White paper

pitney bowes

Shipping & Mailing
Shipping Software & Systems

Shipping 360®

Security-first, SaaS-based sending, receiving, tracking and analytics platform.

Security Overview

The overall security strategy we've taken includes a combination of technical infrastructure controls and a strong security framework. Our security-first strategy is built around defence in depth and includes security policies and procedures, infrastructure controls, and secure application development and architectures.

To ensure the highest level of data protection, the Shipping 360 IT infrastructure includes a host of specific configurations. All public-facing production servers use HTTPS and TLS 1.2 to ensure the latest standards are enforced. In addition, these servers are on a separate network from the backend systems, including the database – enforcing yet another level of security for access to data.

Additional measures include centralised logging and alerting, intrusion detection, network access control, endpoint threat detection and response, host-based firewalls and DDoS protection. The application development lifecycle was 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.

The Shipping 360 Platform, as well as Pitney Bowes-manufactured equipment, is independently pen tested on an annual basis. This solution is IT-friendly, with access to the platform enabled entirely by a minimal set of static IP Addresses across port 443. If the client wishes to use SFTP to upload batch label files, they need only open port 22 with no additional IP authorisation.

For clients wishing to use our locker solutions, there is an option of using cellular lockers which do not need to be connected to the corporate network and will link directly back to cloud-based solution.

Shipping 360: Powering your Pitney Bowes sending, receiving, tracking and analytics solutions

Shipping 360 is a comprehensive platform that combines essential services necessary to manage the shipping, mailing, receiving, and tracking needs of your organisation. It also provides visibility into your postal and shipping spend.
It has several solutions or modules that include the following:

1. Sending
Print both postage and shipping labels for all your carriers with PitneyShip® Pro.

2. Tracking and Receiving with PitneyTrack®
Track inbound letters and parcels for full traceability across the shipping network, right up through the last 100 feet to the recipient.

3. Distribution
ParcelPoint® Smart Lockers, allow secure, contactless, 24/7 parcel and asset delivery, complete chain of custody tracking when integrated with PitneyTrack, and even temporary storage of personal belongings.

4. Analytics
PitneyAnalytics® allows you to gain valuable insight into all aspects of your shipping utilisation. Monitor spending, review inbound/outbound volume or view historical shipping patterns to better understand how and when you ship.

5. Visitor management
Pitney Bowes Smart Access Management® (SAM) extends our tracking capabilities to include guests to your facility. Please see separate SAM product document for further technical details.

Architecture

Shipping 360 is built with the enterprise in mind. Providing a cloud-based solution minimises the need for IT intervention to sustain the solution. Pitney Bowes takes care of upgrades, patches, and security. Pitney Bowes also provides a suite of on-site components such as package scanners, label printers, mailing machines, and scales that seamlessly integrate to the back-end services.

Amazon Web Services (AWS) provides highly secure data centres, which use state-of-the-art electronic and multi-factor access control systems, including:

- A highly secure facility with 24/7 guard protection, closed circuitry, alarmed doors with secure card-key access, biometric scanner, and restricted access to the data floor.
- Constantly monitored building and environmental control alarms.
- Server Locations

Network Defensibility
Several approaches are taken to protect against intruders, including:

- Redundant, fault-tolerant firewalls segment and secure traffic.
- A platform secured by a website certificate (HTTPS).
- Presentation layer services solely present in the demilitarised zone (DMZ).

Shared Responsibility for Deployment of Application in Amazon Web Services (AWS)
AWS' responsibilities:

1. Network security
2. Data-centre security
3. Enablement for disaster recovery (DR) and Business Continuity Plan (BCP)

Pitney Bowes' application-specific responsibilities:

1. Application security scans
2. Application penetration testing
3. AWS infrastructure security reviews
4. Application static-code analysis
5. Intrusion detection

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

Pitney Bowes' Responsibility for Application Deployment in AWS

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

- Provide and maintain SaaS platform.
- 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 breach we become aware of that affects your data.
- Operate within the law of the various jurisdictions we do business in.

