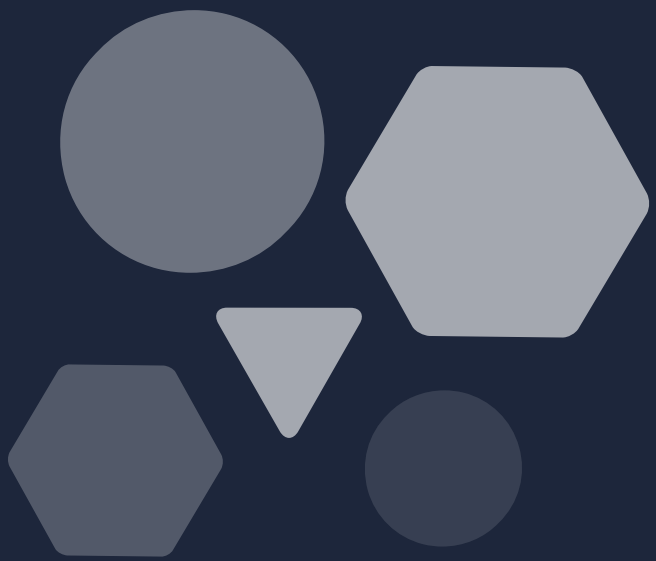
CloverDX

How CloverDX builds security into its platform

Table of contents

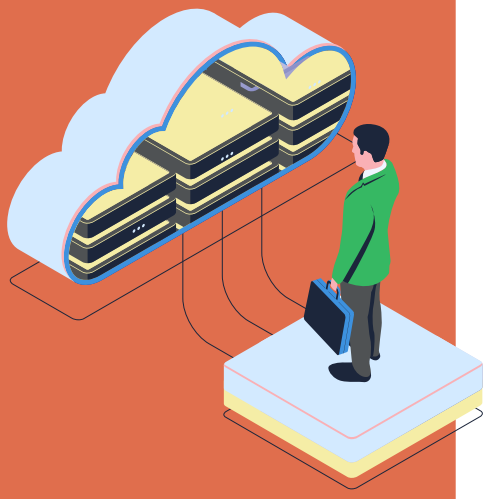


Did you know that improving IT security is a top priority for **61 percent** of organizations?

It's no surprise. In today's data-overloaded world, securing sensitive information is important for business prosperity and customer trust. Couple this with the need to comply with relevant data regulations, and the issue of data security becomes something of a necessity.

On top of establishing internal data security teams, skills and policies within your organization, you'll also need to ensure your data toolkit is secure.

So, to provide you with the reassurance you need, we've created a complete overview of how CloverDX builds security into its platform. We'll cover our overall approach and commitments.



Hosting the CloverDX platform

Before we dive into the security details, it's important to note that we do not host the CloverDX platform. It's always fully under your control, residing in your infrastructure (whether that's on-premise or in the cloud), and hinging on your security configurations.

The CloverDX teams do not have access to any of your data.

Securing your data on CloverDX

Now, let's delve into five security approaches embedded within CloverDX and why they're important. These include:

1. **User authentication**
2. **Backend database**
3. **External communication**
4. **Temporary files**
5. **Passwords and secrets**

We'll mention both the CloverDX Designer and CloverDX Server products, which make up the overall CloverDX platform.

1. User authentication

What Clover does

To access the CloverDX Server, your users must first sign on with their username and password. Alternatively, you can use a single sign-on.

In addition to this, CloverDX supports LDAP and SAML. These protocols enforce your company's unique security policies and prevent user credentials from being stored in your internal database.

While CloverDX can publish its interface as plain HTTP, we recommend publishing via an encrypted HTTPS protocol. This enables you to keep your passwords and security tokens secret, whether you're in the office or a public space.

Why it matters

With **55 percent** of workers not using any form of authentication at work, it's never been more critical to secure your data with the right security functions.

Prioritizing an **HTTPS protocol** over an HTTP protocol offers:

- In-transit data protection
- Layered encryption

In addition to this, LDAP and SAML enable key user access controls.

LDAP allows your organization to manage accounts in one central location. You no longer need to define separate users in CloverDX, but can use your LDAP to manage them.

SAML can reduce the number of times your users need to log in. They can log in just once and use all your company apps, without having to log into CloverDX Server separately.

2. Backend database

What Clover does

CloverDX Server processes data as a stream and does not store your data after the job has ended. Nevertheless, it requires a database that is used to store Server configuration, job history and logs.

CloverDX **only stores meta information**, such as execution statistics and logs, in a backend database. Not data. This is to help you with monitoring, developing and troubleshooting.

Specifically, this information includes:

- User privileges and security group configuration
- Project runtime settings and permissions
- Automation settings
- Miscellaneous server configuration

We recommend encrypting the connection between the database and your instance. This will add another layer of assurance.

Why it matters

While CloverDX doesn't store any PII data, you'll still need to choose a platform that's watertight and promotes good data security practices.

