CAST
Software Intelligence for Digital Leaders

CAST Highlight – Security Summary

June 2024

A secure technology used by companies with strict security requirements (Gov / BFSI / Utilities)

And many others...

ISO 27001, 27017, 27018 and 27701 Certifications

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

- Executive and Product Management
- Development and **Quality Assurance**
- **Release management**
- Operating and Facilities management

The certification has been extended :

- 2019
  - ISO 27017: Information security controls for Cloud services
  - ISO 27018: Protection of personally identifiable information (PII) in public clouds
- **2023**
  - ISO 27701: Privacy Information Management requirements and guidelines

The latest certificate was delivered by Bureau Veritas on:

- April 30th, 2024 for ISO 27001,
- April 26th, 2022 for ISO 27107 and ISO 27018,
- April 5th, 2023 for ISO 27701.

Audit – Penetration Testing

Software and services are regularly assessed

- Yearly penetration test by third party specialists since 2014

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. No known issues remain with the application or supporting infrastructure that would allow an attacker to compromise CAST's customer accounts or the application's supporting infrastructure. "*

AGIO 2021

"*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.*"

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

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 management,
- Change management,
- Cryptography management,
- Disaster recovery and Business continuity,
- Incident and Nonconformity management,
- Monitoring policy,
- Physical Management,
- Network management,
- Vulnerability management,
- ...

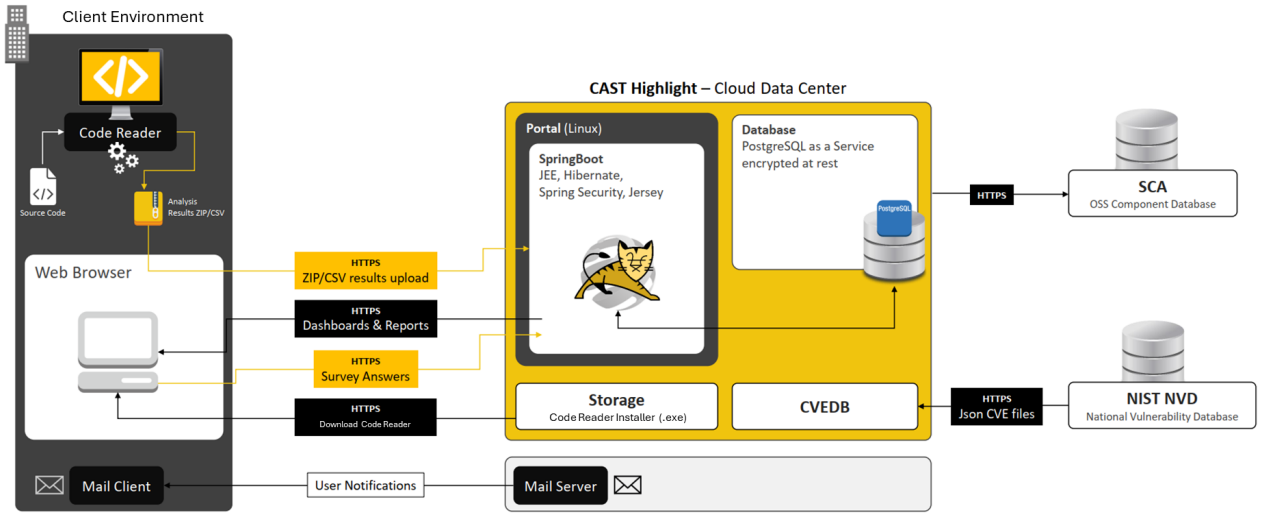
Risk Management is an ongoing process inspired from the guidelines provided in ISO/IEC 27005.

