RELATED TO DEVELOPMENT, MAINTENANCE AND OPERATIONS OF THE CAST CLOUD BASED SOFTWARE ANALYSIS SERVICES.

Statement of Applicability Version number and release date : GRCC-CAST Highlight - ISO_IEC 27001_2022-2025.20.xlsx

Original cycle start date :	04 February 2019
Expiry date of previous cycle :	04 February 2025
Certification / Recertification Audit date :	19 March 2025
Certification / Recertification cycle start date:	19 March 2025

Certified by another certification body before 07/11/2022

Subject to the continued satisfactory operation of the organization's Management System, this certificate expires on : **18 March 2028**

Certificate No. *FR096017* Version : 1 *Revision date : 19 March 2025*
Contract No. *25266146*

Samuel DUPRIEU - Président

Certification body address:
Bureau Veritas Certification France : 9, cours du Triangle - CS 40100, 92937 Paris-La-Défense Cedex - France

Further clarifications regarding the scope of this certificate and the applicability of the management system requirements may be obtained by consulting the organisation.
To check this certificate validity please call: + 33(0) 1 41 97 00 60

Audit – Penetration Testing

Software and services will be regularly assessed

- Yearly penetration test by third party specialists

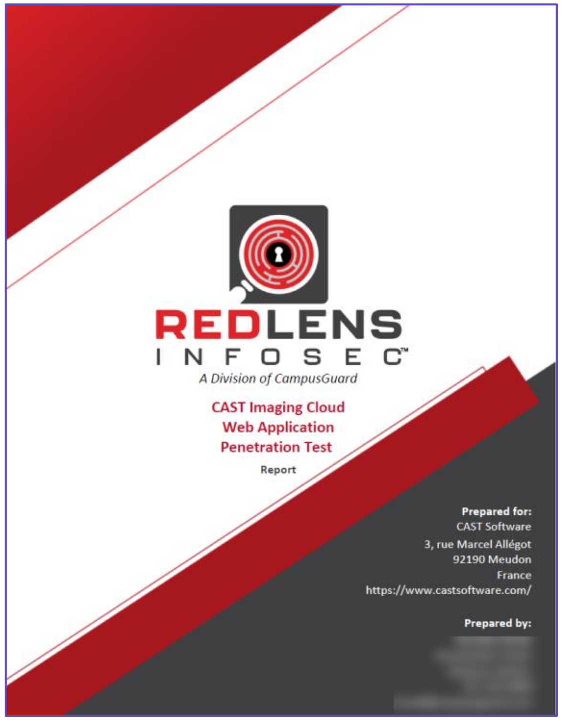
  Campusguard Redlens 2025

  > *“Overall, RedLens feels that the CAST Imaging – application closely follows industry standards for application security and that the CAST team takes the addressing, fixing, and retesting of discovered vulnerabilities seriously and implements these changes in a timely and efficient manner”*

- Automatic code scan integrated within the CI

- Open-source code used within CAST Imaging is evaluated monthly through the generation of a BOM

- CAST has conducted penetration testing with consistently positive assessments for various products and services since 2014



REDLENS
INFOSEC™
A Division of CampusGuard

CAST Imaging Cloud
Web Application
Penetration Test
Report

Prepared for:
CAST Software
3, rue Marcel Allégot
92190 Meudon
France
https://www.castsoftware.com/

Prepared by:
[redacted]