Customer Responsibility for Deployment of Application in AWS

The customer is responsible for ensuring user access to the application is governed by the policy of the organisation and follows the principles of least privileges securing their data that is part of the SaaS offering. It is the responsibility of the customer to:

- Manage and protect the information within the account.
- Manage users and user accounts accessing the data, periodically review the list of users with access to your data and remove access from anyone who shouldn't have it.
- Operate within the law of the jurisdictions in which you do business.

Performance

Shipping 360 requires minimal, if any, IT resources to deploy and maintain performance across your organisation.

System performance is monitored to ensure optimal performance for our customers. As additional resources are needed, they are automatically brought online. The platform is built to handle tens of thousands of transactions per minute, and load testing at an excess of 150% anticipated peak demand is a standard component of the Shipping 360 development lifecycle.

Throughput

Shipping 360 was designed for customers of all sizes and throughput requirements. Whether you're processing a few packages per day as an office user or thousands per hour as part of your order fulfilment operation, Shipping 360 has throughput scales to manage it.

Scalability

Shipping 360 cloud infrastructure, along with the modules and solutions that reside on the platform, is both robust and secure. Redundant routers, cloud instances, database server clusters, and backup systems are used to ensure high availability and redundancy of systems.

The Shipping 360 stateless architecture allows for scalability and reliability using standard load balancers. The load balancers transparently distribute incoming requests among Shipping 360 cloud servers, with each request routed based on system availability to ensure consistent responses for our customers. As requirements for resources increase, additional cloud servers can easily be added to maintain availability and performance. The system is replicated both within a region and across geographic regions to ensure minimal latency and maximum availability of the platform.

Service Level Agreement (SLA)

The Shipping 360 cloud platform is built to provide 99.99% availability, excluding scheduled maintenance windows.

To ensure system availability and data integrity, both the databases and business logic are replicated within the same region, as well as being replicated across the United States, leveraging data centres on east coast and west coasts. Further, nightly backups are performed, allowing

us to restore to any point in time and ensuring no data loss or downtime.

Amazon Web Service (AWS) Standards

Shipping 360 is hosted by Amazon Web Services (AWS). The IT infrastructure that AWS provides is designed and managed in alignment with best security practices and is certified to a variety of IT Security standards, including SOC 1/SSAE 16/SAE 3402, SOC 2, SOC 3, FISMA, DIACAP and FedRAMP, PCI DSS Level 1, ISO 27001,ISO/IEC 27017:2015, ISO/IEC 27018:2014, ISO 9001, ITAR, and FIPS 140-2.

Secure Practices and Policies

Shipping 360 (and all other solutions on the platform) implements industry-standard defence and in-depth strategies and technologies to protect our customers' data. You can rest assured that as a tenant on the Shipping 360 platform, your data is secure and backed by rigorous policy, procedure, and practice. The remainder of this paper focuses on the steps you can take to ensure the security of your Shipping 360 deployment.

The Pitney Bowes corporate policies and control frameworks are aligned with industry standards, such as NIST Cybersecurity Framework (CSF) and Centre 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 us to maximise 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.

Login, Authentication Settings and Single Sign-On Options

Shipping 360 is powered by the Pitney Bowes Shipping 360 platform, which is a single login experience. Should a customer choose to, the Shipping 360 platform will integrate to your Pitney Bowes Smart Access Management® (SAM) solution, enabling the customer to maintain access controls via their corporate policies, as well as maintain password and authenticator compliance.

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 available on our corporate site at: 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 fulfil 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, as appropriate.

Data residency is based on the geography of the client. For US-based customers, data resides in the US. Clients located in Canada have their data residing in Canada; EU clients' data resides in the EU; Australia, New Zealand, and Japan clients' data resides in the EU. For Pitney Bowes Smart Access Management® (SAM), client data resides in London for UK customers and in Australia for EMEA customers.

Pitney Bowes is compliant with the European Union's General Data Protection Regulation (GDPR), which took effect on

May 25, 2018, including the new GDPR Standard Contractual Clauses ("New EU SCC's"). We are in the process of issuing similar amendments to our suppliers as the "old" Standard Contractual Clauses, which allow for the transfer of European Personal Data into the United States, expire on December 27 of this year. They need to be replaced with these new clauses that were issued in 2021. These are only required if we are processing any European Personal Data as part of our solutions with the client. This is managed by a global project team led by our privacy and data protection team, both for our internal processes and for our commercial offerings.

