SISENSE

SISENSE SECURITY OVERVIEW

September 2016

Introduction

Security is a critical component of all information technology, but is especially important for Business Intelligence solutions. BI solutions are commonly used to view highly sensitive information like company finances, payroll, sales data, even personally identifiable information. When a BI application stores or accesses such sensitive data, it is critical that only the right users can see the right information. Sisense prioritizes data security in our product development and support processes to make sure that organizations can always safely deploy and manage the solution.

Organizations often struggle with a tradeoff between security and the complexity of implementation and maintenance. Sisense addresses this challenge with a combination of robust security built into the product and customization options that make it easy to fit an organization's unique security needs. Sisense's out of the box security functionality helps organizations deploy quickly in accordance with their best practices. Built from the ground up with an API framework, Sisense also provides programmatic access to all security functions in order to reduce or eliminate the complexity of customization. This helps businesses easily scale their own security policies across users and data.

Sisense's approach to security encompasses four main categories:

- **Process level security:** the procedures, tests and controls used to ensure the highest levels of data security.
- **System level security:** user management, authentication and permissioning for the entire Sisense application.
- **Object level security:** the features provided for controlling access to different solution components.
- **Data level security:** features relating to granular control over exactly what data within the data source(s) is viewable by certain users.

Process Level	System Level	Object Level	Data Level
• SDLC • OWASP • Regular Audits and Penetration Tests	• User and Group Management • SSO • Active Directory • REST API	• ElastiCube Access • Dashboard Access	• Row Based Security • Row Level Defaults

Process Level Security

Sisense adheres to industry standard security practices to ensure that high levels of security discipline are followed throughout our development and support processes, so that organizations can easily implement and manage the solution safely.

The main security standards we follow are:

- The Secure Development Life Cycle (SDLC) methodology with full security reviews.
- The DREAD methodology for classifying system vulnerabilities.
- Annual security audit and penetration test, performed by an external review company following the OWASP Testing Guide V4 for product security testing.

The Sisense solution is tested regularly in accordance with the OWASP Testing Guide V4 industry standard including the following domains:

- Information Gathering
- Configuration and Deployment Management Testing
- Identity Management Testing
- Authentication Testing
- Authorization Testing
- Session Management Testing
- Input Validation Testing
- Error Handling
- Cryptography

- Business Logic Testing
- Client Side Testing

Sisense takes all security issues seriously and quickly responds to all verifiable problems. Following the audit process, Sisense addresses all high risk vulnerabilities in the next release and medium risk vulnerabilities within two quarters.

System Level Security

System-level security encompasses role-based access options. This includes user and server management, connection to an active directory, Single Sign-On (SSO), and the security REST API.

User and Group Management

Organizations can assign one of three primary roles to Sisense users or groups:

- Viewers: Can access and view dashboards
- Designers: Can create and edit dashboards
- Administrators: Can create users and user groups, set up Active Directory, and more.

ElastiCube Server Access Rights

Organizations can assign access rights to different ElastiCube servers for individual users, groups or to everyone.

Active Directory

An organization's Active Directory can be leveraged to reduce deployment time by applying existing security policies and sharing properties to the Sisense application.

Single Sign-On (SSO)

SSO facilitates seamless integration between Sisense and other systems while offering standardization of authentication policies.

REST API

The REST API provides the ability to automate and customize system security settings to fit a particular environment and security policies. The API can be used to integrate and automate restrictions and access control based on rules and standards, as well as to specify access rights and security to dashboards, ElastiCubes and data. The API can also be used in user management to create, edit and assign new users or groups.

Encryption

The Sisense web interface fully supports encryption using standard SSL to ensure privacy and security. Sisense encryption is compliant with the Federal Information Processing Standard (FIPS).

Object Level Security

Object security defines access rights for different users and groups to various components within Sisense. The two main objects are ***Dashboards*** and ***ElastiCubes***.

Dashboards

Dashboards can be shared on either a user or group level. Admins can configure access rights for all users and define which designers may edit a Dashboard.

ElastiCubes

Access rights for different ElastiCubes can be defined on a user or group level. This provides flexibility to create ElastiCubes for specific user or group with strict access control.

Data Level Security

Sisense enables precise control of the data that users can see. With Data Level Security, a single dashboard can be shared with many users, with each viewer accessing only the data they have permission to see. This not only provides fine-grained security, but reduces development time because replicated dashboards do not need to be built or adjusted independently.

Row Level Security

User and group permissions can be set to view specific rows in the source data. For each ElastiCube, multiple rules can be applied to enforce granular access control.

Row Level Defaults

Security Defaults can be used to automate rules that make certain data accessible to specific users or groups. For example, a default can be set so that new employees can only access a restricted data set until they are added to relevant groups. This feature provides organizations a custom, scalable method of applying security across their entire user base.

Summary

Strong security is critical for enterprise software, especially with applications that store or access highly sensitive data like Business Intelligence. Sisense adheres to stringent security practices to ensure that organizations can implement our solution safely and in accordance with their unique needs. Our security outlook combines rigorous processes and regular testing with industry standard technologies like encryption, authentication and access control methods. Sisense provides deep functionality that allows organizations to secure components of the solution and their data with fine-grained detail, without compromising ease of use, time-to-market, or adding unnecessary complexity.

For more information, please reference the Sisense Security Documentation page:
https://www.sisense.com/documentation/security/

To download Sisense for a free demo, please visit:
https://www.sisense.com/demo/