Information Security Management System

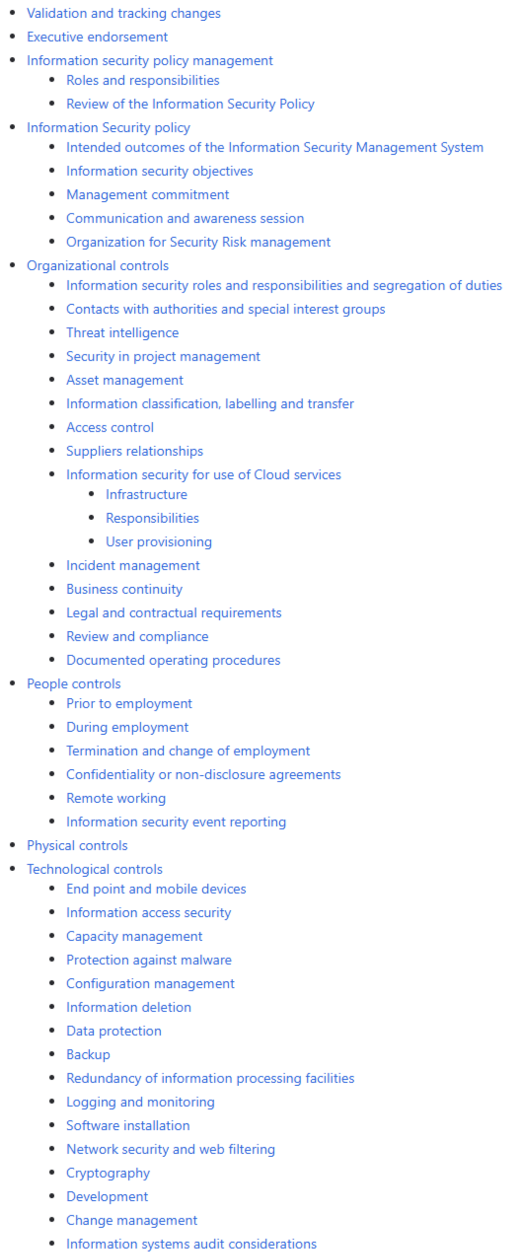
Since 2008, CAST has implemented an information security policy that ensures that risk is minimized and that any security incidents can be effectively responded to.

The ISMS of CAST covers and addresses following topics:

- Access control policy,
- Asset and Configurations management,
- Change management,
- Cryptography management,
- Data Leakage Prevention,
- Disaster recovery and Business continuity,
- Incident and Nonconformity management,
- Information Security and Information Security for computing,
- Monitoring and Logging management,
- Physical Security Management,
- Privacy Management,
- Network management,
- Threat Intelligence and Vulnerability management,
- …

Risk Management is an ongoing process inspired from the guidelines provided in ISO/IEC 27005.