Pitney Bowes is compliant with the European Union's General Data Protection Regulation (GDPR), which took effect on May 25, 2018. This is managed by a global project team led by our privacy and data protection team, both for our internal processes and for our commercial offerings.

Shipping 360 has been subject to a Privacy Impact Assessment (PIA) and inter alia, the following requirements are met:

- **Data minimalisation –** defined fields (e.g., pre-populated lists/dropdowns, etc.) are used in favour 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

We make reasonable efforts to hold data for a rolling twenty-five (25) month period. Upon request, you may receive a file of your data for the twenty-five (25) months prior to the date of termination. The information will be provided in comma-separated value (.csv) format, along with attachments in their native format. This request must be made within thirty (30) days after the effective date of termination of a purchased services subscription, after which, we shall have no obligation to maintain or provide any of your data and may, unless legally prohibited, delete all your data in our possession or under our control. Should you require longer storage needs, arrangements can be made through your sales executive.

Profiles

A profile is like a role in many enterprise applications, except each user must have only one profile. Profiles help manage the permissions process, allowing you to assign users only the access they need.

Every profile includes one or more permissions that define what a user can do within Shipping 360. These authorisations can be set up globally for all users or defined based on user profiles or individual users.

Since profiles are the first step in determining authorisation rights, they should be reviewed closely. If custom profiles have been used, each profile should be

examined to determine which privileges are included and which users have been assigned to the profile.

Roles

Roles within Shipping 360 do not entirely relate to the traditional concept of a role in Role-Based Access Control (RBAC). Instead, a role is more closely tied to one of two types: User or Administrator. Within each role, you can control privileges and easily add or remove users, or customise permissions based on your business needs.

Encryption

Encryption is used for data in transit via HTTPS and TLS 1.2. This ensures that the latest industry standard controls are in place. No communication between components or systems happens other than via HTTPS. This starts right at the load balancer, which rejects all HTTP 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 140-2 validated encryptors. Wherever available the Shipping 360 platform leverages FIPS 140-2 compliant endpoints.

Security monitoring

Pitney Bowes maintains a 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 SendPro 360 platforms. Further we leverage our SIEM to monitor the security posture of the platform. Within the platform the perimeter is protected by multiple firewalls; the infrastructure 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

Recommendations

The Shipping 360 web app and client apps are validated on the Apple and Windows operating systems and runs on Google Chrome, Microsoft Edge, and Safari. It is always recommended that users have the latest version of the browser they are using, with the latest operating system updates and up-to-date virus software. No matter how secure our systems are in the cloud, it's equally important that the systems that access it are current and employ secure processes.

Disaster recovery

Shipping 360 is deployed from both a primary and secondary data centre, which are mirrored to each other using SQL Availability Groups. In addition, should there be a disaster, nightly backups ensure that we can restore your information to any point in time.

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 standardised approach to security and risk assessment for cloud technologies and federal agencies. Shipping 360 security status is located here.

Summary

Shipping 360 is designed to provide a secure environment for shipping and other transportation functions. Our cloud-based solution scales easily across your organisation, allowing employees to create carrier shipping labels and print postage, regardless of location. In addition, real-time data provides better insights and visibility into your shipping activity, helping you save time and money on every package you send.

United Kingdom
Langlands House
130 Sandringham Avenue
Harlow
CM19 5QA
0800 840 0001
pitneybowes.com/uk

Australia
Level 1, 68 Waterloo Road
Macquarie Park NSW 2113
13 23 63
pitneybowes.com/au

New Zealand
Building B, Unit 2 & 3
72 Apollo Drive
Rosedale
Auckland 0632
0800 748 639
pitneybowes.com/nz

India
Unit No 015
Ground floor
Time Tower Building
M G Road Gurgaon
Haryana – 122002
pitneybowes.com/in

23-SENDTECH-02943