BarTender Cloud™
BY SEAGULL SCIENTIFIC

BarTender Cloud™ Security and Infrastructure

October 21, 2022

BarTender®
BY SEAGULL SCIENTIFIC

Table of Contents

Introduction

For over 30 years, BarTender software has been trusted by more than 100,000 companies around the globe in every industry including those in the most heavily regulated industries — from aerospace, to healthcare, to manufacturing to power their labeling operations. This expertise and reliable performance are now available in the cloud with BarTender Cloud™. Designed as a true Software as a Service (SaaS) product offering, BarTender Cloud provides a simple, easy yet powerful labeling solution without the need for customers to install and maintain their own software and hardware.

This document details the key security and infrastructure underpinnings of BarTender Cloud. BarTender Cloud's system architecture, along with its defined operations, provides its customers with high availability and strong safeguards for our customer's data with a robust and comprehensive privacy and security program.

Infrastructure

High availability

BarTender Cloud guarantees 99.9% high service availability as defined in our Service Level Agreement.

BarTender Cloud has been designed to be a secure, reliable, and scalable architecture. Customers are deployed across multiple redundant clusters of nodes allowing for automatic scaling of resources based on demand. Customer and system data is replicated and continuously backed up with automated failover.

BarTender Cloud, including its customer data, is hosted on AWS (Amazon Web Services). AWS is the world's most comprehensive and broadly adopted cloud platform with unmatched experience, maturity, reliability, security, and performance. For over 16 years, AWS has been delivering cloud services to millions of customers around the world running a wide variety of use cases.

Health monitoring

BarTender Cloud's architecture design integrates industry leading tools including Amazon CloudWatch for continuous network, application, and system monitoring to provide system-wide visibility and resource optimization and to ensure operational health. Our technical teams monitor for possible security threats while continuously ensuring performance and scalability.

Maintenance and updates

BarTender has a regular release cadence to address issues as they arise along with providing feature enhancements and improvements. Each release goes through a defined release process before deployment.

Disaster recovery

In the unlikely event of a widespread system failure, our technical teams have a comprehensive disaster recovery plan for restoring customer data back from regular data backups for service.

Data retention

Customer data, including stored label template files, will be retained if their BarTender Cloud account remains active. Upon expiration of the BarTender Cloud account, customer data will be retained for up to 90 days after which point it will be deleted. Activity history will be retained for a maximum of one year for the Essentials Plan and indefinitely for the Automation Plan while the BarTender Cloud account is active. Note that Activity history log storage counts against the overall account storage size.

Internet connectivity

BarTender Cloud requires Internet connectivity to enable printing at customer's locations. Our Professional Services team can advise on best practices or design solutions for using BarTender Cloud in your network environment to meet your labeling needs.

Security

The focus of BarTender Cloud's security operations is to prevent unauthorized access to BarTender Cloud and to safeguard our customer's data. Our Engineering, DevOps and Security teams work together to take exhaustive steps to identify and mitigate risks, implement best practices, and constantly develop ways to improve our security.

Privacy

We are committed to safeguarding the privacy of our customer's data as detailed in our Privacy Policy.

Layered security

BarTender Cloud ensures that any data stored is safe through its architectural design, implementation, deployment, and ongoing management operations. Layered security controls including physical and logical, technical, and administrative controls which have been designed to protect customer data and reduce risk.

Network security and server hardening

BarTender Cloud's system architecture divides its systems into separate networks to better protect sensitive data. Systems supporting testing and development activities are hosted in a separate network from systems supporting BarTender Cloud's production infrastructure. All servers within our production environment are hardened (e.g., disabling unnecessary ports, removing default passwords, etc.) and have a base configuration image applied to ensure consistency across the environment.

Network access to BarTender Cloud's production environment from the open Internet is restricted, with only a small number of production servers accessible from the Internet. Network security is integrated into BarTender Cloud's software and system architecture and includes firewalls, role-based access controls (RBAC) and other access restriction techniques along with intrusion detection. Privileged access is restricted via a combination of VPN tunneling and the use of public key authentication or randomly generated passwords.

Security compliance

BarTender Cloud is continuously monitoring, auditing, and improving the design and operating effectiveness of our security controls. These activities are regularly performed by both third-party credentialed assessors and BarTender Cloud's internal technical teams. Audit results are shared with senior management and all findings are tracked to resolution in a timely manner.

BarTender Cloud is hosted on AWS which supports more security standards and compliance certifications than any other offering, including PCI-DSS, HIPAA/HITECH, FedRAMP, GDPR, FIPS 140-2, and NIST 800-171. For further details on AWS, see https://aws.amazon.com/compliance.

Database security

Each BarTender Cloud customer's data is hosted in our shared infrastructure and logically separated from other customers' data. Customer data is only accessible by that customer. BarTender Cloud is hosted in AWS data centers offering state-of-the-art physical protection for the BarTender Cloud servers and infrastructure.

Data encryption

BarTender Cloud provides a high level of security by encrypting customer data including data in transit and data at rest.

Data in transit

All data transmitted between BarTender Cloud clients and the BarTender Cloud service uses strong encryption protocols. BarTender Cloud supports the latest recommended secure cipher suites to encrypt all traffic in transit, including use of TLS 1.2 protocols, AES256 encryption, RSA and Elliptic Curve DSA, and SHA384 signatures, whenever supported by the clients.

Data at rest

Data at rest in BarTender Cloud's production network is encrypted using FIPS 140-2 compliant encryption standards, which applies to all types of data at rest within BarTender Cloud's systems—databases, file stores, database backups, etc. All encryption keys are stored in a secure server on a segregated network with very limited access. We have implemented appropriate safeguards to protect the creation, storage, retrieval, and destruction of secrets such as encryption keys and service account credentials.

API security

BarTender Cloud offers programmatic access via the BarTender REST API. Access via this API goes through an API gateway and Security API. Secure authentication is available via an access token or industry standard OAuth protocols and providers.

Internal testing

BarTender Cloud builds upon the proven software practices developed over the past 30 years with BarTender software ensuring the highest quality and security. These best practices include a robust and proven set of software principles and design. We employ a variety of hybrid agile development techniques such as Scrum and test-driven development (TDD). Code reviews are performed on changes against established coding standards. We also ensure quality with comprehensive unit, regression, and integration testing.

Third-party security assessments

In addition to our compliance audits, independent entities are engaged to conduct application-level and infrastructure-level penetration tests at least annually.

Results of these tests are shared with senior management and are triaged, prioritized, and remediated in a timely manner.

Our third-party security assessment providers use the OWASP Testing Guide for test execution and verification. The Open Web Application Security Project, or OWASP, is an international non-profit organization dedicated to web application security.

Additional resources

These documents are available upon request.

Note: Some documents may require a signed non-disclosure agreement.

1) BarTender Cloud Terms of Service

2) BarTender Cloud Service Level Agreement

3) BarTender Privacy Policy

4) The AWS Cloud Security Alliance (CSA) Consensus Assessment Initiative Questionnaire (CAIQ) has been completed using the current CSA CAIQ standard, v4.0.2 (06.07.2021 update), and is available for download.

5) Penetration testing reports. Assessments from our third-party security company showing tests performed for BarTender Cloud, test time intervals, any vulnerabilities, and their conclusions on software security.

6) (In progress) The BarTender Cloud Consensus Assessment Initiative Questionnaire (CAIQ) shows compliance with CSA® (Cloud Security Alliance) best practices.

BarTender®
BY SEAGULL SCIENTIFIC

www.SeagullScientific.com