SISENSE

Sisense Security Overview

Table of Contents

The information contained in this document is confidential, proprietary and only for the information of the intended recipient and may not be used, published or redistributed without the prior written consent of Sisense Ltd.

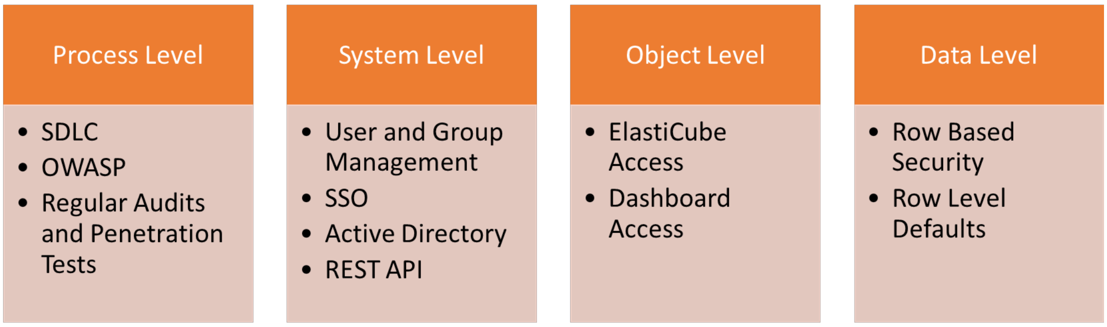
Sisense Product Security

Maintaining a high level of security is essential for all information technology projects and business data. For Business Intelligence (BI) platforms, which are commonly used to view highly sensitive information across a wide-range of users and departmental use cases, security requires paramount robustness and administrative flexibility across databases, applications, and users. This means making sure the appropriate users have access to the right data at the right depth while adhering to company security protocol. At Sisense we prioritize data security at every stage of our product development cycle and implementation processes; ensuring that security and safety are naturally integrated from deployment to scaling and software updates.

For many organizations, scaling in complexity of implementation and data can create problems with maintaining the highest level of security. Sisense addresses this challenge with a combination of robust security built directly into the product. Regardless of how the platform is used internally, Sisense's customization options make it easy to fit an organization's unique security needs and scale policies across users and data. 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.

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 permissions 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

- SDLC
- OWASP
- Regular Audits and Penetration Tests

System Level

- User and Group Management
- SSO
- Active Directory
- REST API

Object Level

- ElastiCube Access
- Dashboard Access

Data Level

- Row Based Security
- Row Level Defaults

Process Level Security

Sisense adheres to industry standard security practices to ensure the highest level of security discipline is followed throughout our development, implementation and support processes. Sisense is architected for organizations to easily implement and manage their BI 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 independent 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 promptly 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. Sisense can integrate with either SAML 2.0 or JWT based SSO.

REST API

The REST API provides the ability to automate and customize system security settings to fit environmental needs and security policies. It can be used to create, edit, and assign users or groups as well as to integrate and automate restrictions and control access based on rules and standards. The REST API can also be used to specify access rights and security for external applications, dashboards, ElastiCubes and data.

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 140-2).

Sisense encrypts sensitive information such as account credentials and authorization profiles for Sisense and for data source connections before writing to disk. Sisense uses the following encryption algorithms: SHA-256& AES-256.

Operating System based disk encryption, Windows file system encryption - Transparent Data Encryption (TDE), can be used for encrypting data at rest. When using Windows transparent encryption, the key pair (private/public) is bound to the user identity.

Data imported into and retrieved from Sisense can also be encrypted. For data import into Sisense, the import protocol depends on the protocols supported by the data source. Sisense also supports SSL for data movement from the Sisense Web Server into the user's the web browser.

Tracking and Monitoring Data

Upon installation, Sisense collects data for internal and support related purposes such as improving customer experience and resolving technical issues. At no time is any personal information collected and all personal identifiers can be obfuscated. Additionally, tracking and monitoring of data can be turned off at any time.

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. Security for external applications, embedded analytics, and white labeled applications is managed the same way.

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. One key benefit of the ElastiCube is creating a single hub for managing data security, regardless of where the data is originally stored.

Data Level Security

Sisense enables precise control of 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 provides fine-grained security and 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.

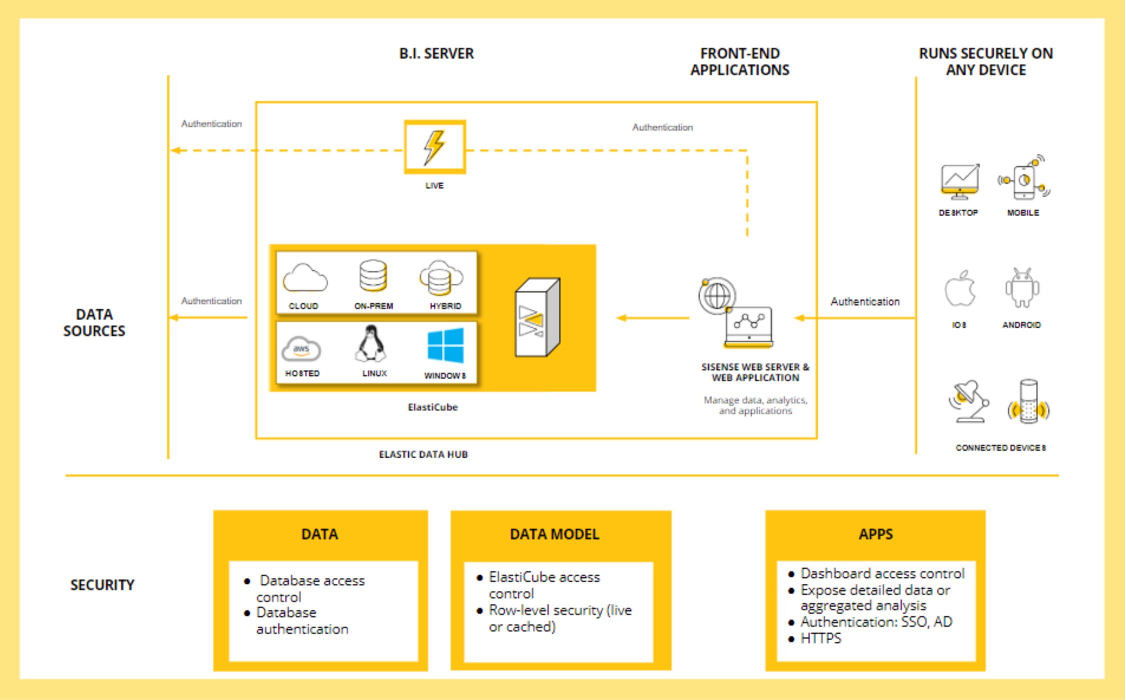
Row Level Defaults

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.

Sisense Product Security Summary

Sisense adheres to stringent security practices to ensure that organizations can implement our solution safely and in accordance with their unique security 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 their solution and data with fine-grained detail, without compromising ease of use, time-to-market, or adding unnecessary complexity.

Security Diagram



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/

Sisense Managed Cloud Security

Sisense Cloud hosts its servers on Amazon Web Services. On an infrastructure level, this enables Sisense's software to take advantage of the robust security and compliance certifications available on AWS. Sisense applies the highest standards to ensure security and compliance in-line with industry standards.

Security and Compliance

Sisense's infrastructure is hosted in AWS data centers using a network architecture built to meet the requirements of the most security-sensitive organizations. As an industry leader in Cloud Security, AWS enforces strong safeguards to protect customer privacy. All data is stored in highly secure AWS data centers. More information about AWS Security can be found at https://aws.amazon.com/security/

By tying together governance-focused, audit-friendly service features with applicable security compliance regulations or audit standards, AWS Compliance enablers build on traditional programs; they help customers establish and operate in an AWS security-controlled environment. A list of certifications and assurance programs can be found at https://aws.amazon.com/compliance/.

Amongst many other certifications, AWS is compliant to the following:

- CSA
- ISO 9001
- ISO 27001
- ISO 27017
- ISO 27018
- SOC 1
- SOC 2
- SOC 3

More certifications and accreditations to which AWS is compliant can be found at https://aws.amazon.com/compliance/programs/ .

Sisense's System Environment Secure Deployment

AWS Account

Management of the AWS Account is made available to designated IT, support, and NOC staff. Accessing the AWS account requires logging in via multifactor authentication (MFA) to ensure that only the right people can access the system with an additional something-you-have authentication method.

Sisense Server Network Security

Sisense deploys a dedicated and isolated virtual server in the AWS for each customer. Each customer's deployment is completely independent of, and does not have access to, any other Sisense customer's deployment.

Windows OS

Sisense Cloud Service keeps Windows OS up to date with the latest upgrades as well as timely installation of any Windows security patches.

Windows Hardening

Windows OS is hardened according to CIS benchmarks.

Sisense Windows Passwords

All passwords are required to meet Windows complexity requirements. Passwords must be changed on a quarterly basis for all users with access to a Sisense server.

Control Open Ports

All incoming and outgoing ports are blocked by default. There is a predefined list of ports that are open for the Sisense application, as follows:

- Incoming port for Sisense UI (HTTPS - 443)
- Incoming port for access to Sisense ElastiCube Manager (RDWeb - 8443)
- Incoming port for service restart manager – (HTTPS – 8444)
- Incoming port for file transfer (FTPS – 990)
- Outgoing ports for DB connectors

Anti-Malware

Sisense runs anti-malware software (currently Palo Alto Traps) on its cloud servers.