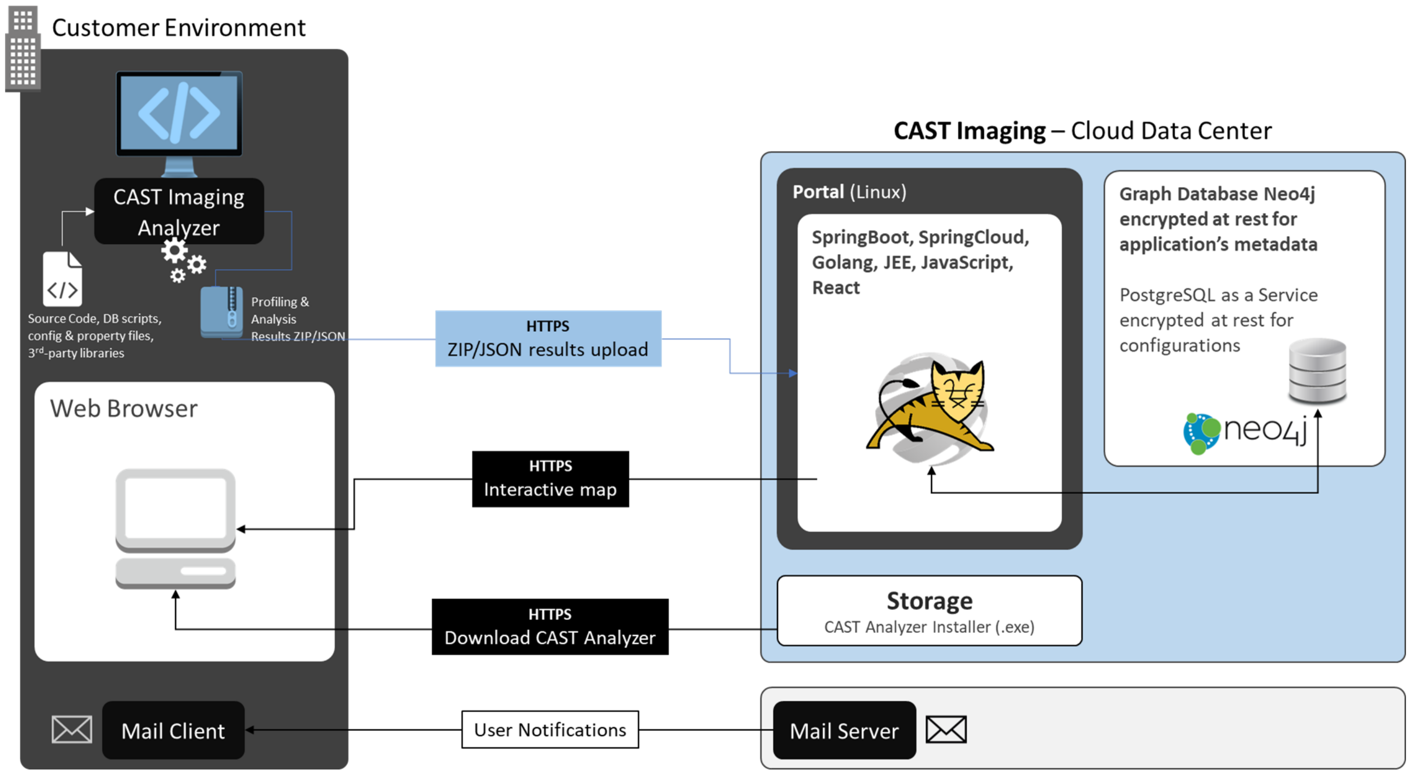
A Risk Assessment is done each year before the Internal audit or after each change considered as major in the context of the organization.



