BillingPlatform

Best-in-Class
Enterprise-Grade Security

Minimize Risk and Ensure Compliance with BillingPlatform

Confidence in deploying a cloud infrastructure to manage business operations continues to grow. “Cloud-first” strategies are becoming more common, even among risk-averse organizations such as banks and financial institutions. As organizations continue to move their applications and data to the cloud, CIOs and CISOs are requiring complete control of their business operation and demanding secure and compliant solutions that can adapt to any market regulation or standard.

Enterprise-level security provides a set of policies, methods and technologies that protect infrastructure, data and applications that are cloud-based. It is designed to keep data:

- Safe from theft, unauthorized deletion and data leakage
- Protected from unauthorized access
- Private and secure to support regulatory compliance requirements

BillingPlatform was built with security and compliance in mind. Our cloud-based solution offers a full set of enterprise tools and policies that comply with industry best practices offering CIOs and CISOs confidence through its enterprise-level security. Plus we continue to incorporate new solutions, policies and processes while staying current with industry compliance standards to provide the most secure and scalable solution to help customers provide the best experience for their customers.

Below are details on the physical & network security and application-level security offered by BillingPlatform.

Physical & Network Security

Infrastructure

BillingPlatform is hosted in Amazon Cloud (AWS) and takes advantage of AWS enterprise-grade network management and security services. As such, physical access to the network is strictly limited and monitored. Restrictive firewalls protect communication entering the network and

between private networks. Access to BillingPlatform's network and services is strictly logged with audit logs reviewed on a regular basis.

In addition, BillingPlatform performs the following on a regular basis and provides applicable reports to its customers:

- Internal and external network penetration tests
- Two-factor authentication and strong password controls are required for access
- Data loss prevention (DLP) techniques to ensure data protection
- Annual SOC 1 and 2 and PCI level 1 certification

Multi-Factor Authentication

Multi-factor authentication (MFA) is an authentication method that requires users to provide two or more pieces of evidence (or factors) to verify their identity to access the application.

MFA is typically based on one of three types of information:

- Something you know (knowledge), such as a password or PIN
- Something you have (possession), such as an authenticator app or security key
- Something you are (inherence), such as a biometric like fingerprints or voice recognition

By tying user access to multiple types of factors, MFA makes it much harder for common threats like phishing attacks and account takeovers to succeed.

Code Safety & Reviews

BillingPlarform follows a strict development process that enforces code to be reviewed before releasing into the core product. These reviews include a manual code review by at least one independent reviewer along with QA testing that is both manual and automated to affirm the application exhibits only expected functional behaviors. Every release is validated using an industry-leading security vulnerability scanning tool. The vulnerability scan also includes an audit of all third-party dependencies used within the application.

SOC 1 and 2 Compliance

SOC 1 and 2 are designed to help organizations assess whether or not proper controls are in place for both data reporting and data management. SOC 1 focuses on the financial side, while SOC 2 evaluates how companies protect consumer information.

As a provider that manages billing and customer data for its customers, BillingPlatform maintains SOC 1 and 2 compliance to ensure the proper internal controls over financial reporting and the privacy of customer data.

PCI Data Security Standard Compliance

BillingPlatform is Payment Card Industry Data Security Standard (PCI-DSS) Level 1 compliant, a standard that specifies best practices and various security controls for credit card payment processing. We meet the following PCI DSS requirements:

- Build and maintain a secure network
- Protect cardholder data
- Maintain a vulnerability management program
- Implement strong access control measures
- Regularly monitor and test networks
- Maintain an information security policy

GDPR

The EU data privacy landscape has changed significantly due to the General Data Protection Regulation (GDPR), which took effect on May 25, 2018. The GDPR has harmonized the patchwork of data protection laws in Europe. BillingPlatform allows customers to process personal data within their billing operations while complying with the GDPR.

BillingPlatform can integrate seamlessly into any GDPR compliance program. Largely, the BillingPlatform solution does not collect personal data from consumers directly or use that information for purposes other than billing. Therefore, finance leaders who wish to store private data in our solution find they only need to make small adjustments when configuring BillingPlatform to fulfill GDPR requirements. It's a plug-and-play, GDPR-compliant solution. In addition, BillingPlatform allows customers to choose which personal information will be stored in the platform as well as configure security and access rules.

Application-Level Security

Role-based Permissions

BillingPlatform provides role-based access control down to the field level to ensure only authorized users can access sensitive customer data and audit logs. With the ability to define user-specific roles with read-write, read-only or no access, customers are able to ensure private customer data is only shared with those in the organization who absolutely need it. Customers can also manage access to objects and fields as well as control sharing settings for data visibility. Every change made is recorded in the system with a clear audit trail, ensuring confidential customer data is accessible only to the appropriate people.

Sharing Groups

Sharing groups within BillingPlatform allow customers to limit access to specific records of users based on defined filters. Users who are assigned to a sharing group will be limited to the data

defined for that group. This feature can be leveraged in customer and partner portals to extend application features without the risk of exposing the wrong information.

Approvals Framework

The approvals framework from BillingPlatform allows customers to apply a maker/checker policy for approving changes in the solution. A maker/checker policy requires two separate people to authorize a transaction—the first user (“maker”) creates a request to make a change, and the second user (“checker”) validates and approves the request.

Change requests can be made for custom entities, products, packages, pricing, contract rates and rate class changes. Customers can define which data changes require approvals to trigger and route requests to the appropriate approver and set approval chains as single or multi-level depending upon the significance of the request.

Auditing

BillingPlatform audit logs make auditing changes in the system easy and accessible. The audit logs centralize all user activity, allowing customers to track changes on any data element, including changes to configuration and data modifications to see what actions users performed, what changed and when. These changes are tracked at a field level enabling customers to see the most granular modifications to their data.

Application-Level Encryption

Application-level encryption is considered the most secure approach to enterprise data protection by going beyond the common step of securing data at rest to ensure that only authenticated users with the appropriate privileges can access sensitive data.

BillingPlatform addresses this by encrypting highly sensitive and user-defined data prior to storage, adhering to FIPS 140-2 encryption Level 2 and Level 3 standards.

All encryption and decryption occurs by means of encryption keys. Customers manage these keys directly, guaranteeing control over the level of access granted to their data.

Threat Detection

BillingPlatform offers a proactive threat detection service that continuously monitors for malicious activity and unauthorized behavior such as traffic patterns, account changes and workloads.

With data security a major concern for businesses of all sizes, BillingPlatform continually explores capabilities to enhance the security, compliance and auditability of the solution, from the foundational code level up through threat detection in the cloud infrastructure.

To learn more about how enterprise-level security can secure your operation, contact us.