BOC Cloud Services - Security Overview

Table of contents

Acronyms

Acronym	Description
BPM	Business Process Management
HTTPS	Hypertext Transfer Protocol Secure
IPSec	Internet Protocol Security
IaaS	Infrastructure-as-a-Service
RBAC	Role Based Access Control
SaaS	Software-as-a-Service
VPN	Virtual Private Network

1 Introduction

BOC is offering different operation models of the BOC Management Office tools based on cloud technology. When choosing one of these models, it is evident that security aspects need to be analyzed. Whether for legislative rules, regulatory constraints, or company policies, some of the questions to be answered are:

- Where is the application data located?
- Who has access to the data?
- How is separation of client data achieved?

This document provides a transparent description of various security-relevant aspects of BOC's cloud services, in order to support the decision making.

2 Partners

BOC cloud services are implemented on standardized infrastructure services (IaaS) of the following providers:

Option 1 – AWS Germany as main location

- Primary IaaS-Provider
  - Amazon Web Services EMEA Sàrl, 38 Avenue John F. KennedyL-1855 **Luxembourg**, Data Center in **Germany** (eu-central-1)
- Disaster Recovery IaaS Provider:
  - Amazon Web Services EMEA Sàrl, 38 Avenue John F. KennedyL-1855, **Luxembourg**, Data Center in **France** (eu-west-3)

Option 2 – Cloudsigma Switzerland as main location

- Primary IaaS-Provider
  - Cloudsigma AG, Badenerstrasse 549, 8048 Zurich, Data Center in **Switzerland**
- Disaster Recovery IaaS Provider:
  - Amazon Web Services EMEA Sàrl, 38 Avenue John F. KennedyL-1855, **Luxembourg**, Data Center in **France** (eu-west-3)

All partners are committed to strict security principles, involving minimum required permissions for their staff members, appropriate access control systems, processes for dealing with security breaches and advanced logging systems for access and change tracking.

3 Secure Platform Architecture

BOC's platform powering the cloud services has been developed with the objective to provide best protection of client data. Access to the cloud services is only possible with HTTPS. Management of the infrastructure components is granted solely to authorized staff members through a 2-Factor authenticated VPN connection. The platform utilizes several network segments to separate the environment into appropriate zones, reducing

the allowed traffic among these zones to the required minimum. Any changes to the platform are enacted and logged by means of a configuration management system, backed by a version control system, and can be triggered only by authorized staff members. Strong password policies are in place for all administrative accounts. All systems are being kept up to date with regard to security patches.

4 Secure Software

The BOC Management Office tools are being developed, tested, and maintained with a strong commitment to best practices in secure software development. To accomplish this, the development teams follow the guidance provided by the OWASP ASVS project. The source code is continuously scanned for typical security loopholes by means of static code analyzers and changes are reviewed by developers with a strong focus on web application security. Additionally, penetration tests are performed on a regular basis in order to validate the effectiveness of the implemented security measures. The Software Development Process is certified according to ISO27001.

5 Tenant Separation

BOC Management Office tools are being provided as cloud services in different operation models. The differences of these models in terms of client data separation are highlighted below.

5.1 ADONIS Starter Edition

ADONIS Starter Edition provides a pre-configured BPM tool as a service in a subscription model. ADONIS Starter Edition users have private data containers allocated in a database which is shared with other clients and computing resources are also provided on shared applications stacks. The separation of data is ensured by the permission mechanisms built into the software.

5.2 Enterprise Edition

Any BOC Management Office tool provided in the Enterprise Edition variant is open for client specific customizations. As a consequence, every account has its private database and a dedicated application stack. The databases are located on shared database servers and there are multiple application stacks hosted on a single virtual machine.

6 Backup

Client data is backed up on two destinations. One is a separate storage on the primary site and the other is a storage in the respective disaster recovery infrastructure. The traffic between the two locations is encrypted. Retention policies ensure that any data expiring from the retention period is deleted on both backup destinations. Except for ADONIS Starter Edition, immediate deletion of client data including backups can be requested by authorized client representatives.

7 Encryption

Confidentiality of client data is ensured by applying encryption wherever needed. Any data transmitted over insecure networks is protected by state-of-the-art transport layer encryption. Data at rest can be protected applying one of the common models: *provider owned key, hold your own key, bring your own key*. For details, please refer to the document *BOC Cloud Services – Encryption.pdf*.

8 Access Control

BOC Management Office tools offer various methods of controlling access to content. Authentication methods range from tool managed user accounts to federated identity management based on SAML 2.0 or OIDC, including auto provisioning. A sophisticated rights management capability supports full role-based-access-control (RBAC). Operations engineers are subject to strong authentication when connecting to the SaaS platform following the least privilege and need to know principles.