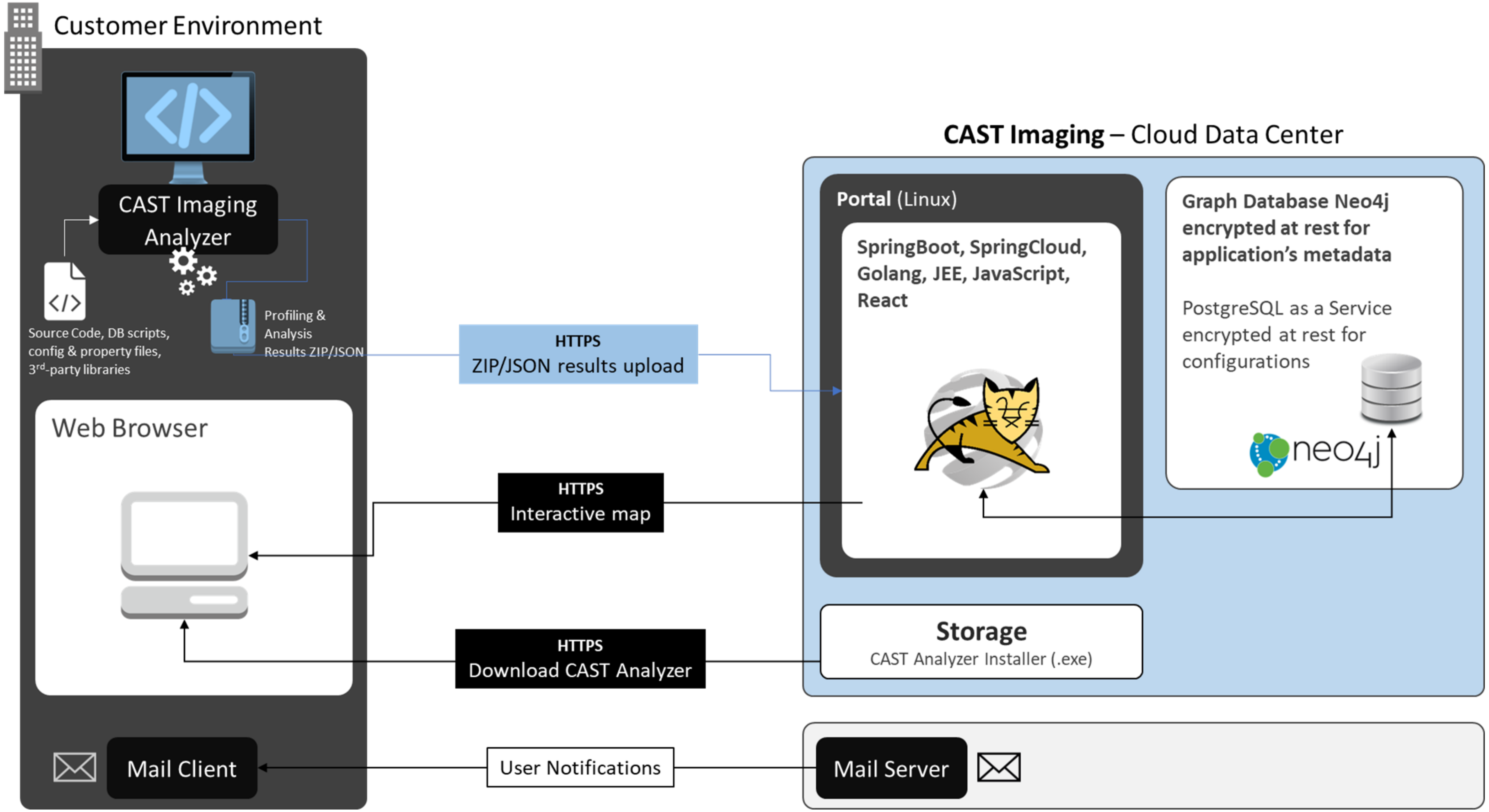
- Validation and tracking changes
- Executive endorsement
- Information security policy management
    - Roles and responsibilities
    - Review of the Information Security Policy
- Information Security policy
    - Intended outcomes of the Information Security Management System
    - Information security objectives
    - Management commitment
    - Communication and awareness session
    - Organization for Security Risk management
- Organizational controls
    - Information security roles and responsibilities and segregation of duties
    - Contacts with authorities and special interest groups
    - Threat intelligence
    - Security in project management
    - Asset management
    - Information classification, labelling and transfer
    - Access control
    - Suppliers relationships
    - Information security for use of Cloud services
        - Infrastructure
        - Responsibilities
        - User provisioning
    - Incident management
    - Business continuity
    - Legal and contractual requirements
    - Review and compliance
    - Documented operating procedures
- People controls
    - Prior to employment
    - During employment
    - Termination and change of employment
    - Confidentiality or non-disclosure agreements
    - Remote working
    - Information security event reporting
- Physical controls
- Technological controls
    - End point and mobile devices
    - Information access security
    - Capacity management
    - Protection against malware
    - Configuration management
    - Information deletion
    - Data protection
    - Backup
    - Redundancy of information processing facilities
    - Logging and monitoring
    - Software installation
    - Network security and web filtering
    - Cryptography
    - Development
    - Change management
    - Information systems audit considerations

CAST Imaging Express Architecture Security

- Your source code never leaves your infrastructure nor control: CAST Imaging Express Analyzer, which runs on your machine behind your firewall uses source code as input and generates JSON files which are zipped in a .casticr file.
- CAST Imaging Express Analyzer operates in two modes: Connected and Offline. In Connected mode, it dynamically downloads extensions during analysis and automatically uploads .casticr file to the Data Center. Offline mode installs all extensions by default on your infrastructure and requires manual uploading of .casticr file.
- CASTICR file is securely transmitted over HTTPS link (TLS 1.2 and above) for processing and secure storage (AES-256-GCM) in the .
- CAST Imaging Express supports role-based access to ensure data segregation.
- Front, website and database are segregated in distinct networks whose access are restricted to required flows.
- Authentication can be delegated to your IDP (SSO) through the support of SAML2 or OpenID Connect
- User provisioning is managed by the individual designated by you as the administrator.
- Access to the platform by CAST for administration purpose is done through a VDI and multi-factor authentication.


