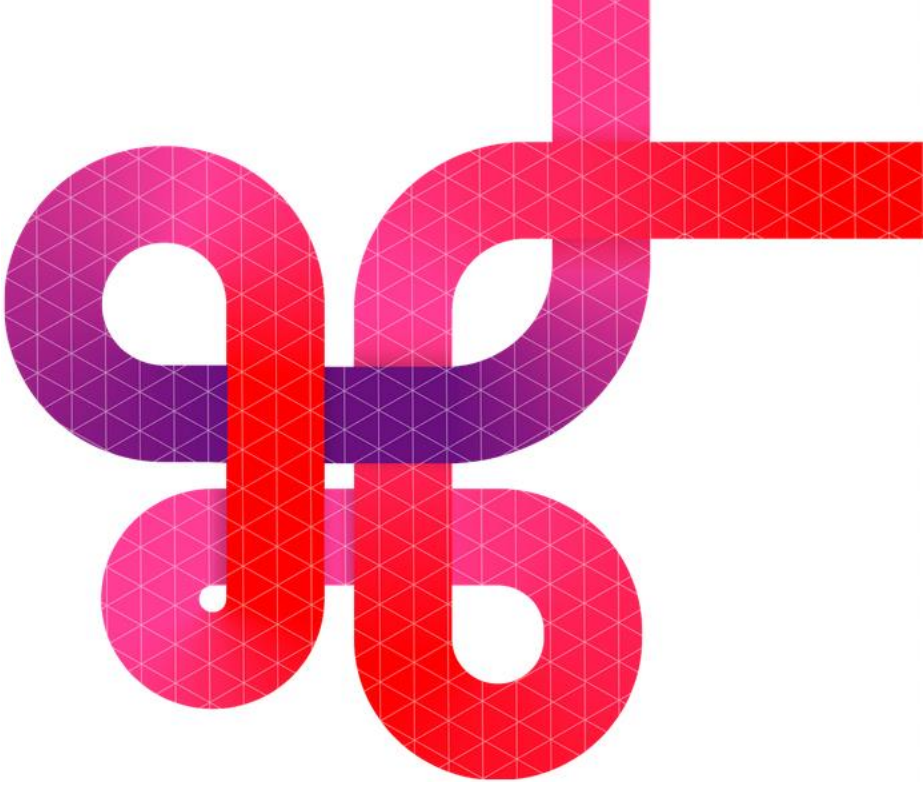

IT Security Overview

Celonis Intelligent Business Cloud

August 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 data. Security in your IBC team is a shared responsibility between you as customer and Celonis, as service provider. Celonis provides services that are designed with a high security standard. Customers are responsible for both the configuration and usage of the services provided by Celonis.

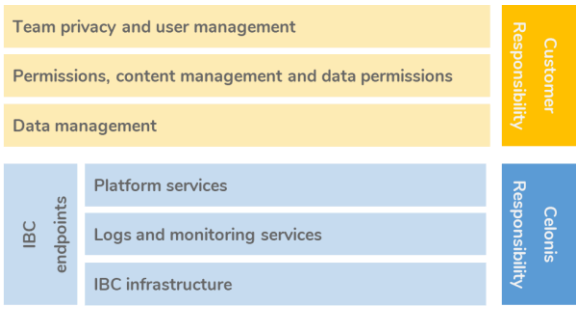

Figure 1: Security responsibilities of customer and Celonis

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

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

- ❏ 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 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 mechanisms within 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 that data and information is accessed by authorized users only. User access to all objects and elements in the IBC can be specified with user and group permissions. The realm 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 select both region and realm where the data is stored.

Data Encryption

In the IBC, all customer data (incl. backup 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 attacks. 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 (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 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 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 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 holds a full ISO27001 certification and has successfully implemented an Information Security Management System (ISMS) according to ISO27001 standards.

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 servers. The Event Collection with data extractors, the analytics data store, and the Celonis Process Mining Engine fully run on the customer owned infrastructure (see figure 2 below). Analytics configuration, user management and content management stay on the IBC side. The connection between both is established via a secure SSH tunnel.

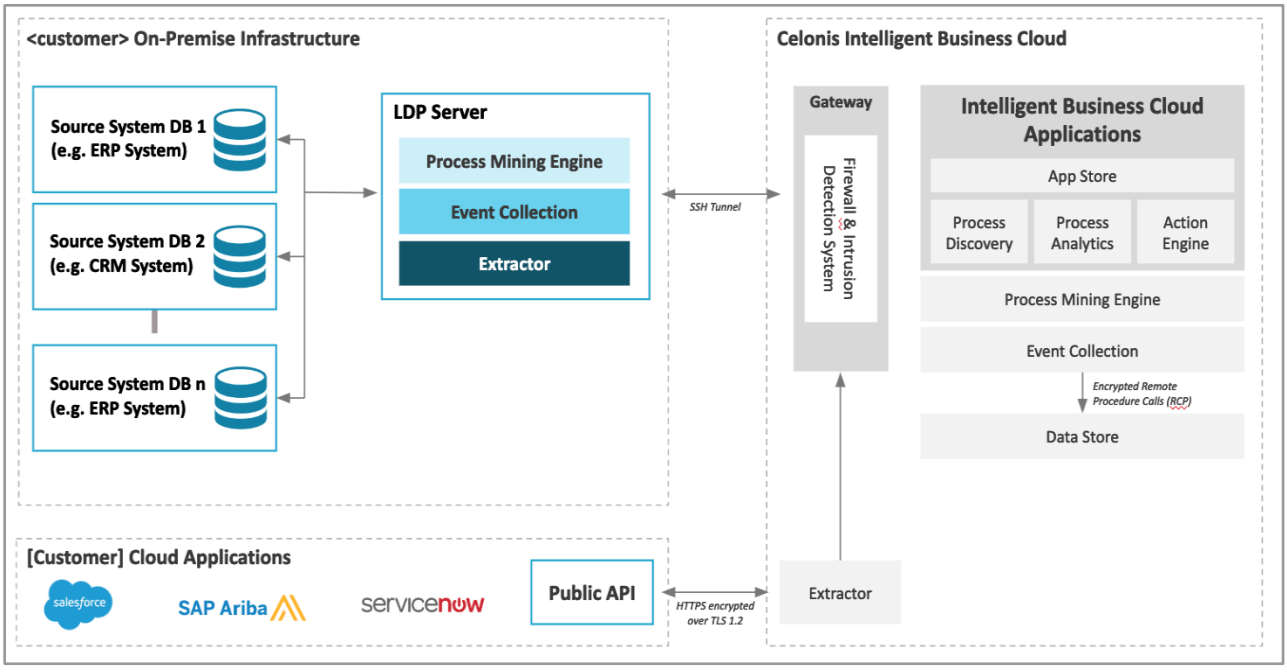

Figure 2: IBC Leave-your-data-in-place architecture

Conclusion

The Celonis Intelligent Business Cloud is a platform developed in alignment with the security by design approach where security has been fundamental to the architecture, implementation and operation of Celonis service from the very beginning. 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: