White paper

Shipping & Mailing
Shipping Software & Systems

Pitney Bowes Shipping 360®Platform

Security-first, SaaS enterprise shipping and mailing technology platform.

Table of Contents

Shipping 360: SaaS platform for complete visibility and control of shipping and mailing across your enterprise

Introduction

The Shipping 360 platform is the secure SaaS foundation shared by our suite of applications that remove complexity from shipping and mailing. This cloud-based platform provides a common architecture for cloud security, scalability, and enterprise administration delivering complete visibility and control of shipping, mailing, and receiving operations across your enterprise.

Shipping 360 delivers the power of our SaaS shipping and mailing portfolio in a seamless enterprise experience:

01. **Shipping—** Simplify shipping across your entire enterprise with technology that enables employees to make smarter shipping decisions, while centralizing management of carriers and users.

02. **Mailing —** Print USPS® postage from anywhere without a postage meter, and simplify every step of preparing, tracking and managing USPS Certified Mail.

03. **Analytics —** Capture and organize every mailing and shipping expense into a single place for complete visibility with new insights and recommendations for cost control and efficiency improvement.

04. **Receiving —** Streamline receiving of inbound packages and parcels with full chain-of-custody visibility and control.

05. **Distribution —** Provide a secure and convenient way to deliver incoming packages and internal assets.

Architecture Overview and Characteristics

Shipping 360 is a cloud-based Pitney Bowes managed SaaS service that caters to businesses of all sizes. This service is offered alongside additional components and peripherals such as package scanners, label printers, mailing machines, scales, handheld devices, and smart lockers that seamlessly integrate with the cloud-based Shipping 360 platform.

Shipping 360 is available on the MacOS and Windows operating systems and runs on Google Chrome, Microsoft Edge and Safari.

Service Performance

Shipping 360 is designed and built ground up using modern cloud-native technologies. This enables the service to deliver a highly performant, reliable, and scalable service.

Scale and performance

Kubernetes forms the underlying technology platform for Shipping 360. The application uses a stateless microservices based architecture and leverages containerized deployments. The microservices rely on a database service that scales (up or down) automatically to meet the variable load. In summary, the autoscaling database and the containerized microservices combined provides a cost effective and flexible system that adjusts to varying client demands. This enables Shipping 360 to deliver on its throughput and performance commitments.

Reliability and availability

Every component within the Shipping 360 stack is designed and deployed as a redundant and highly available configuration.

01. Shipping 360 is hosted in two AWS regions (US-East and US-West) for US based clients. Within an AWS region, Shipping 360 service leverages the multi-AZs (availability zones) deployment model. Thus, the architecture offers a highly available service that is tolerant to single region outages.

02. Database service is hosted in three AWS regions (US-East, US-West and US-Central) and the data is seamlessly replicated across these regions to provide a highly available database that offers protection against single region failures. Additionally, the data is backed up following the best practices.

03. Infrastructure components such as firewalls, load balancers, routers, etc. are deployed in a highly available redundant configuration.

04. Application components are designed and deployed as containerized load-balanced multiple instances within the highly available Kubernetes cluster.

05. Shipping 360 system is continuously monitored using cloud native tools such as Prometheus to ensure system performance and availability. Realtime dashboards and alerting provide an up-to-the-minute operational view of the system.

06. Shipping 360 is a 24x7x365 service that provides an overall system availability of 99.9% on a yearly basis.

Security Overview

Pitney Bowes security-first strategy is built around defense in-depth and includes security policies and procedures, infrastructure controls, and secure application development and architectures.

- All public-facing services require at a minimum a TLS 1.2 based connection.
- Access to the services is protected using firewalls and API gateways.
- The Shipping 360 deployment model follows the established best practices for VPCs as well as for subnets (private and public) to restrict access to backend systems.
- Endpoint Detection and Response Solutions (EDR) are deployed and configured to detect and block suspicious behavior.
- Additional measures include centralized logging (such as AWS CloudTrail and AWS CloudWatch) and alerting, intrusion detection.
- Network access control, host-based firewalls and DDoS protection.
- Data is encrypted in transit as well as at rest using FIPS validated encryptors.
- The application development lifecycle is designed with an emphasis on information security.
- Pitney Bowes developers are trained in secure-coding best practices and every feature requires an intensive review before being released into production.
- To further ensure protection of your data, both internal staff and third-party experts regularly perform assessments of data privacy, data integrity and data availability.