Customer Environment
CAST Imaging Analyzer
Source Code, DB scripts, config & property files, 3rd-party libraries
Profiling & Analysis Results ZIP/JSON
Web Browser
Mail Client
HTTPS
ZIP/JSON results upload
HTTPS
Interactive map
HTTPS
Download CAST Analyzer
User Notifications
CAST Imaging – Cloud Data Center
Portal (Linux)
SpringBoot, SpringCloud, Golang, JEE, JavaScript, React
Graph Database Neo4j encrypted at rest for application's metadata
PostgreSQL as a Service encrypted at rest for configurations
neo4j
Storage
CAST Analyzer Installer (.exe)
Mail Server

CAST Imaging Express Architecture Diagram


Customer Environment
CAST Imaging Analyzer
Source Code, DB scripts, config & property files, 3rd-party libraries
Profiling & Analysis Results ZIP/JSON
Web Browser
Mail Client
HTTPS
ZIP/JSON results upload
HTTPS
Interactive map
HTTPS
Download CAST Analyzer
User Notifications
CAST Imaging – Cloud Data Center
Portal (Linux)
SpringBoot, SpringCloud, Golang, JEE, JavaScript, React
Graph Database Neo4j encrypted at rest for application's metadata
PostgreSQL as a Service encrypted at rest for configurations
neo4j
Storage
CAST Analyzer Installer (.exe)
Mail Server

CAST Imaging Express Analyzer Outputs

You execute CAST Imaging Express Analyzer in your environment/on your machine. It uses source code, DB scripts, 3rd-party libraries, configuration files, property files as inputs, and generates JSON files.

JSON files are text files that can be opened with any text editor so they can be audited by Security or Compliance officer. No source code is embedded in CAST Imaging JSON files.

Those JSON files are not encrypted and can be read and reviewed by anybody.

Those JSON files contain only metrics (numbers relevant to CAST Imaging Express) and the scanned source filenames.

Client can anonymize the source filenames if needed.

