

# CAST Imaging on Cloud

## Security summary

CAST provides secure cloud-based technology used by companies with strict security requirements (Gov / BFSI / Utilities)



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



Since then, the certification has been extended:

- ISO 27017: Information security controls for Cloud services
  - Since 2019. Latest certificate date: April 26<sup>th</sup>, 2022 by Bureau Veritas
- ISO 27018: Protection of personally identifiable information (PII) in public clouds
  - Since 2019. Latest certificate date: April 26<sup>th</sup>, 2022 by Bureau Veritas
- ISO 27701: Privacy Information Management requirements and guideline
  - Since 2023. Latest certificate date: April 5<sup>th</sup>, 2023 by Bureau Veritas



# Audit – Penetration Testing

Software and services are regularly assessed

- Yearly penetration test by third party specialists since 2014

Campusguard Redlens 2025

*"Overall, RedLens feels that the CAST Imaging – Cloud 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"*

Agio 2023

*"The overall results of the web application penetration test show that CAST has a well-maintained web application that shows strong coding practices and sound testing environments. Overall, Agio rates this environment as strong, secure, and well maintained; all components are up to date, and there are no security concerns at this time following the successful remediations."*

Appsec consulting 2019

*"Based on this assessment, AppSec Consulting believes that CAST has adequate controls in place within the Highlight application to protect the security of customer information. CAST was able to quickly and effectively remediate the findings that were identified in the initial security assessment report. "*

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

CAST



# 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 Cloud computing,
- Monitoring and Logging management,
- Physical Security Management,
- Privacy Management,
- Network management,
- Threat Intelligence and Vulnerability management,
- ...

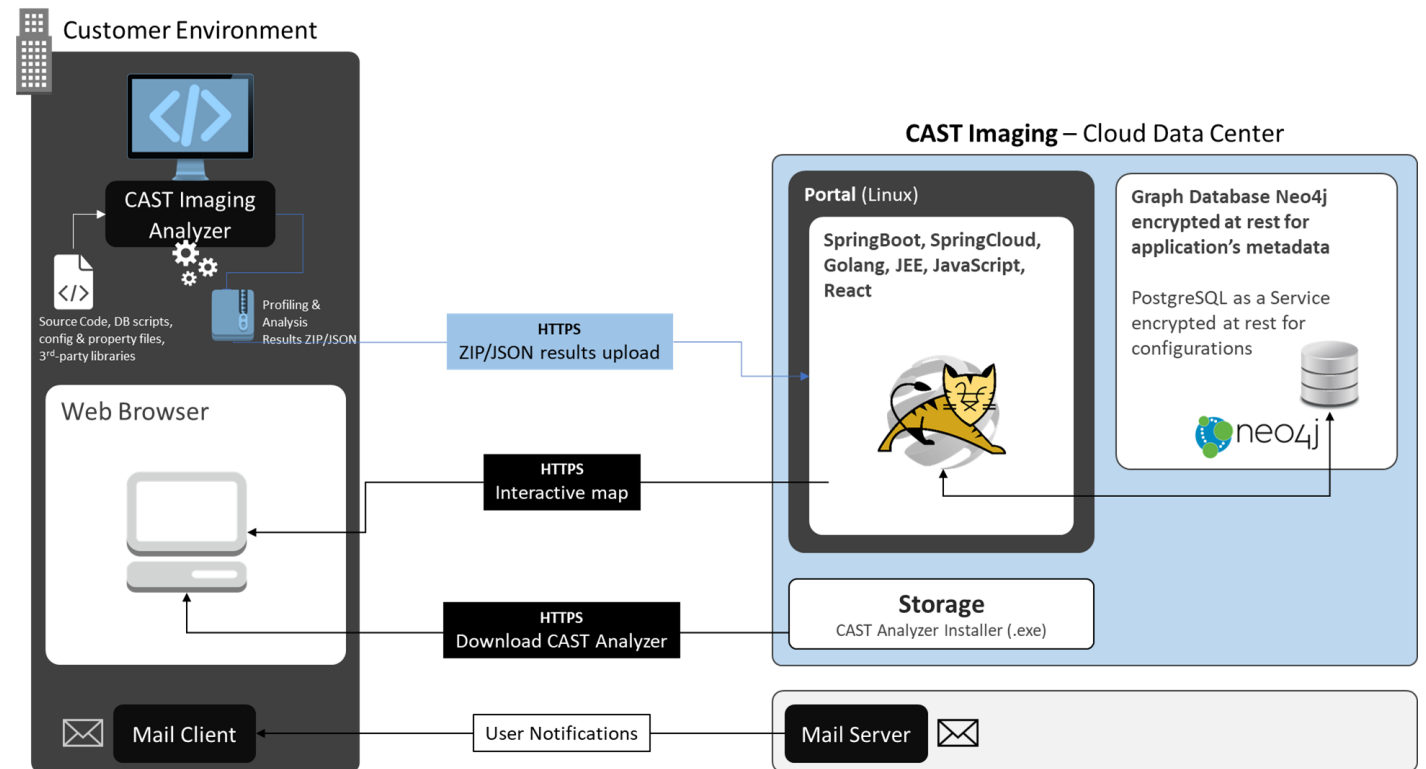
Risk Management is an ongoing process inspired from the guidelines provided in ISO/IEC 27005.