The Shipping 360 Platform, as well as Pitney Bowes manufactured equipment, is independently pen (penetration) tested on an annual basis.

For clients wishing to use our locker solutions, clients can use cellular based connections in lieu of using the corporate network.

Amazon Web Service (AWS) Standards

Shipping 360 is hosted on secure and reliable AWS Cloud platform (Amazon Web Services).

For more information on AWS, visit: https://docs.aws.amazon.com/whitepapers/latest/aws-overview/securityand-compliance.html.

Secure Practices and Policies

Shipping 360 implements industry-standard defense and in-depth strategies and technologies to protect our customers' data.

The Pitney Bowes corporate policies and control frameworks are aligned with industry standards, such as NIST CSF and Center for Internet Security (CIS). This includes pragmatic policies, procedures, standards, and guidelines to support information security requirements, with a focus on the most critical assets. This enables Pitney Bowes to maximize efficiency and effectiveness by leveraging a common set of controls and policies to comply with many regulations.

Pitney Bowes operations and planning activities include security and business continuity considerations. Pitney Bowes' information security practices comply with numerous regulations and standards, including Payment Card Industry Data Security Standards (PCI-DSS) and Sarbanes-Oxley (SOX). Pitney Bowes undergoes numerous internal and external audits annually, including rigorous on-site information security audits by Verizon Business and IBM ISS, to ensure the appropriate security policies and controls are effective.

The SOC-2 framework is driven by NIST 800-53 Rev 5 standard. Data security is based upon a rigorous analysis and backed by the FIPS-199 Data Categorization process. Pitney Bowes received the SOC-2 type 2 report for Security, Availability and Confidentiality.

In addition, Pitney Bowes has implemented a robust Information Security Management System (ISMS) to safeguard sensitive information on the Shipping 360 Platform, which has achieved the globally recognized ISO 27001 certification. The scope covers the management of information and activities that support the development and release of these products.

Pitney Bowes Shipping 360 application- specific responsibilities:

01. Application security scans
02. Application penetration testing
03. AWS infrastructure security reviews
04. Application static-code analysis
05. Third Party and Open-Source Library vulnerability and license compliance
06. Intrusion detection at the infrastructure, operating system, and container levels.

Pitney Bowes Responsibility

The SaaS provider will be responsible for things under their control, such as physical infrastructure, environmental, and network infrastructure. It is our responsibility to:

- Monitor our platforms for bad or malicious use.
- Perform patch and vulnerability management.
- Ensure our system has failover and redundancy built in.
- Maintain system-level back-ups (which includes client's information).
- Notify you of any incidents we become aware of that affects your data.
- Operate within the law of the various jurisdictions we do business in.

Encryption

Encryption is used for data in transit using at a minimum TLS 1.2 - no communication between components or systems happens other than via HTTPS. This starts right at the load balancer, which rejects all unencrypted traffic before it can even access systems or applications. Within the platform data is encrypted from end-to-end including in the Kubernetes clusters. Data at rest is encrypted using FIPS Level 2 validated encryptors.

Security Monitoring

Pitney Bowes maintains an SOC that is manned 24x7x365 and continuously monitors the security and integrity of the platform. Pitney Bowes performs annual Pen Tests on all components of the Shipping 360 Platform. Furthermore, Pitney Bowes leverages our SIEM to monitor the security posture of the platform. Within the platform the perimeter is protected by multiple firewalls; the infrastructure is constantly scanned by industry standard infrastructure scanning tools; the operating systems are vulnerability scanned on a continuous basis; we leverage industry standard container vulnerability scanning. Pitney Bowes maintains intrusion detection tooling at the perimeter, within the infrastructure, within the operating system and finally within the container level ensuring that even the most advanced attack strategies will be ultimately detected and remediated.

Sign-in, and Single Sign-On Options and Role Based Access

Shipping 360 Platform offers two most widely used protocols for SSO (Single Sign -On) authentication - SAML (Security Assertion Markup Language) and OIDC (OpenID Connect). Shipping 360 Platform also offers MFA (MultiFactor Authentication). Email and SMS verification are two common methods used to enhance the security of accounts and the same are offered by 360® Platform.

