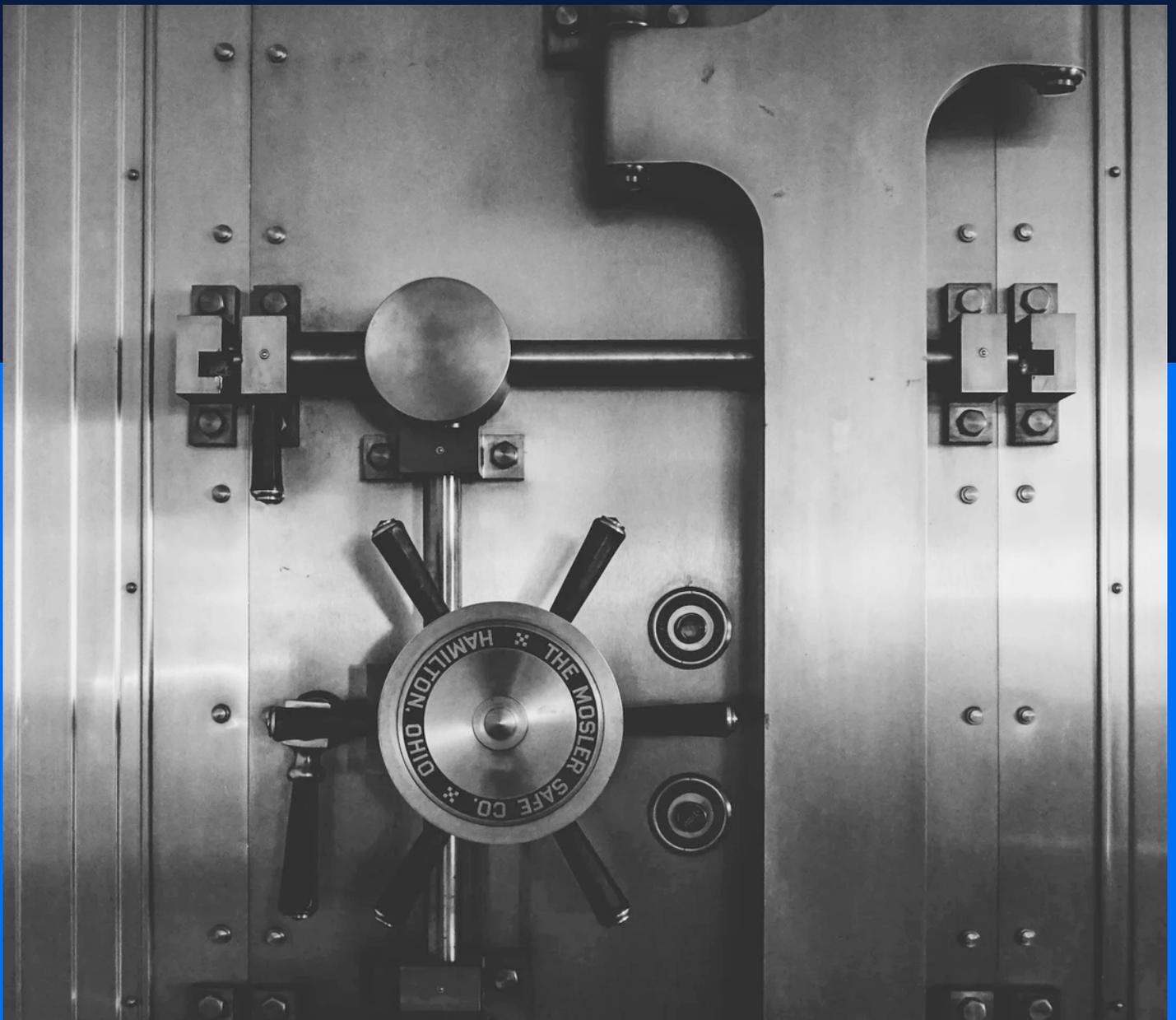


Security Whitepaper → [Weld.so](https://weld.so)

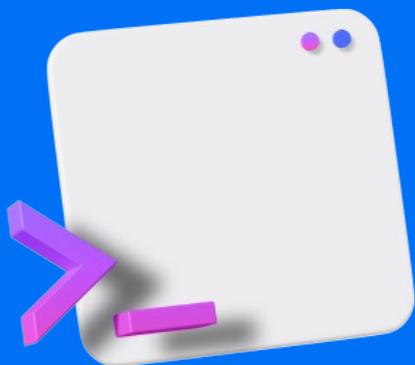


The Weld product

Weld enables a powerful reporting and data activation out of the box - built on top of your data warehouse, your single source of truth.

Weld supports two-way synchronization between the data warehouse, databases and SaaS tools. We fully manage the movement of data end-to-end, so that you don't have to build, host and maintain custom scripts in-house.

The purpose is to enable companies to have the best business intelligence dashboards as well as operational analytics workflows, where users in the SaaS tools e.g. the CRM, have access to detailed customer data. This enables smart workflows across everything from new business, upselling opportunities, identifying churn risk etc.



Best practices for developing secure software

Weld is built by a team of engineers with deep experience in building banking-grade security at Pleo, and we are committed to having Weld as a data company to apply the same high standards.

This goes across Weld's operations, product, and development of which we have built with staging and production environments, encrypted credentials separated from code, and "infrastructure-as-code" that eases auditing and permits fine-grained access to cloud resources.

In addition, we always use 2-factor authentication and secure password generators internally.



Compliant with GDPR (& CCPA)

Weld is designed to not store any personal identifiable information during data synchronization. We recognize that it's important to be compliant with modern data privacy practices, and we have no interest in neither data storing or data profiling, as we exist to move data - not store data.

Please see a [link](#) to our Data Processing Agreement and Privacy Policy.



Data encrypted in transit & at rest

Weld uses recent SSL and TLS versions for all connections between systems. From your browser to the Weld application, from our servers to your data warehouse or SaaS application, as well as internally between our own services and databases. Our own core backend application is located in our HIPAA-compliant AWS deployment, where our servers are in a private subnet without connection to the Internet.

The data pipeline at Weld is fully encrypted in transit and at rest, using the in-memory data structure store Redis running our ephemeral workers. We do therefore not see the data we are moving.

Our authentication system, also fully encrypted, is handled by enterprise - grade solution Auth0 - more details can be found at (<https://auth0.com/security>)



Built on top of the world's most secure cloud infrastructure

Weld is running on top of Amazon Web Services (AWS). We host our servers in the European Union and only work with cloud providers whose datacenters are SOC 2 and ISO 27001 certified. These cloud providers guarantee a best-in-class state of the physical and network security of Weld's servers and help us ensure that our server software is always up to date and protected from any newly-discovered threats.



Use the least privileges needed for handling data

Weld does not require super-user access to your data warehouse, and will request the fewest OAuth scopes needed to your SaaS applications in order to provide the Weld solution. The secrets we store with enterprise-grade AWS Secrets Manager which is both PCI and SOC 2 compliant.

For connection to data warehouses, we support an SSH connection in case the data warehouse is located in a private subnet.



For more information

You can find more information on our [Privacy Page](#).

For any concerns or clarifications do not hesitate to get in touch. Email us at jake@weld.so