



**Postbearbeitung und Versand**

Versandsoftware & Systeme

# Shipping 360<sup>®</sup>

Sicherheit steht an erster Stelle; auf SaaS basierende Plattform für das Senden, Empfangen, Verfolgen und Analysieren.



---

## Sicherheitsübersicht

Die Gesamtsicherheitsstrategie, die wir verfolgt haben, umfasst eine Kombination aus technischen Infrastrukturkontrollen und einem starken Sicherheitsrahmen. Unsere sicherheitsorientierte Strategie basiert auf einer Verteidigung in der Tiefe und umfasst Sicherheitsrichtlinien und -verfahren, Infrastrukturkontrollen sowie sichere Anwendungs- und Architektur-Entwicklung.

Um das höchste Maß an Datenschutz sicherzustellen, umfasst die IT-Infrastruktur von Shipping 360 eine Vielzahl spezifischer Konfigurationen. Alle öffentlich zugänglichen Produktionsserver verwenden HTTPS und TLS 1.2, um die neuesten Standards durchzusetzen. Darüber hinaus befinden sich diese Server in einem separaten Netzwerk von den Backend-Systemen, einschließlich der Datenbank, was eine weitere Sicherheitsebene für den Zugriff auf Daten gewährleistet.

Zu den zusätzlichen Maßnahmen gehören zentrales Protokollieren und Alarmieren, Eindringungserkennung, Netzwerkzugriffskontrolle, Endpunkterkennung und -reaktion auf Bedrohungen, hostbasierte Firewalls und DDoS-Schutz. Der Anwendungs-Entwicklungslebenszyklus wurde mit Schwerpunkt auf Informationssicherheit konzipiert. Die Entwickler von Pitney Bowes sind in bewährten Praktiken des sicheren Codierens geschult und jede Funktion erfordert eine intensive Überprüfung, bevor sie in die Produktion übernommen wird. Um den Schutz Ihrer Daten weiter zu gewährleisten, führen sowohl interne Mitarbeiter als auch externe Experten regelmäßig Bewertungen durch.

Die Shipping 360 Plattform sowie von Pitney Bowes hergestellte Ausrüstung werden unabhängig auf Penetration getestet, und zwar auf jährlicher Basis. Diese Lösung ist IT-freundlich, mit Zugriff auf die Plattform, der ausschließlich durch eine minimale Anzahl von statischen IP-Adressen über Port 443 ermöglicht wird. Wenn der Kunde SFTP verwenden möchte, um Stapel-Labeldateien hochzuladen, müssen sie nur Port 22 ohne zusätzliche IP-Autorisierung öffnen.

Für Kunden, die unsere Schließfachlösungen nutzen möchten, besteht die Möglichkeit, zellulare Schließfächer zu verwenden, die nicht mit dem Unternehmensnetzwerk verbunden sein müssen und direkt mit der Cloud-Lösung verknüpft werden.

## Shipping 360: Unterstützung Ihrer Pitney Bowes Lösungen für Senden, Empfangen, Verfolgen und Analysieren

**Shipping 360 ist eine umfassende Plattform, die die wesentlichen Dienstleistungen kombiniert, die erforderlich sind, um die Versand-, Post-, Empfangs- und Tracking-Bedürfnisse Ihrer Organisation zu verwalten. Es bietet auch Einblick in Ihre Ausgaben für Post und Versand.**

Es hat mehrere Lösungen oder Module, die Folgendes beinhalten:

### 1. Senden

Drucken Sie sowohl Porto- als auch Versandetiketten für alle Ihre Frachtführer mit PitneyShip® Pro.

### 2. Verfolgung und Empfang mit PitneyTrack®

Verfolgen Sie eingehende Briefe und Pakete für eine vollständige Rückverfolgbarkeit im gesamten Versandnetzwerk, bis hin zum Empfänger.

### 3. Verteilung

PitneyLockers ermöglichen sichere, kontaktlose, rund um die Uhr mögliche Paketzustellung, vollständige Rückverfolgung der Besitzkette bei Integration mit PitneyTrack, und sogar vorübergehende Lagerung persönlicher Gegenstände.

