4 Security Principles Every BI Solution Should Have

What You'll Learn:

Today, security of your data and your customers' data is understandably a top concern. But, what constitutes high-quality security when it comes to a Business Intelligence solution? Read this guide to learn four crucial security principals every BI solution should follow.

Who Should Read This:

If you are considering implementing a Business Intelligence solution but want to ensure you are choosing one that provides high-level security for your company's data - read this guide.

The only thing worse than not being able to get to your data is someone else being able to get to your data.

Your customers trust you to keep their details safe, so you need to protect sensitive and financial information from hackers, leaks and thieves. If the recent global ransomware scandal taught us anything, it's that no one can afford to get complacent.

The way we see it, when it comes to BI, security considerations fall into four main categories:

4 Security Principles for True BI Security

Process Level Security

The overall set of controls, test and procedures a system uses to safeguard data.

Any BI vendor you consider should follow all the major industry standards here. That means checking for vulnerabilities using the DREAD methodology, deploying Secure Development Life Cycle (SDLC) methodology, and running regular audits and penetration tests, in line with the OWASP testing guide. This last one should be conducted externally, so you know they're not cheating.

System Level Security

This covers who has access, and to what - i.e. authentication, permissions and user management for the application.

At a basic level, your BI platform should allow you to offer different level of access, depending on whether you want the user to view or create dashboards, or manage whole data projects.

Encryption for data, account credentials and authorization profiles is essential. Also, keep an eye out for integrations with your active directory, with other platforms using Single Sign-On (SSO), and REST API to customize security settings. These will make it far easier to keep your BI in sync with your organization's security standards.

Object Level Security

This refers to tools that manage access to different components within the platform. For example, in Sisense's case, admins control which users or groups can access or edit each dashboard and Elasticube.

Data Level Security

Now we're down to the nitty-gritty, determining precisely which data inside each data source each individual user can see.

A sophisticated BI program will allow you to use row level security to define exactly what each user sees in a dashboard that's been shared with them, or prevent new starters from accessing certain data until they've been added to the right group. That way, you don't hand over the keys to the kingdom until they've earned your faith.

How to Tell If BI Security is Up to Par

The simplest way to judge a vendor's security credentials is to look at their client list.

Banking and healthcare are, for obvious reasons, two of the most data-paranoid industries in the world. If a vendor's security standards are good enough for them, that strongly suggests they have security nailed.

Sisense, for example, works with NASDAQ and GE, as well as healthcare providers like Brightstar and Simplee. So, don't just take a vendor's word for it that their security is top notch – look for proof they've met the high-level requirements of the most demanding customers in the world.

Learn more about our Security in the:

Sisense Security Overview