# IT Security Overview

Celonis Intelligent Business Cloud

celonis

# Celonis Security Model

The Celonis Intelligent Business Cloud (IBC) has been designed to deliver end-to-end data security. We follow best-in-class standards to ensure the best possible protection for our customer data. Security in your IBC team is a shared responsibility between you as customer and Celonis, as service provider. Customers are responsible for both the configuration and usage of services provided by Celonis.

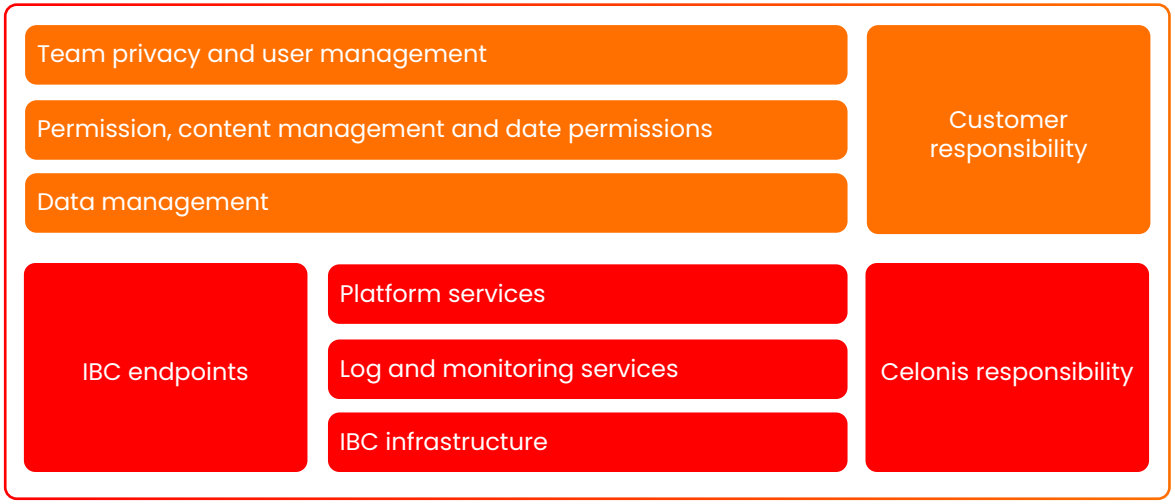



**Figure 1: Security responsibilities of customer and Celonis**

Celonis applies a multi-layered security architecture to protect customer data, which addresses the following:

- External interfaces
- Access controls
- Data storage
- Physical infrastructure

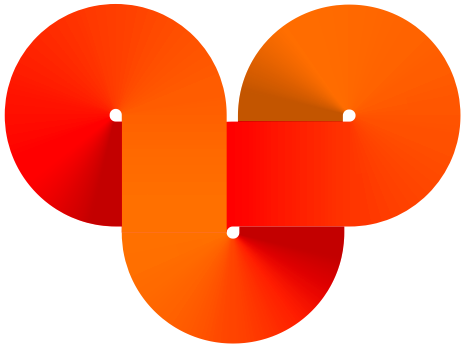
This security architecture is complemented by monitoring, alerts, controls and processes that are part of Celonis' security measures.

# External Interfaces

The Celonis Intelligent Business Cloud (IBC) has been designed to deliver end-to-end data security. We follow best-in-class standards to ensure the best possible protection for our customer data. Security in your IBC team is a shared responsibility between you as customer and Celonis, as service provider. Customers are responsible for both the configuration and usage of services provided by Celonis.

- Celonis' web-based interface
- Celonis' on premise extractors
- IBC Data Push API

All communication between user and Celonis services is encrypted via HTTPS using TLS 1.2 or higher. The IBC supports IP range blocking to enable customers to restrict access to trusted networks only.



# Access Controls

## Authentication

The IBC has robust authentication mechanisms in place. Every request to the IBC must be authenticated and scanned by a web-application firewall. User password hashes are securely stored and strong password policies are enforced. The IBC offers built-in two-factor authentication. For customers who want to manage authentication mechanisms within their account, federated authentication can be set up via SAML 2.0 or OpenID.

## Authorization

The IBC provides a detailed, role-based authorization concept to ensure that data and information is only accessed by authorized users. User access to all objects and elements in the IBC can be specified with user and group permissions. Team administrators can choose from a set of user or role permissions templates or design custom permissions. Access to single data points in an analysis can be restricted using a sophisticated data permissions framework.

## Data Storage

We protect all data stored in the IBC from unauthorized access and from data loss by incorporating data encryption and access restrictions. Additionally, customers can select between regions in Europe, US and Japan to define where the data is stored.

## Data Encryption

In the IBC, all customer data, including backup data, is always encrypted at rest (AES-256) following best-in-class industry standards. All data transferred to the IBC via connector or data push API is always encrypted via HTTPS using TLS 1.2 or higher.