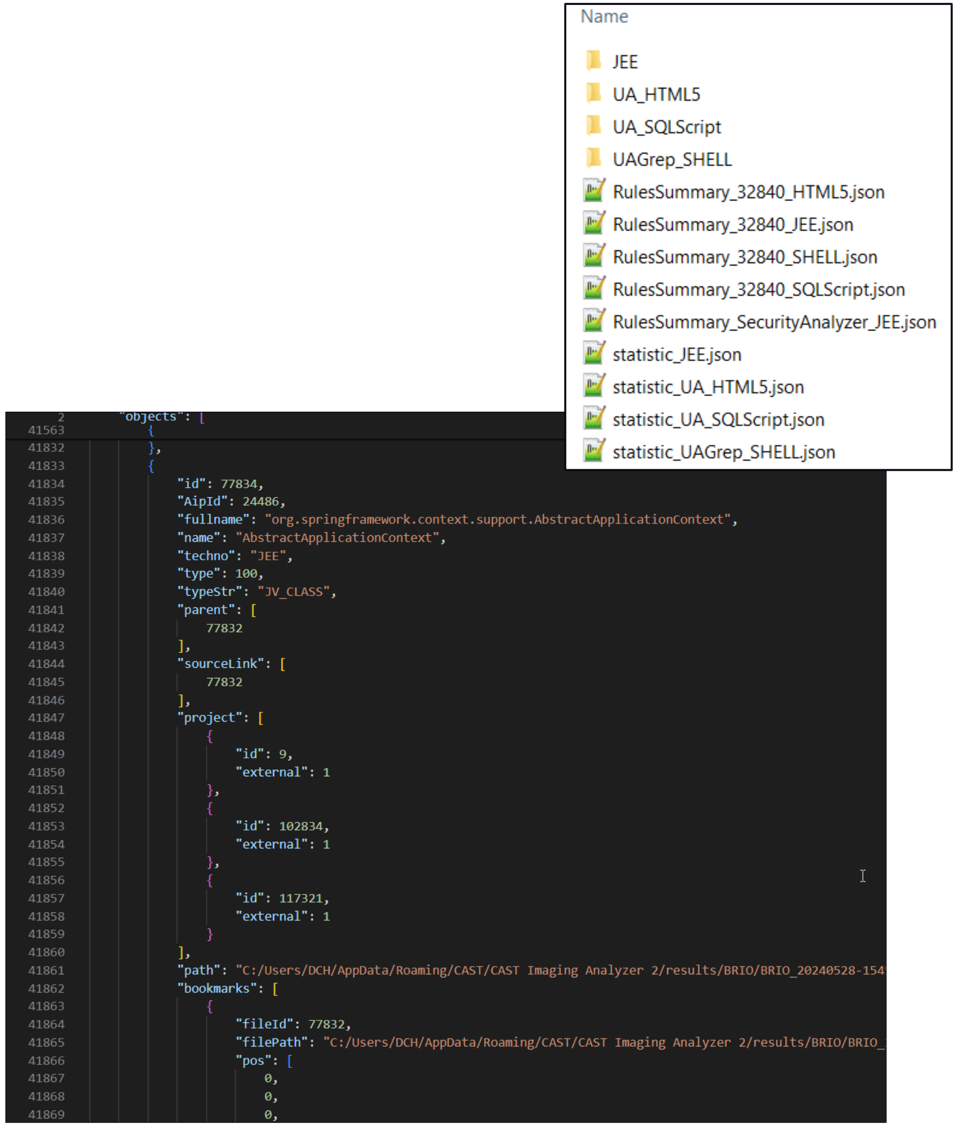
Those JSON files are transmitted to the CAST Imaging Express platform through HTTPS, which is an encrypted protocol using a 256-bit encryption mechanism. File transfer occurs either automatically or manually, depending on which analyzer is used..

All json file are zipped into a .casticr file which can be unzipped (eg: using 7-zip)

The casticr file name and the JSON file names are anonymous by default:

- ImagingResult.05_07_2020_09_22.casticr
- Cf. screenshot of the right for the csv file names

In the CAST Imaging Express platform, the client's name and the application names can also be anonymized if needed.



Name

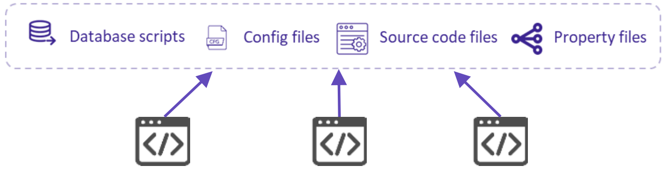
- JEE
- UA_HTML5
- UA_SQLScript
- UAGrep_SHELL
- RulesSummary_32840_HTML5.json
- RulesSummary_32840_JEE.json
- RulesSummary_32840_SHELL.json
- RulesSummary_32840_SQLScript.json
- RulesSummary_SecurityAnalyzer_JEE.json
- statistic_JEE.json
- statistic_UA_HTML5.json
- statistic_UA_SQLScript.json
- statistic_UAGrep_SHELL.json

```
    "objects": [
        {
        },
        {
            "id": 77834,
            "AipId": 24486,
            "fullname": "org.springframework.context.support.AbstractApplicationContext",
            "name": "AbstractApplicationContext",
            "techno": "JEE",
            "type": 100,
            "typeStr": "JV_CLASS",
            "parent": [
                77832
            ],
            "sourceLink": [
                77832
            ],
            "project": [
                {
                    "id": 9,
                    "external": 1
                },
                {
                    "id": 102834,
                    "external": 1
                },
                {
                    "id": 117321,
                    "external": 1
                }
            ],
            "path": "C:/Users/DCH/AppData/Roaming/CAST/CAST Imaging Analyzer 2/results/BRIO/BRIO_20240528-154
            "bookmarks": [
                {
                    "fileId": 77832,
                    "filePath": "C:/Users/DCH/AppData/Roaming/CAST/CAST Imaging Analyzer 2/results/BRIO/BRIO_
                    "pos": [
                        0,
                        0,
                        0,
```