### 4. Analytics

PitneyAnalytics® ermöglicht es Ihnen, wertvolle Einblicke in alle Aspekte Ihrer Versandnutzung zu gewinnen. Überwachen Sie die Ausgaben, überprüfen Sie die eingehenden/ausgehenden Versandmengen oder betrachten Sie historische Versandmuster, um besser zu verstehen, wie und wann Sie versenden.

### 5. Besuchermanagement

Pitney Bowes Smart Access Management® (SAM) erweitert unsere Tracking-Fähigkeiten, um auch Gäste in Ihrem Unternehmen einzuschließen. Bitte beachten Sie das separate SAM-Produktdokument für weitere technische Details.

## Architektur

Shipping 360 wurde als Unternehmenslösung entwickelt. Die Bereitstellung einer cloudbasierten Lösung minimiert den Bedarf an IT-Unterstützung.

Pitney Bowes kümmert sich um Upgrades, Patches und Sicherheit. Pitney Bowes bietet auch eine Reihe von Vor-Ort-Komponenten wie Paketscanner, Etikettendrucker, Frankiermaschinen und Waagen, die nahtlos in die Back-End-Services integriert sind.

Amazon Web Services (AWS) bietet hochsichere Rechenzentren, die modernste elektronische und mehrstufige Zugangskontrollsysteme verwenden, einschließlich:

- Ein hochsicherer Standort mit 24/7-Wachschutz, geschlossener Schaltung, alarmierten Türen mit sicherem Kartenzugang, biometrischem Scanner und eingeschränktem Zugang zum Datenraum.
- Ständig überwachte Gebäude- und Umweltkontrollalarme.
- Serverstandorte

### Netzwerksicherheit

Es werden mehrere Ansätze verfolgt, um sich gegen Eindringlinge zu schützen, darunter:

- Redundante, fehlertolerante Firewalls segmentieren und sichern den Datenverkehr.
- Eine Plattform, die durch ein Website-Zertifikat (HTTPS) gesichert ist.
- Präsentationsschichtdienste ausschließlich in der entmilitarisierten Zone (DMZ) vorhanden.

### Gemeinsame Verantwortung für die Bereitstellung von Anwendungen in Amazon Web Services (AWS)

#### AWS-Verantwortlichkeiten:

1. Netzwerksicherheit
2. Rechenzentrumsicherheit
3. Unterstützung für Notfallwiederherstellung und Geschäftskontinuitätsplan

### Anwendungsspezifische Verantwortlichkeiten von Pitney Bowes:

1. Anwendungssicherheitsscans
2. Anwendungspenetrationstests
3. AWS-Infrastruktursicherheitsüberprüfungen
4. Statische Codeanalyse der Anwendung
5. Eindringungserkennung

Für weitere Informationen zu AWS besuchen Sie: [docs.aws.amazon.com/whitepapers/latest/aws-overview/security-and-compliance.html](https://docs.aws.amazon.com/whitepapers/latest/aws-overview/security-and-compliance.html)

### Verantwortung von Pitney Bowes für die Bereitstellung von Anwendungen in AWS

Der SaaS-Anbieter ist für Dinge verantwortlich, die unter ihrer Kontrolle stehen, wie physische Infrastruktur, Umwelt- und Netzwerkinfrastruktur. Es ist unsere Verantwortung,:

- Bereitstellen und Warten der SaaS-Plattform.
- Überwachen unserer Plattformen auf schlechte oder böswillige Nutzung.
- Patch- und Schwachstellenmanagement durchführen.
- Stellen Sie sicher, dass unser System Failover und Redundanz eingebaut hat.
- Systemweite Backups (einschließlich der Informationen des Kunden) aufrechterhalten.
- Sie über jede Verletzung informieren, von der wir erfahren, die Ihre Daten betrifft.
- Innerhalb des Gesetzes der verschiedenen Rechtsgebiete operieren, in denen wir Geschäfte tätigen.