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

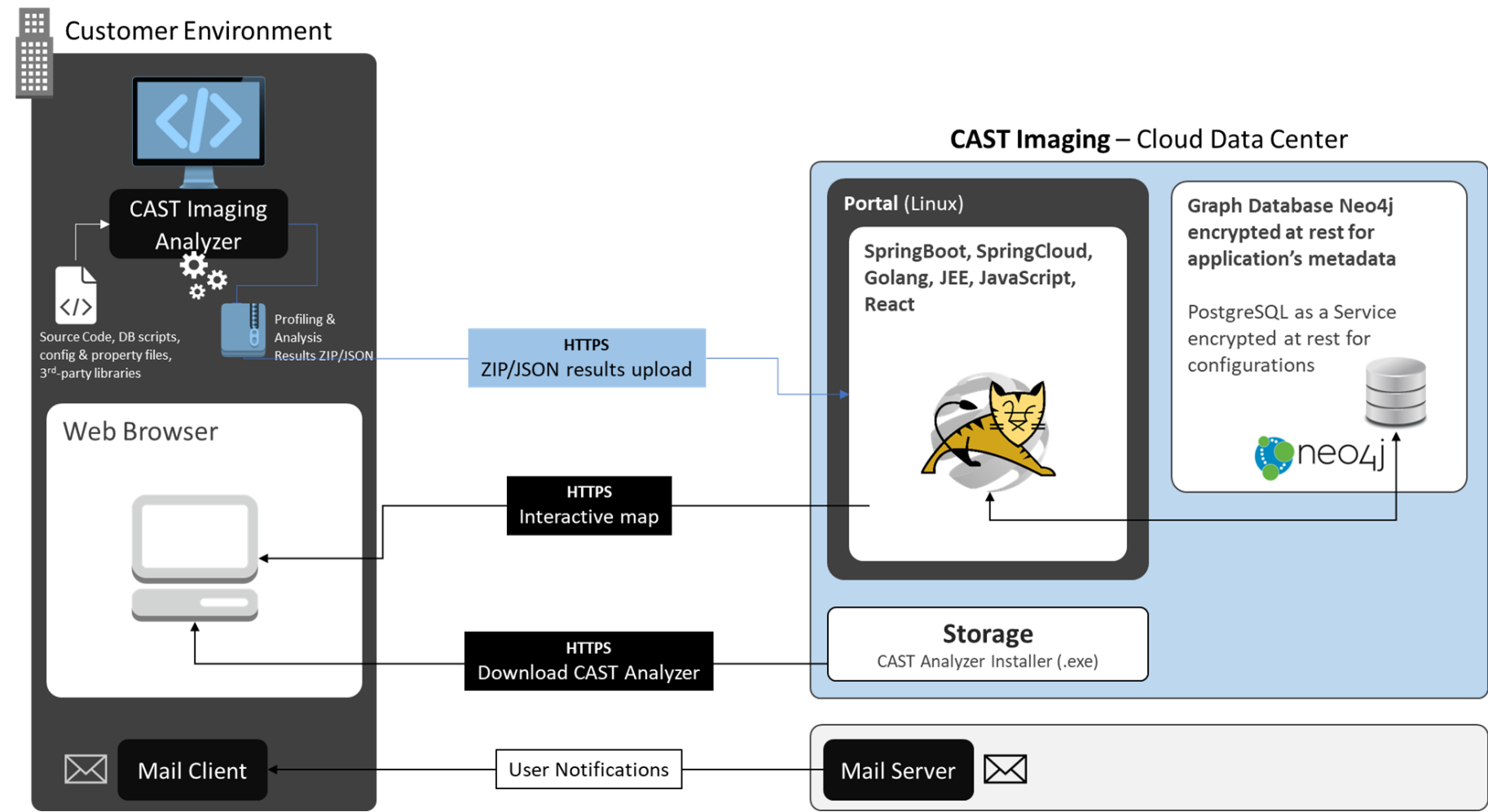
- Validation and tracking changes
- Executive endorsement
- Information security policy management
  - Roles and responsibilities
  - Review of the Information Security Policy
- Information Security policy
  - Intended outcomes of the Information Security Management System
  - Information security objectives
  - 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 on Cloud Architecture Security

- Your source code never leaves your infrastructure nor control: CAST Imaging Analyzer, which runs on your machine behind your firewall uses source code as input and generates JSON files.
- JSON files are securely transmitted over HTTPS link (TLS 1.2 and above) for processing and secure storage (AES-256-GCM) in the cloud.
- CAST Imaging 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.
- 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.