Data Privacy and Residency

Data privacy, or access to your data, is controlled by several features and the cloud deployment model. At the core of data privacy is the segmentation of data. In addition, all public facing systems/applications are on a separate network from the backend database, ensuring optimal control over access.

Pitney Bowes Privacy Statement

Pitney Bowes is committed to respecting the privacy of our clients and users. This Privacy Statement is available on our corporate site at: https://www.pitneybowes.com/us/legal/privacy-statement.html describes how our websites, services, and products operate, and how we collect, use, and share information. This Privacy Statement applies to pitneybowes.com and Pitney Bowes websites, services, and products that collect data and display these terms, and that are owned and operated by Pitney Bowes and Pitney Bowes subsidiaries, collectively, "Pitney Bowes." Pitney Bowes websites, services, and products are referred to in this statement as "Sites." These terms do not apply to Pitney Bowes sites that do not display or link to this statement or that have their own privacy statements.

Purpose of Data Collection

Pitney Bowes Inc. and its controlled U.S. subsidiaries and affiliates receive personal information from the UK, EU/EEA, and Switzerland to enable us to provide goods and services to customers. We use the personal information for several purposes, including the following: order processing, delivery of products and services, payment processing, communication with customers and service providers, marketing and promoting products, product development and enhancement, and general maintenance and management of customer and user accounts. Pitney Bowes Inc. also receives employee personal information from the UK, EU, and Switzerland to provide human resources management and administration services, process employee benefits, and as required to fulfill other employment related legal and compliance obligations. All personal information transfers are covered by data transfer agreements that have been approved by the appropriate UK/EU data processing authority.

Data residency is based on the geography of the client or their desired provisioned locale. For US based customers, product data resides in the US. Clients located in Canada have their product data residing in Canada; EU clients' product data resides in the EU; Australia, New Zealand, and Japan clients' product data reside in the EU.

Pitney Bowes Shipping 360 is compliant with the General Data Protection Regulation (GDPR), which took effect on May 25, 2018, including the new GDPR Standard Contractual Clauses ("New EU SCC's").
Pitney Bowes has been subject to a Privacy Impact Assessment (PIA) and inter alia, the following requirements are met:

- Data Minimalization - defined fields (e.g., pre-populated lists/dropdowns, etc.) are used in favor of free-form text fields, and no more is collected/kept than is necessary to achieve a specific purpose. The user interface (UI) distinguishes between optional and required fields. Data to be transferred is limited to that which is minimally necessary to achieve the purpose of the transfer, and use of free-form text fields is avoided.

- Purpose Limitation - the purpose of every data element is identified prior to collection, the specific purpose for every data element is documented, and data is never collected to have "just in case."

- Data Accuracy - validation controls are in place to filter out old, inconsistent, incomplete, or inaccurate data.

- Storage Limitation - data inventory review and deletion or archiving processes are in place. Retention schedules and deletion/archiving triggers have been set.

Data Retention

The default Data Retention policy for Shipping 360 is 24(twenty-four) months. Should you require longer storage needs, arrangements can be made through your sales executive.

For Government Clients

There are two options available for government clients. There is a fully FedRAMP moderate certified platform available to State and Federal agencies. Further the commercial solution complies with all states' NASPO agreements.

FedRAMP Compliance

Available for the Federal government, FedRAMP is a government-wide program that promotes the adoption of secure cloud services across the federal government by providing a standardized approach to security and risk assessment for cloud technologies and federal agencies. Shipping 360 Platform's security status is located at https:// marketplace.fedramp.gov/#!/products.

Summary

Shipping 360 Platform is designed to provide a secure environment for your shipping, mailing, and receiving needs. Our cloud-based platform easily scales across your organization, seamlessly delivering capabilities to employees, like printing carrier shipping labels or postage, regardless of their location. Shipping 360 provides the data for better insights and visibility into opportunities for shipping and mailing improvements with the technology to implement and control changes that help you save time and money on everything shipping and mailing.

United States
3001 Summer Street
Stamford, CT 06926-0700

For more information, please contact your Pitney Bowes sales representative.

23SENDTECH05324_US