### Kundenverantwortung für die Bereitstellung der Anwendung in AWS

Der Kunde ist dafür verantwortlich, sicherzustellen, dass der Benutzerzugriff auf die Anwendung durch die Richtlinie der Organisation geregelt wird und den Grundsätzen der minimalen Berechtigungen folgt, um ihre Daten zu sichern, die Teil des SaaS-Angebots sind. Es ist die Verantwortung des Kunden,:

- Die Informationen im Konto verwalten und schützen.
- Benutzer und Benutzerkonten verwalten, die auf die Daten zugreifen, regelmäßig die Liste der Benutzer mit Zugriff auf Ihre Daten überprüfen und den Zugriff von Personen entfernen, die ihn nicht haben sollten.
- Innerhalb des Gesetzes der Rechtsgebiete operieren, in denen Sie Geschäfte tätigen.

## Performance

Für den Einsatz und die Aufrechterhaltung der Leistung in Ihrer Organisation sind minimale oder keine IT-Ressourcen erforderlich.

Die Systemleistung wird überwacht, um eine optimale Leistung für unsere Kunden sicherzustellen. Wenn zusätzliche Ressourcen benötigt werden, werden sie automatisch online gebracht. Die Plattform ist darauf ausgelegt, Zehntausende von Transaktionen pro Minute zu verarbeiten, und Lasttests mit einer Überlastung von 150% der erwarteten Spitzenlast sind ein Standardbestandteil des Entwicklungslebenszyklus von Shipping 360.

### Durchsatz

Shipping 360 wurde für Kunden aller Größen und Durchsatzanforderungen entwickelt. Ob Sie als Büronutzer nur wenige Pakete pro Tag verarbeiten oder als Teil Ihres Auftragsabwicklungsbetriebs Tausende pro Stunde, Shipping 360 verfügt über Durchsatzskalen, um dies zu verwalten.

### Skalierbarkeit

Die Cloud-Infrastruktur von Shipping 360 sowie die Module und Lösungen, die auf der Plattform vorhanden sind, sind robust und sicher. Redundante Router, Cloud-Instanzen, Datenbankserver-Cluster und Backup-Systeme werden verwendet, um eine hohe Verfügbarkeit und Redundanz der Systeme sicherzustellen.

Die zustandslose Architektur von Shipping 360 ermöglicht Skalierbarkeit und Zuverlässigkeit unter Verwendung von Standard-Lastenausgleichern. Die Lastenausgleicher verteilen eingehende Anfragen transparent zwischen den Cloud-Servern von Shipping 360, wobei jede Anfrage basierend auf der Systemverfügbarkeit geroutet wird, um konsistente Antworten für unsere Kunden sicherzustellen. Mit steigenden Anforderungen an Ressourcen können zusätzliche Cloud-Server problemlos hinzugefügt werden, um Verfügbarkeit und Leistung aufrechtzuerhalten. Das System wird sowohl innerhalb einer Region als auch über geografische Regionen hinweg repliziert, um minimale Latenzzeiten und maximale Verfügbarkeit der Plattform sicherzustellen.

### Service-Level-Vereinbarung (SLA)

Die Cloud-Plattform von Shipping 360 ist darauf ausgelegt, eine Verfügbarkeit von 99,99 % zu bieten, mit

Ausnahme von geplanten Wartungsfenstern.

Um die Systemverfügbarkeit und Datenintegrität sicherzustellen, werden sowohl die Datenbanken als auch die Geschäftslogik innerhalb derselben Region repliziert, sowie über die Vereinigten Staaten hinweg repliziert, wobei Datenzentren an der Ost- und Westküste genutzt werden. Darüber hinaus werden nächtliche Backups durchgeführt, die es uns ermöglichen, zu jedem Zeitpunkt wiederherzustellen und keine Datenverluste oder Ausfallzeiten zu gewährleisten.

### Amazon Web Service (AWS) Standards

Shipping 360 wird von Amazon Web Services (AWS) gehostet. Die IT-Infrastruktur, die AWS bereitstellt, ist nach den besten Sicherheitspraktiken konzipiert und verwaltet und ist nach einer Vielzahl von IT-Sicherheitsstandards zertifiziert, einschließlich SOC 1/SSAE 16/SAE 3402, SOC 2, SOC 3, FISMA, DIACAP und FedRAMP, PCI DSS Level 1, ISO 27001, ISO/IEC 27017:2015, ISO/IEC 27018:2014, ISO 9001, ITAR und FIPS 140-2.