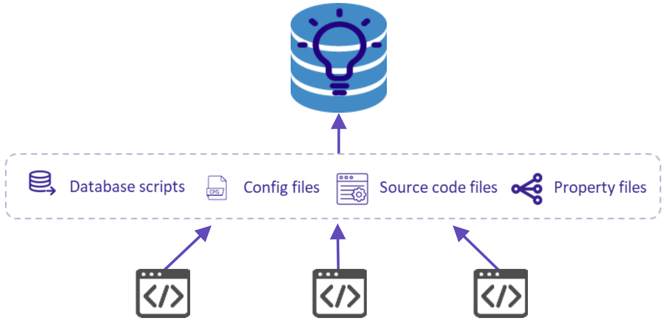
CAST Imaging Express Operating Model

Simple 3 Step Process – Rapid to implement, easy to use and scale, based on facts

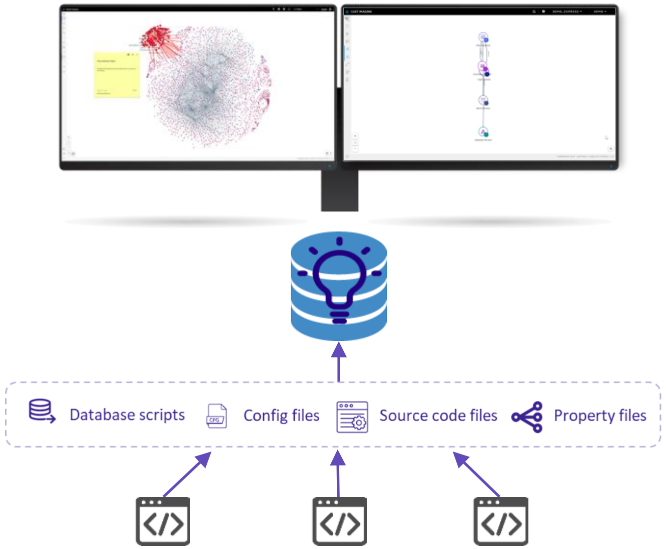
3-step process to set up and automate the living knowledge base of your software asset



Step 1 – Gather all artifacts that make up the application. Later on, automate the artifact extraction.



Step 2 – CAST Imaging generates automatically the knowledge base of your software inner workings.



Step 3 – Everyone can navigate the intelligence via interactive maps and collaborate in context.

CAST Imaging Express Analyzer Requirements

What are the hardware/software requirements to scan my source code with CAST Imaging Express Analyzer?

- Microsoft Windows Operating System superior or equal to Windows 10
- Chrome (highly recommended for better experience), Microsoft Edge, FireFox ESR
- 1.3 GB free disk space (for installation), 4GB memory (for execution)
- Source code is available and stored in text files accessible from local machine