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

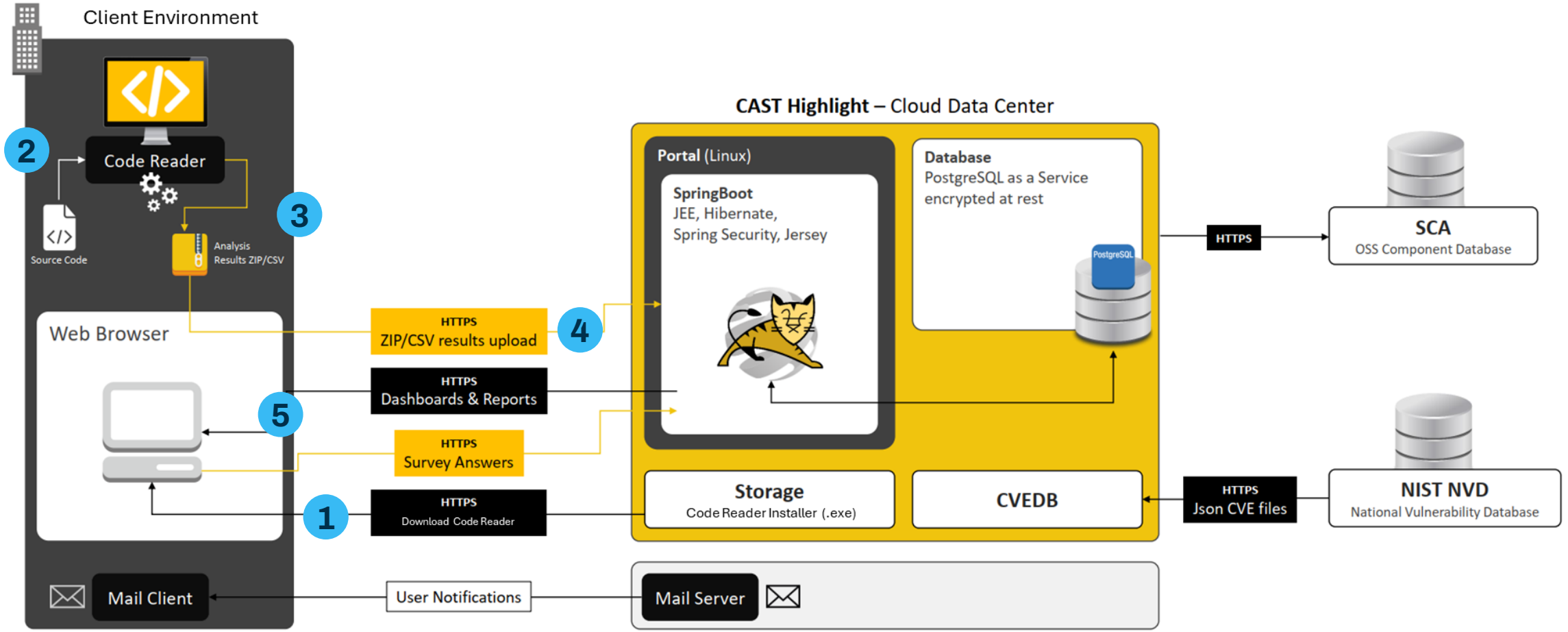
- Validation and tracking changes
- Executive endorsement
- Information security policy management
  - Roles and responsibilities
  - Review of the Information Security Policy
- Information Security policy
  - Information security objectives
  - Management commitment
  - Communication and awareness session
  - Organization for Risk Management
- Organization of information security
  - Information security roles and responsibilities and segregation of duties
  - Membership in associations
  - Security in project management
  - Mobile devices and teleworking
- Human resource security
  - Prior to employment
  - During employment
  - Termination and change of employment
- Asset Management
  - Responsibility for assets
  - Information classification
  - Media handling
- Access control
  - Business requirements of access control
  - User access management
  - User responsibilities
  - System and application access control
- Cryptography
- Physical and environmental security
  - Secure areas
  - Equipment
- Operations security
  - Operational procedures and responsibilities
  - Protection from malware
  - Backup
  - Logging and monitoring
  - Control of operational software
  - Technical vulnerability management
  - Information systems audit considerations
- Cloud services
  - Infrastructure
  - Responsibilities
  - User provisioning
- Communications security
  - Network security management
  - Information transfer
- System acquisition, development and maintenance
  - System requirements of information systems
  - Security in development and support processes and tests data
- Supplier relationships
  - Information security in supplier relationships and supplier service delivery management
- Information Security Incident Management
- Information security aspects of Business Continuity Management
- Compliance
  - Compliance with legal and contractual requirements
  - Information security review

CAST Highlight Architecture Security

- Your source code never leaves your infrastructure. The CAST Highlight Code Reader generates csv files on your computers
- Data is encrypted in transit (tls 1.2 and above) and at rest (AES-512)
- CAST Highlight supports role-based access to ensure data segregation
- Front, website and database are segregated in distinct networks which 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 portfolio administrator
- Access to the platform by CAST for administration purpose is done through a VDI and multi-factor authentication



CAST Highlight Architecture Diagram



CAST Highlight Code Reader Outputs

CAST Highlight Code Reader generates csv files (executed on your computers – the source code never leaves your infrastructure)

CSV 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 Highlight CSV files.

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

Those CSV files contain only metrics (numbers relevant to CAST Highlight measurement model) and the scanned source filenames.