### Sichere Praktiken und Richtlinien

Shipping 360 (und alle anderen Lösungen auf der Plattform) implementiert branchenübliche Verteidigungs- und Tiefenstrategien und -technologien zum Schutz der Daten unserer Kunden. Sie können sicher sein, dass Ihre Daten als Mieter auf der Shipping 360-Plattform sicher sind und durch strenge Richtlinien, Verfahren und Praktiken unterstützt werden. Der Rest dieses Papiers konzentriert sich auf die Schritte, die Sie unternehmen können, um die Sicherheit Ihrer Shipping 360-Bereitstellung zu gewährleisten.

Die Unternehmensrichtlinien und Kontrollrahmen von Pitney Bowes sind mit Branchenstandards wie dem NIST Cybersecurity Framework (CSF) und dem Centre for Internet Security (CIS) abgestimmt. Dies umfasst pragmatische Richtlinien, Verfahren, Standards und Leitlinien zur Unterstützung von Informationssicherheitsanforderungen mit einem Schwerpunkt auf den wichtigsten Vermögenswerten. Dies ermöglicht es uns, Effizienz und Effektivität zu maximieren, indem wir einen gemeinsamen Satz von Kontrollen und Richtlinien nutzen, um mit vielen Vorschriften konform zu sein.

Die Betriebs- und Planungsaktivitäten von Pitney Bowes umfassen Sicherheits- und

Geschäftskontinuitätsüberlegungen. Die Informationssicherheitspraktiken von Pitney Bowes entsprechen zahlreichen Vorschriften und Standards, einschließlich der Payment Card Industry Data Security Standards (PCI-DSS) und Sarbanes-Oxley (SOX). Pitney Bowes unterzieht sich jährlich zahlreichen internen und externen Prüfungen, einschließlich strenger Vor-Ort-Prüfungen der Informationssicherheit durch Verizon Business und IBM ISS, um sicherzustellen, dass die entsprechenden Sicherheitsrichtlinien und -kontrollen wirksam sind.

## Anmeldung, Authentifizierungseinstellungen und Single Sign-On-Optionen

Shipping 360 wird von der Pitney Bowes Shipping 360-Plattform betrieben, die ein einheitliches Anmeldeerlebnis bietet. Sollte ein Kunde sich dafür entscheiden, wird die Shipping 360-Plattform in Ihre Pitney Bowes Smart Access Management® (SAM)-Lösung integriert, sodass der Kunde den Zugriff über ihre Unternehmensrichtlinien steuern und die Passwort- und Authentifizierungskonformität aufrechterhalten kann.

## Datenschutz und Residenz

Der Datenschutz oder der Zugriff auf Ihre Daten wird durch mehrere Funktionen und das Cloud-Bereitstellungsmodell kontrolliert. Im Kern des Datenschutzes steht die Segmentierung von Daten. Darüber hinaus befinden sich alle öffentlich zugänglichen Systeme/Anwendungen in einem separaten Netzwerk vom Backend-Datenbank, um eine optimale Kontrolle über den Zugriff sicherzustellen.

### Datenschutzerklärung von Pitney Bowes

Pitney Bowes verpflichtet sich, die Privatsphäre unserer Kunden und Benutzer zu respektieren. Diese Datenschutzerklärung, die auf unserer Unternehmenswebsite unter [pitneybowes.com/us/legal/privacy-statement.html](https://pitneybowes.com/us/legal/privacy-statement.html) verfügbar ist, beschreibt, wie unsere Websites, Dienste und Produkte funktionieren und wie wir Informationen sammeln, verwenden und teilen. Diese Datenschutzerklärung gilt für pitneybowes.com und die Websites, Dienste und Produkte von Pitney Bowes, die Daten sammeln und diese Bedingungen anzeigen und die von Pitney Bowes und den Tochtergesellschaften von Pitney Bowes im Besitz und betrieben werden, genannt „Pitney Bowes“. In dieser Erklärung werden die Websites, Dienste und Produkte von Pitney Bowes als „Sites“ bezeichnet. Diese Bedingungen gelten nicht für Pitney Bowes-Websites, die diese Erklärung nicht anzeigen oder verlinken oder die ihre eigenen Datenschutzerklärungen haben.