# CAST Imaging on Cloud Architecture Diagram



# CAST Imaging Analyzer Outputs

You execute CAST Imaging Analyzer in your environment/on your machine. It uses source code, DB scripts, 3<sup>rd</sup>-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 on Cloud) and the scanned source filenames.

Client can anonymize the source filenames if needed.

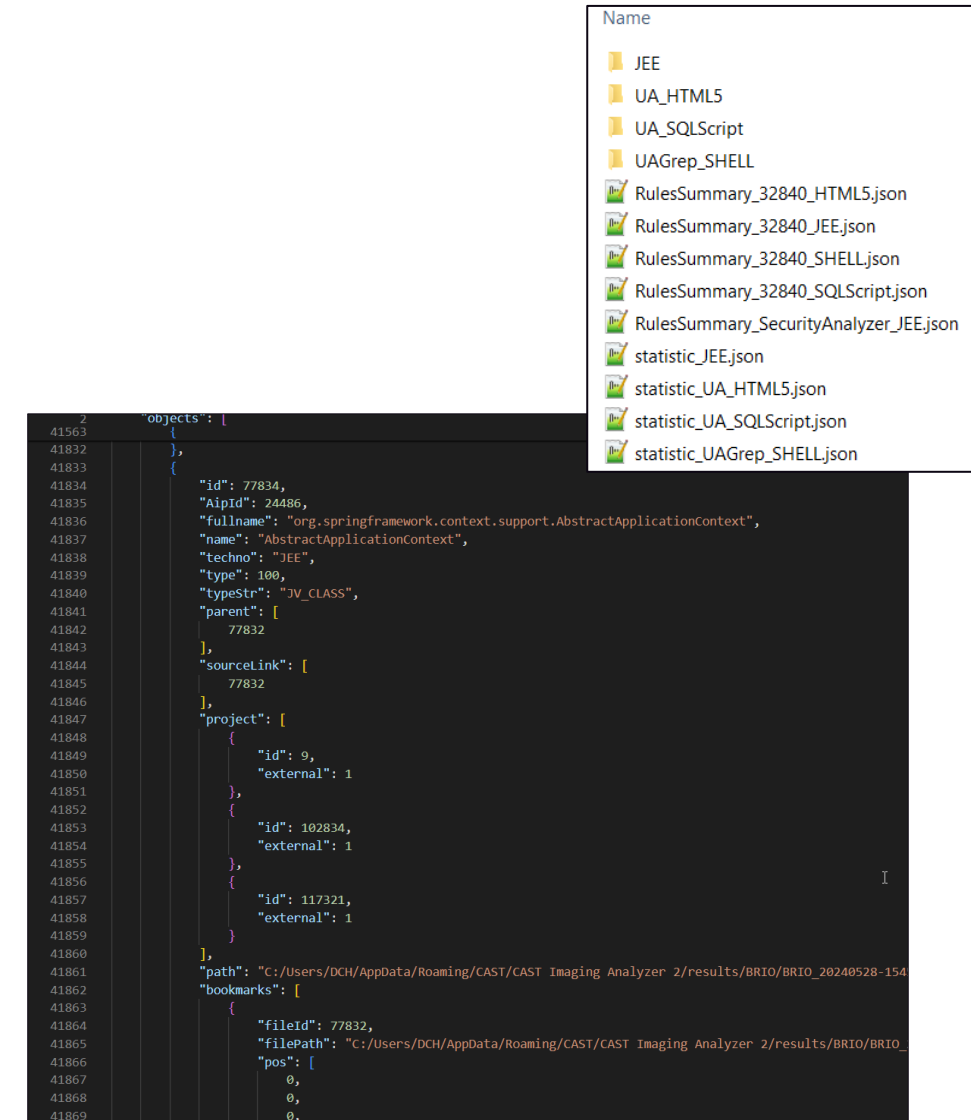
Those JSON files are transmitted to the CAST Imaging on Cloud platform through HTTPS, which is an encrypted protocol using a 256-bit encryption mechanism.

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 on Cloud platform, the client's name and the application names can also be anonymized if needed.