Restricted Access to Sisense Server

Access to Sisense server is restricted to follow directives defined for utmost security.

IP Restriction

By Sisense - access to Sisense server in the cloud, RDP, is performed via a secure VPN connection.

By customer – access to approved applications on the Sisense server in the cloud, RDWeb, is performed from designated IP’s only.

The Cloud Access IP Whitelist is maintained by the Sisense IT team.

Staff Restriction and Security Training

Access to Sisense server is restricted to designated Sisense staff with a demonstrated need to service the application or infrastructure. Access to the Sisense server may be required by: IT, Sisense Cloud Service, Sisense Support and Sisense NOC.

All members of staff undergo customer data privacy and security training.

Non-disclosure of Customer Data

Upon completion of the customer data privacy and security training, each Sisense staff member signs a customer data non-disclosure memorandum.

End-to-End Business Security

To minimize the possibility of a security breach, Sisense has established security controls that cover the end-to-end business workflow from data modeling to analysis and insight delivery.

Sisense Deployment Architecture to Prevent Direct Access to Server

To enable the customers to perform necessary business actions while avoiding direct access to the Sisense server, Sisense deployed an architecture that limits customers to approved actions only.

Access to ElastiCube Manager is performed via RDWeb. This secure and encrypted access is limited to working with a designated application and file folders only.

Secure Web Access

Web access uses secure HTTPS (TLS) secure protocol with *.sisense.com certificate (Other domain certificates can be configured upon request).
Hardening to certain SSL/TLS protocols or cipher suites can be done upon request.

Moving Assets to Sisense BI in the Cloud – Secure FTP

As part of the Sisense BI business lifecycle, a customer may need to move files and other components to the Sisense BI server. Such assets include:

- UI Plugins
- REST API Connectors
- ODBC driver
- Rebranding logos
- Dashboard files
- ElastiCube & dashboard migration between environments

Manual transfer of files to designated folders is performed via FTPS. Automated transfer is realized via FTPS enabled on the Sisense BI server.

Independent Security Penetration Test

Sisense conducts annual penetration tests by an external, certified, 3rd party auditor. The company and technology are also subjected to security audits performed by the world’s most secure organizations, our customers, across a variety of sectors and client needs. We carefully review the results and are committed to resolve every High and Critical security item either as an immediate Hotfix or within the following version release. Medium and Low issues are evaluated thoroughly, added to our roadmap and fixed according to urgency and severity.

For minor and medium security items that are a priority for a customer, Sisense works closely with stakeholders to promptly address and fix issues in the following version release.

The penetration tests are conducted by an external 3rd party consulting company to proactively maintain and illustrates Sisense's commitment to security. The most recent penetration tests conducted in 2018 returned no critical items with all other significant considerations fixed with the Sisense 7.3 release. In addition, as part of the Secure Development Life Cycle, we conduct periodical security reviews on every new functionality and organize security awareness training campaigns for our staff and, when appropriate, partners

Security isn't limited to our product and we are in the process of getting ISO 27001 accreditation, which covers securely managing customer assets, labs, hosting environment, and facility security.

For more information on the results of the Penetration Test Report, or to review outcomes, please contact us.

Sisense Corporate Security, Policies & Procedures

Protocols, policies and procedures

Sisense has strict procedures and policies that are implemented and enforced to mitigate risks and comply with the high security standard we set for ourselves. Aspects covered by those security policies include:

- Acceptable Use Policy
- Access Control Policy
- Change Management Policy
- Secure Software Development Lifecycle Protocol
- Disaster Recovery Plan
- Incident Management Policy

All protocols, policies and procedures are set to comply with ISO27002 standards.

Corporate Network Security

Sisense implemented well known networking best practices to comply with high security standards. Amongst those networks are:

- Development Network – this network is used for developing the software and testing it.
- Corporate Network – this network is used to access corporate services. Sisense, as a cloud-oriented company has embraced the different cloud solutions as its corporate services so it's corporate network mostly services internet connectivity for employees.
- Production – AWS cloud, managed service machines.

Security Personnel

Sisense employs a chief information security officer (CISO) who is responsible for ensuring the company follows and maintains strict security policies and protocols, to ensure all company and customer assets are adequately protected, and any security incident is quickly resolved. As CISO, he is leading our ISO 27001 accreditation process. Additionally, Sisense has a security oversight committee chaired by the CEO, to ensure a high focus on security, across the company.

Sisense Security Conclusion

Sisense employs the most rigorous security protocols in line with industry standards and the robustness requirements of global Enterprise clients. From on-premises installations to private and managed cloud infrastructures, Sisense ensures security is of paramount priority from product development cycles, to deployment, maintenance, and version updates. Additionally, Sisense conducts regular penetration tests to assess and act on changing security tends and the latest regulations for business security For more information, please reference the Sisense Security Documentation page: https://www.sisense.com/documentation/security/.