celonis

Intelligent Business Cloud
IT Security Overview

February 2019

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's data. Security in your IBC team is a shared responsibility between you, the customer, and Celonis, the service provider. Celonis provides services that are designed with a high security standard. The configuration and utilization of the services are the responsibility of you.

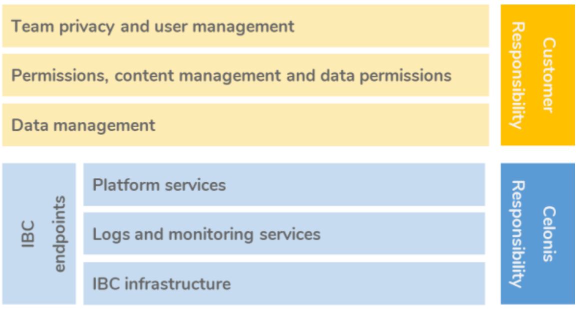
Team privacy and user management
Permissions, content management and data permissions
Data management
Customer Responsibility
IBC endpoints
Platform services
Logs and monitoring services
IBC infrastructure
Celonis Responsibility

Figure 1: The security responsibilities of the customer and Celonis

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

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

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

EXTERNAL INTERFACES

Users access the IBC via the Internet using secure protocols. It is possible to connect to the services with the following options:

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

All communication between the user and the 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 Celonis IBC has robust authentication mechanisms in place. Every request to the IBC must be authenticated and is 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 mechanism to their account, federated authentication can be set up via SAML 2.0 or OpenID.

Authorization

The Celonis IBC provides a detailed, role-based authorization concept to ensure data and information access by authorized users only. User access to all objects and elements in the IBC can be specified with user and group permissions. The customer can choose from a set of templates for the user or role permissions or design custom permissions. Access to single data points in the analyses can be restricted with 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 choose region and realm where the data is stored.

Data Encryption

In the IBC, all customer data is always encrypted at rest 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.

Tenant separation

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

Data integrity protection

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

Security Monitoring and Alerting

To protect the platform from malicious attacks multiple layers of defense have been set up and integrated into the IBC architecture. The system is protected on OS level through system hardening policies and guidelines. On network level, firewalls and network zoning ensure only whitelisted applications are exposed, this is reduced to the application itself. On application layer, access controls and policies ensure only authorized access. Elevated privilege access is only possible through a jump server, creating an additional barrier. Highly specialized systems are used for dedicated service tasks to reduce attack surface.

Log and monitoring services in the IBC are used to manage and orchestrate all tenants. All logs are captured and synchronized into a centralized log storage. Our centralized logging store includes logs from Application Logs, Audit Logs, Firewall Logs, and Application Change Logs.

Physical Security

The Celonis IBC is hosted in Amazon Web Services (AWS) or Microsoft Azure data centers and is available in multiple regions. AWS and Azure data centers are certified as ISO 27001 and PCI/DSS Service Provider Level 1. AWS' and Azure's data centers are state of the art, utilizing innovative architectural and engineering approaches. They employ many physical security measures, including biometric access controls, 24-hour armed guards, and video surveillance to ensure that no unauthorized access is permitted. As a standard security measure, neither Celonis personnel nor Celonis customers have access to these data centers.

SECURITY COMPLIANCE

Celonis monitors security on the platform with a dedicated IT security team and works with certified third-party auditors to validate and maintain security. On application level, Celonis runs its own tests (once a quarter), while on infrastructure level the cloud providers' standards apply. External penetration tests for application/network are performed half-yearly.

Celonis is dedicated to high security across all aspects of the organization. We are using the ISO27002 best practices as Celonis goes through the full ISO27001 certification and has successfully implemented an Information Security Management System (ISMS) according to ISO27001 standards.