## Data Access

Each customer has full ownership and access control for their IBC tenant. Tenant access is fully transparent via built in audit logs, and multiple security measures can be set in place to further protect and restrict tenant access. Customers can restrict and delegate user authentication to an external identity provider, enforce two-factor authentication and/or restrict access to a tenant to specific IP ranges.

Similar to most major SaaS platforms, Celonis infrastructure administrators require privileged access to the underlying infrastructure of the IBC for maintenance. This administrative access is restricted to a small number of specialized Celonis employees whose access is logged, monitored and reviewed regularly to prevent abuse according to Celonis' strict policies and access controls.

## Data Integrity Protection

Celonis protects data from accidental or intentional destruction due to user errors, system failures or malicious attacks. Backups for application and analytics data are created daily and, if necessary, can be recovered for 30 days.

## Security Monitoring and Alerting

To protect the platform from malicious attacks, the IBC architecture includes multiple layers of defense. To reduce the risk of malicious attacks, highly specialized systems are used for dedicated service tasks.

System hardening policies and guidelines are used to protect the operating system. Firewalls and network zoning, combined with access controls and application-level policies ensure only authorized users can access the Celonis application.

Celonis manages and orchestrates overall IBC system security via logging and monitoring. All telemetry data is captured and centrally stored.

## Tenant Separation

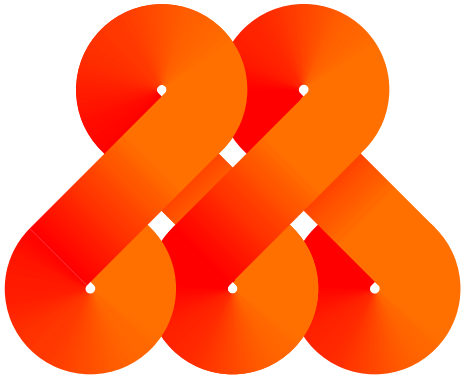
The IBC is run on a multi-tenant architecture in which each team in the IBC is one tenant. Tenant separation follows a metadata driven approach and industry best-in-class standards. Application data as well as analytical data are separated between all tenants.

## Physical Security

The IBC supports our main geographic regions (Americas/Europe/Japan) through data centers hosted by Amazon Web Services (AWS) and Microsoft Azure.

AWS and Azure data centers are certified as ISO 27001 and PCI/DSS Service Provider Level 1.

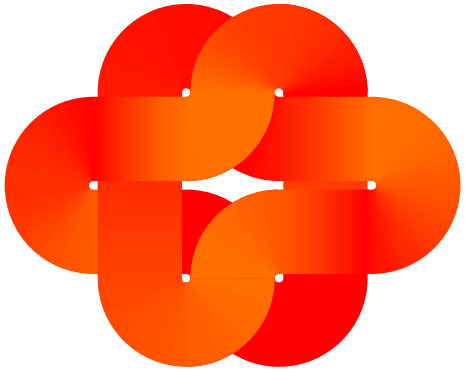
AWS and Azure data centers are state of the art and utilize innovative architectural and engineering approaches. They employ comprehensive physical security measures, including biometric access controls, 24-hour armed guards and video surveillance to ensure that unauthorized access is not permitted at any time. As a standard security measure neither Celonis personnel nor Celonis customers have access to these data centers.



# Security Compliance

Celonis' dedicated IT security team monitors platform security and works with certified third-party auditors to validate and maintain security. Celonis runs its own security tests on a quarterly basis and our infrastructure providers follow their documented standards. External application and network penetration tests are performed half-yearly.

Celonis is dedicated to high security across all aspects of the organization. Celonis uses the ISO 27002 best practices. Additionally, Celonis holds a full ISO 27001 certification and has successfully implemented an Information Security Management System (ISMS) according to ISO 27001 standards.

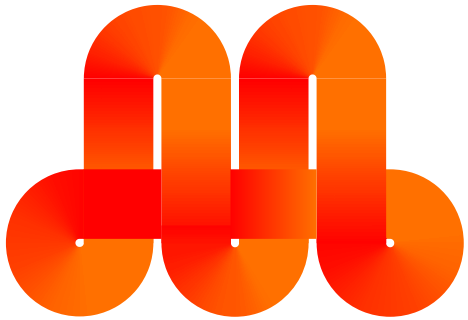


# Conclusion

The Celonis Intelligent Business Cloud (IBC) is a platform developed in alignment with a security-by-design approach wherein security has been fundamental to the architecture, implementation and operation of Celonis from the very beginning. Across all scenarios and deployment options the IBC offers a secure and protected platform for customer data from current and evolving threats. The features built into the IBC provide enterprise-class security by default without the additional effort, complexity and management that traditional solutions require from customers. Every aspect of the IBC is built to protect our customers' data.

## Disclaimer:





celonis.com