The screenshot displays a JSON file viewer interface. On the right side, a list of files is shown under the heading 'Name'. The files include folders for 'JEE', 'UA\_HTML5', 'UA\_SQLScript', and 'UAGrep\_SHELL', followed by various 'RulesSummary' and 'statistic' JSON files for each category. On the left side, a detailed JSON object is displayed, showing metadata for a specific application context (AbstractApplicationContext) and its associated project details, including IDs, parent links, and file paths.

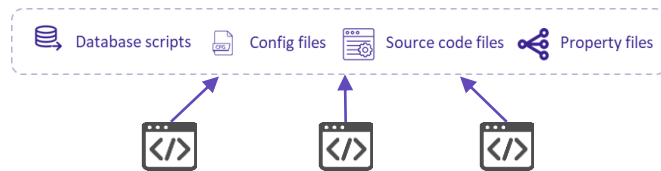
```
41563 {
41832 },
41833 {
41834   "id": 77834,
41835   "AipId": 24486,
41836   "fullname": "org.springframework.context.support.AbstractApplicationContext",
41837   "name": "AbstractApplicationContext",
41838   "techno": "JEE",
41839   "type": 100,
41840   "typeStr": "JV_CLASS",
41841   "parent": [
41842     77832
41843   ],
41844   "sourceLink": [
41845     77832
41846   ],
41847   "project": [
41848     {
41849       "id": 9,
41850       "external": 1
41851     },
41852     {
41853       "id": 102834,
41854       "external": 1
41855     },
41856     {
41857       "id": 117321,
41858       "external": 1
41859     }
41860   ],
41861   "path": "C:/Users/DCH/AppData/Roaming/CAST/CAST Imaging Analyzer 2/results/BRIO/BRIO_20240528-154",
41862   "bookmarks": [
41863     {
41864       "fileId": 77832,
41865       "filePath": "C:/Users/DCH/AppData/Roaming/CAST/CAST Imaging Analyzer 2/results/BRIO/BRIO_20240528-154",
41866       "pos": [
41867         0,
41868         0,
41869         0
41870       ]
41871     }
41872   ]
41873 }
```



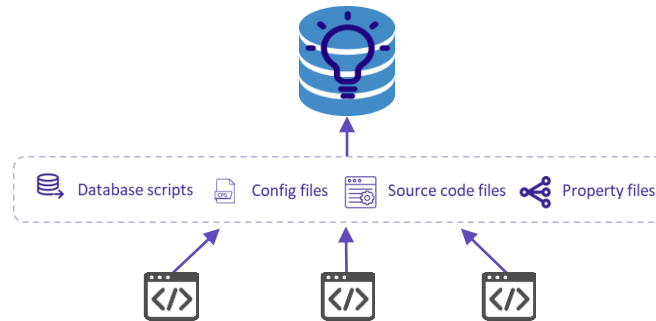
# CAST Imaging Operating Model

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

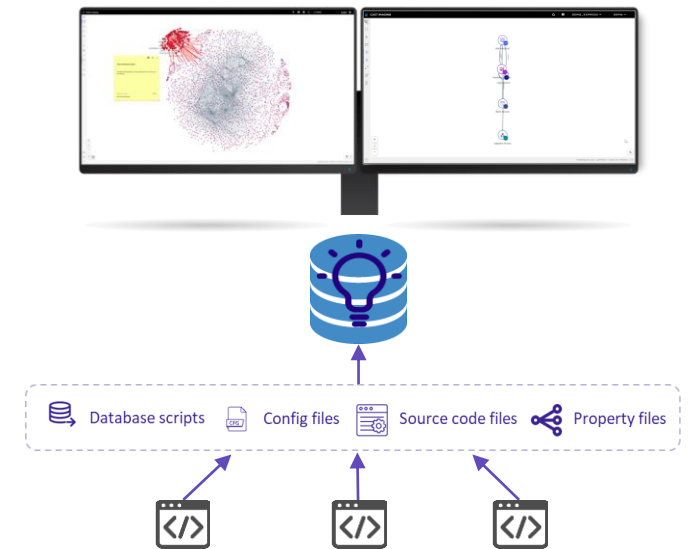
3-step process to set up and automate the living knowledge base of your software asset



**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 Analyzer Requirements

**What are the hardware/software requirements to scan my source code with CAST Imaging 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 on Cloud

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

Web platform - embedded components

- [Keycloak](#)
- [Neo4j](#)
- [Linkurious Ogmia](#)

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	<a href="http://www.eclipse.org/org/documents/edl-v10.php">http://www.eclipse.org/org/documents/edl-v10.php</a>

On this page

Web platform - embedded components

Web platform - dependencies

Local analyzer - dependencies