CloverDX ensures your data doesn't leak outside of the platform by:

- Automatically deleting temporary files
- Disabling debugging by default on the CloverDX Server
- Recommending HTTPS protocols

3. External communication

What Clover does

CloverDX supports the latest secure connections (typically HTTPS, SSL). We strongly recommend using those over unsecured, legacy connections.

If you choose to enable HTTPS encryption, you can encrypt all communications with the CloverDX Server (whether it's Server-to-Server or Server-to-Designer) via SSL. That said, the Server will happily connect to HTTP only or other unsecured connections.

It's worth noting that the Server sends out no external communications; it only communicates what's implemented in the graphs/job flows.

By default, the CloverDX Server does **not** collect any debugging data. You must explicitly request debug mode by either running your job manually from Designer or force-enable it on the Server. When a job runs in a debug mode, CloverDX stores debug data in its temp directory, unencrypted. This data is then deleted after some time depending on your configuration settings.

Why it matters

SSL certificates ensure the encryption and authentication of data transmitted externally. They're an essential data security defence and something you should actively look for in any data platform.

CloverDX's predetermined 'off' setting for job debugging also reduces the likelihood of 'unknown' stored data. That said, if you choose to turn this functionality on, the HTTPS protocol's data security features will offer some protection.

4. Temporary files

What Clover does

CloverDX Server may create various temporary files as it is processing data. These files are used, for example, to store data that does not fit into memory when processing large data sets. The Server can be configured to encrypt these temporary files to protect sensitive data in all stages of the job. Temporary files only exist while the job is running and are deleted afterwards. Additionally, you can explicitly request not to save any temp files in order to achieve pure in-memory processing, e.g. for compliance purposes.

If your users request job debugging, you can keep track of the data flowing through your systems. This is transported over either an HTTP or HTTPS connection, depending on what you've configured for the Server. (Again, we recommend the latter to ensure optimal data security.)

Unless explicitly configured, your data won't be stored on the Server once your executed job is complete.

Why it matters

As you're probably well aware, you should store data for the **shortest possible time**, unless there's good reason to keep it.

CloverDX's ability to encrypt temporary files or run transformations purely in memory offers the assurance that all data will be both protected during processing and terminated by default once each job is complete.

5. Passwords and secrets

What Clover does

CloverDX does not store any passwords in plaintext in its backend database.

That said, it will store the Master (encryption) password. Additionally, if you don't deploy LDAP or SAML protocols, CloverDX will store user account passwords. User account passwords are salted and hashed, whereas the master password is encrypted (not hashed).

Should you need a secret for the proper function of a job, you can encrypt and store it within a project. You can do this by using the secure parameters function.

You can find more information on our Secure Parameters **here**.

Why it matters

Did you know that compromised passwords are responsible for **81 percent** of hacking-related breaches?

Fortunately, CloverDX platform's security is watertight when it comes to storing passwords.

Your passwords are disguised behind **salting and hashing**. So, should they be breached, a hacker will have a hard time deciphering them.

Of course, we will always suggest adopting password best practices within your organization to secure your data even further.

Our security commitment

We hope the five security approaches we've listed have given you some added reassurance in the CloverDX platform.

But, we want to take things a step further.

Security isn't just a checklist exercise for CloverDX. As well as baking security features into our Designer and Server, we also champion a strong commitment to security. This commitment is centered around complete transparency.

We can break this down into three core areas: processes, release notes, and our security and feedback loop.

1. Processes

We bake security into our product and processes.

As a tool that encourages organizations to champion data security best practices, such as data anonymization, we take our own security very seriously. To summarize our security approaches, the CloverDX platform offers:

- Salting and hashing of passwords
- LADL and SAML protocols
- HTTPS encryption and SSL certificates
- Short term, temporary data storage

So, while you're solving your complex data challenges, you can rest assured that CloverDX handles your data appropriately.

In addition to this, CloverDX can also:

- **Implement the encryption or decryption of files** at rest or in transit. We support any encryption process by calling an external program at the beginning or end of the data pipeline.
- **Assist with any data audit needs**. We've undergone many IT audits, code source audits and QA testing audits to help businesses such as yours achieve compliance.

2. Release notes

We transparently publish release notes at https://support.cloverdx.com/releases.

In these release notes, expect to find:

- Latest integrations and connections
- Security updates and patches
- New platform features

You can sign up to receive the latest in CloverDX's features, support and security information by email. This will ensure you don't miss any vital updates.

3. Security and feedback loop

In addition to release notes, the CloverDX team also follows a strict Security Advisory process.

This is where we announce major known security flaws, as well as their solutions. Ultimately, we want to make our security and feedback loop as transparent as possible for our customers. That way, you can trust that we're monitoring our platform and championing security best practices.

You can find these security announcements here.

CloverDX: Your secure Data Management Platform

Our goal is to help you solve your complex data challenges. Using the CloverDX platform, you can make this a reality.

Of course, we realize the wider data security concerns your organization may have.

So, consider this our assurance that CloverDX has been built with your security needs in mind. From our embedded technical approaches, to our ongoing commitment to transparency, CloverDX has you covered.

Of course, if you have any questions, please do not hesitate to **get in touch**. Our team is more than happy to answer your questions and provide necessary reassurance.

Contact us today