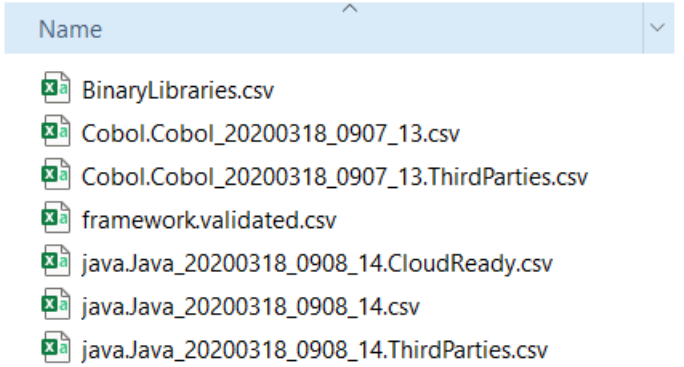
Client can anonymize the source filenames if needed.

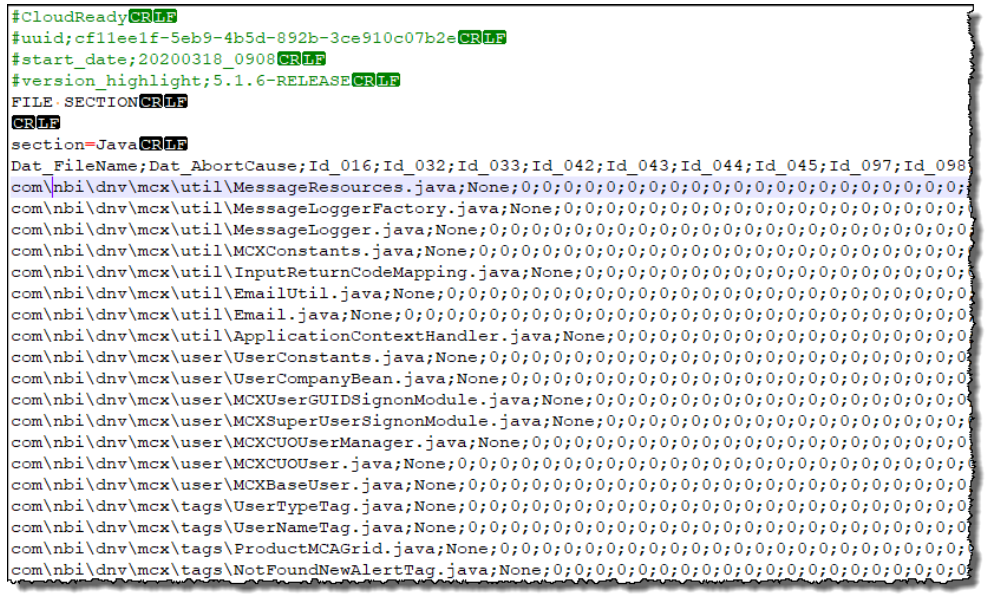
Those CSV files are transmitted to the CAST Highlight platform through HTTPS, which is an encrypted protocol using a 256-bit encryption mechanism.

The zip file name and the csv file names are anonymous by default:

- HighlightResult.05_07_2020_09_22.zip
- Cf. screenshot of the right for the csv file names

In the CAST Highlight platform, the client name and the application names can also be anonymized if needed.





CAST Highlight Operating Model

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

Step 1 – Automatically scan source code repositories, 100s of applications per week, updated continuously and automatically

Step 2 – Encrypted statistical results uploaded to secure cloud (27001-certified), no code leaves the premises

Step 3 – Instant visibility with automatically generated and customizable dashboards, heat maps, charts; actionable recommendations; integrate data with other systems via API

CAST Highlight – Local Code Reader Requirements

What are the hardware/software requirements to scan my source code with the Local Code Reader?

- Microsoft Windows Operating System superior or equal to Windows 8 (Linux and Mac also supported)
- Chrome (highly recommended for better experience), Microsoft Edge, FireFox ESR
- Local Code Reader Install/Scan: 300MB free disk space, 4GB memory
- 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?

- Java 11 or above
- Perl 5 (tested on Strawberry 5.12.3.0)
- libjson-perl, libxml-libxml-perl
- More details online

Thank You

CAST

Software Intelligence for Digital Leaders

castsoftware.com

How to ensure rapid adoption by client accounts

Infosec review

- Emphasize the fact that the source code never leaves the client environment
- Reference the ISO 27001 certification (CAST Highlight certified since 2015)
- Use the CAST Highlight Security FAQ and the supporting documentation in the following slides (security certificates, slides detailing platform architecture, etc.)

Integrate into existing CI/CD processes

- Leverage existing pipelines to limit effort
- Use a weekly or sprint-level cadence (no need for more)
- Use the existing integrations: Azure DevOps, Atlassian BitBucket, Github Actions, Docker scanner, Command line scanner
- Use the REST API to extract scan results automatically