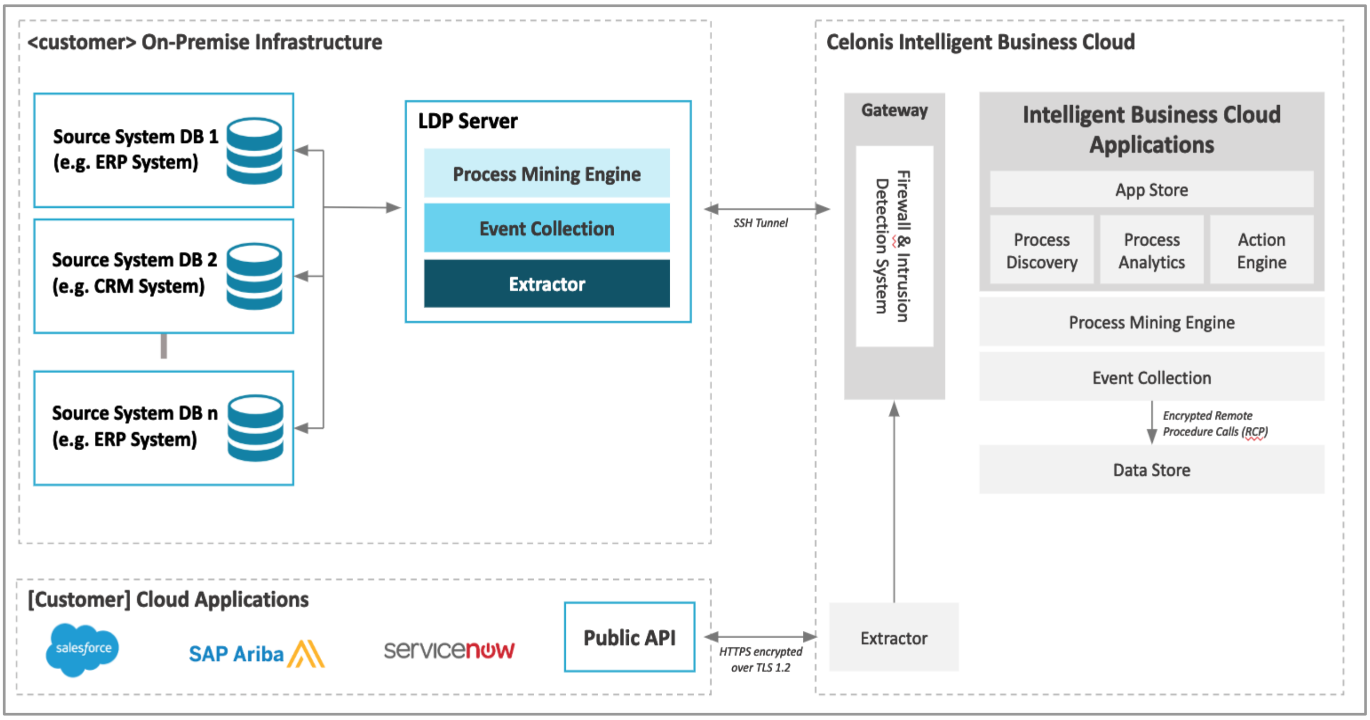
<customer> On-Premise Infrastructure
Source System DB 1 (e.g. ERP System)
Source System DB 2 (e.g. CRM System)
Source System DB n (e.g. ERP System)
LDP Server
Process Mining Engine
Event Collection
Extractor
SSH Tunnel
Celonis Intelligent Business Cloud
Gateway
Firewall & Intrusion Detection System
Intelligent Business Cloud Applications
App Store
Process Discovery
Process Analytics
Action Engine
Process Mining Engine
Event Collection
Encrypted Remote Procedure Calls (RCP)
Data Store
[Customer] Cloud Applications
salesforce
SAP Ariba
servicenow
Public API
HTTPS encrypted over TLS 1.2
Extractor

Figure 2: IBC Leave-your-data-in-place architecture

LEAVE YOUR DATA IN PLACE

Celonis offers several scenarios for the IBC where the customer can decide how the data processing is configured. The Leave your data in place (LDP) scenario allows the customer to fully move the data processing to his or her premises or a virtual private cloud hosted and managed by the customer. In the LDP scenario the analytics data is fully managed and utilized on the customer's servers. The Event Collection with data extractors, the analytics data store, and the Celonis Process Mining Engine are fully run on the customer owned infrastructure (see figure above). Analytics configuration, user management, and content management stay at the IBC's side. The connection between both is established via a secure SSH tunnel.

CONCLUSION

The Celonis Intelligent Business Cloud is a platform developed from the ground up for the cloud where security is fundamental to the architecture, implementation, and operation of Celonis' service. Across all scenarios and deployment options the Celonis 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. Security is a top priority, from the CEO to every Celonis employee, to ensure this high standard every day.

Disclaimer

This document is protected by copyright laws and contains material proprietary to Celonis SE, its affiliates (jointly "Celonis") and its licensors. The receipt or possession of this document does not convey any rights to reproduce, disclose, or distribute its contents, or to manufacture, use, or sell anything that it may describe, in whole or in part.

This document is provided for informational purposes only. It represents Celonis' current product offerings and practices as of the date of issue of this document, which are subject to change without notice. Customers are responsible for making their own independent assessment of the information in this document and any use of Celonis' products or services, each of which is provided "as is" without warranty of any kind, whether express or implied. This document does not create any warranties, representations, contractual commitments, conditions or assurances. The responsibilities and liabilities of Celonis to its customers are controlled by Celonis agreements, and this document is not part of, nor does it modify, any agreement between Celonis and its customers.