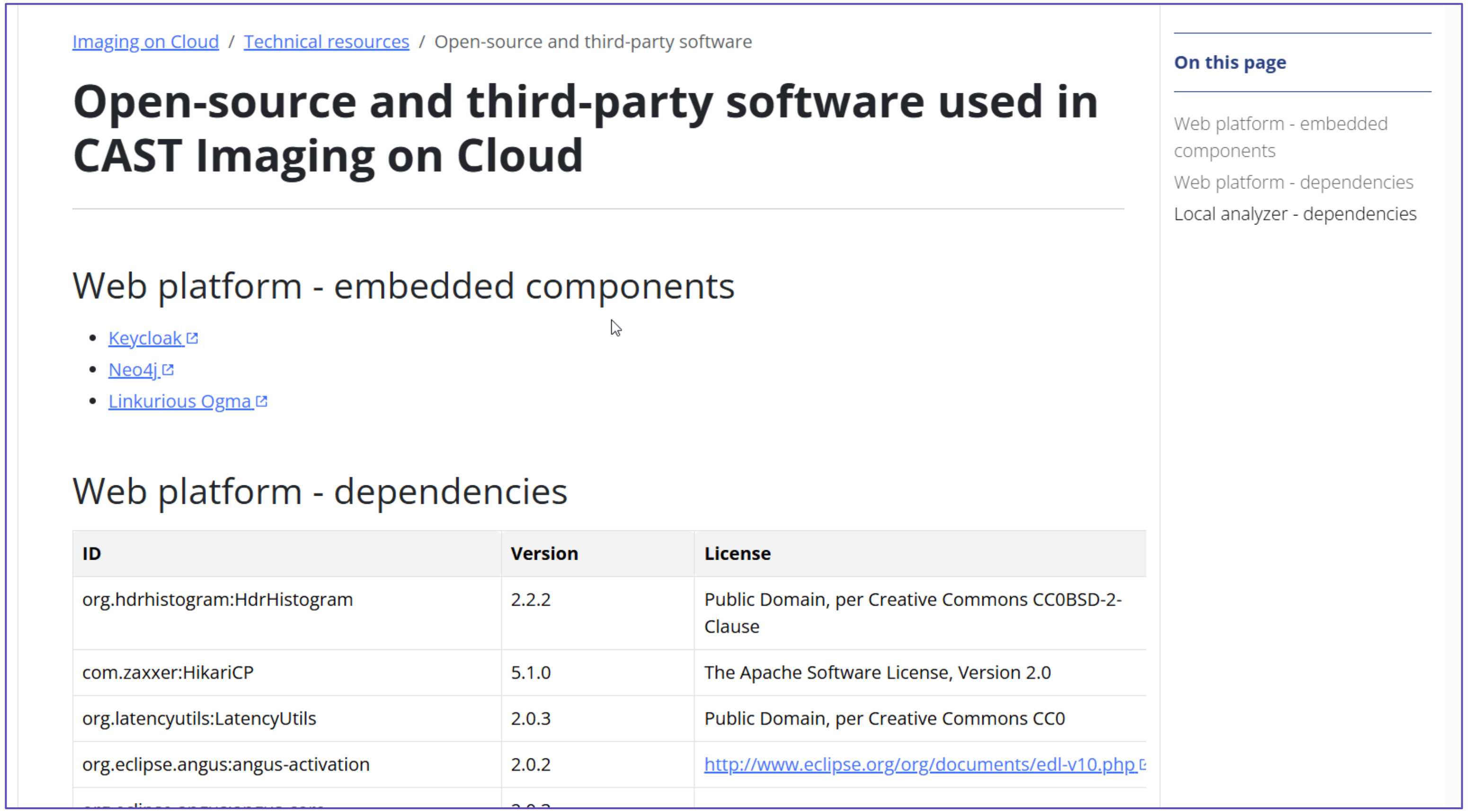
What are the hardware/software requirements to scan my source code with the CLI?

- Microsoft Windows Operating System superior or equal to Windows 10
- Microsoft Windows Server superior or equal to 2019
- More details online

Open-source and third-party software used in CAST Imaging Express

The documentation documents and makes accessible all dependencies components used in the web platform or the local analyzer.

[Documentation link]



Imaging on Cloud / Technical resources / Open-source and third-party software

Open-source and third-party software used in CAST Imaging on Cloud

On this page

Web platform - embedded components

Web platform - dependencies

Local analyzer - dependencies

Web platform - embedded components

- Keycloak
- Neo4j
- Linkurious Ogma

Web platform - dependencies

ID	Version	License
org.hdrhistogram:HdrHistogram	2.2.2	Public Domain, per Creative Commons CC0BSD-2-Clause
com.zaxxer:HikariCP	5.1.0	The Apache Software License, Version 2.0
org.latencyutils:LatencyUtils	2.0.3	Public Domain, per Creative Commons CC0
org.eclipse.angus:angus-activation	2.0.2	http://www.eclipse.org/org/documents/edl-v10.php
org.eclipse.angus:angus-core	2.0.2	