

SECURITY & THE COGNITE DATA PLATFORM

Cognite commits to being a Trusted Custodian of our customers' data. Security is a feature of everything we do.

The Cognite Data Platform (CDP) is designed to integrate seamlessly with your existing equipment and infrastructure, to provide you with full visibility and total control. Your data is always your own. But you trust Cognite to help you extract value from your data using the CDP. That's why we are committed to our role as a Trusted Custodian of your data. As such, we hold ourselves to the highest standards of operational excellence, security, integrity, and transparency.

To fulfil our responsibility as a Trusted Custodian, we have developed the Cognite Security Commitment: six principles that focus on People, Processes, and Technology to inform the design of the Cognite Data Platform.

To ensure our success, the Cognite Security Commitment is supported by a variety of processes and policies that are woven into the fabric of Cognite and the Cognite Data Platform. These include:

The Cognite Security Commitment



Secure

The capacity to safeguard assets and their integrity



Robust

The capacity to remain healthy and uncompromised



Responsive

The capacity to absorb disturbances while maintaining functionality



Reliable

The capacity to maintain consistent performance



Resilient

The capacity and services to react and recover quickly



Flexible

The capacity to adapt easily to new requirements

- Rigorous testing and validation of source code
- Realtime monitoring of service and security posture
- Logging and audit trail
- Detailed reporting against key metrics
- Training and development

WHAT DOES THE COGNITE SECURITY COMMITMENT MEAN IN PRACTICE?



Cognite will keep your data private

Maintaining the security and privacy of our customers' data is foundational to both Cognite and the Cognite Data Platform. The platform is designed and built to ensure that data is only accessible to those who have been granted access.

Data is encrypted in transit and rest, with Cognite authenticating, authorizing, and logging all transactions through the data platform.



Cognite will enable controlled access to your data

Ease of access to targeted data is a primary function of the Cognite Data Platform. The data owner will retain full control over who has access to what, both internally and externally.

Cognite ensures this capability by controlling, restricting, and granting access through user/group permissions and security categories. User access is gated by a managed directory (e.g., Azure AD). Machine access is granted through managed API keys.

WWW.COGNITE.COM



Cognite will keep your data integrity intact

Data contextualization and enrichment are critical aspects of any successful digitalization effort. At Cognite, we also recognize the importance of preserving the original data.

Cognite will maintain a continuously updated history of your data. The base information in the Cognite Data Platform is an exact replication of your data, regardless of the source system(s). To maintain accuracy, Cognite will verify data integrity.



Cognite will monitor and audit the platform and services

Continuous monitoring and security and health assessments are important to our customers.

Cognite carries out a variety of audit and assessment activities. These include an immutable audit trail for any interactions with customer data and related infrastructure, as well as realtime reporting on the CDP status.