### Zweck der Datensammlung

Pitney Bowes Inc. und seine kontrollierten US-Tochtergesellschaften und verbundenen Unternehmen erhalten personenbezogene Informationen aus dem Vereinigten Königreich, der EU/EEA und der Schweiz, um

uns zu ermöglichen, Waren und Dienstleistungen für Kunden bereitzustellen. Wir verwenden die personenbezogenen Informationen für verschiedene Zwecke, einschließlich der folgenden: Auftragsabwicklung, Lieferung von Produkten und Dienstleistungen, Zahlungsabwicklung, Kommunikation mit Kunden und Dienstleistern, Marketing und Werbung für Produkte, Produktentwicklung und -verbesserung sowie allgemeine Wartung und Verwaltung von Kunden- und Benutzerkonten. Pitney Bowes Inc. erhält auch Mitarbeiterpersonaldaten aus dem Vereinigten Königreich, der EU und der Schweiz, um Personalmanagement- und Verwaltungsdienstleistungen bereitzustellen, Mitarbeiterleistungen zu verarbeiten und wie erforderlich andere arbeitsbezogene rechtliche und Compliance-Verpflichtungen zu erfüllen. Alle Übertragungen persönlicher Informationen werden durch Datenübertragungsvereinbarungen abgedeckt, die von der entsprechenden britischen/europäischen Datenverarbeitungsbehörde genehmigt wurden, wie es angemessen ist.

Die Datenresidenz basiert auf der Geografie des Kunden. Für Kunden mit Sitz in den USA befinden sich die Daten in den USA. Kunden in Kanada haben ihre Daten in Kanada; EU-Kunden haben ihre Daten in der EU; Daten von Kunden aus Australien, Neuseeland und Japan befinden sich in der EU. Für Pitney Bowes Smart Access Management® (SAM) befinden sich die Kundendaten in London für Kunden aus dem Vereinigten Königreich und in Australien für Kunden aus der EMEA-Region.

Pitney Bowes entspricht der Datenschutz-Grundverordnung (DSGVO) der Europäischen Union, die in Kraft getreten ist.

25. Mai 2018, einschließlich der neuen Standardvertragsklauseln der DSGVO ("Neue EU-SCC"). Wir sind dabei, ähnliche Änderungen an unsere Lieferanten herauszugeben, da die "alten" Standardvertragsklauseln, die die Übertragung europäischer personenbezogener Daten in die Vereinigten Staaten ermöglichen, am 27. Dezember dieses Jahres auslaufen. Sie müssen durch diese neuen Klauseln ersetzt werden, die im Jahr 2021 herausgegeben wurden. Diese sind nur erforderlich, wenn wir im Rahmen unserer Lösungen mit dem Kunden personenbezogene Daten aus Europa verarbeiten. Dies wird von einem globalen Projektteam unter der Leitung unseres Datenschutz- und Datensicherheitsteams

verwaltet, sowohl für unsere internen Prozesse als auch für unsere kommerziellen Angebote.

Pitney Bowes entspricht der Datenschutz-Grundverordnung (DSGVO) der Europäischen Union, die am 25. Mai 2018 in Kraft getreten ist. Dies wird von einem globalen Projektteam unter der Leitung unseres Datenschutz- und Datensicherheitsteams verwaltet, sowohl für unsere internen Prozesse als auch für unsere kommerziellen Angebote.

Shipping 360 wurde einer Datenschutz-Folgenabschätzung (PIA) unterzogen und unter anderem werden die folgenden Anforderungen erfüllt:

- **Datenminimierung** – definierte Felder (z.B. vorab ausgefüllte Listen/Dropdowns usw.) werden zugunsten von Freitextfeldern verwendet, und es wird nicht mehr gesammelt/aufbewahrt als für einen bestimmten Zweck erforderlich ist. Die Benutzeroberfläche (UI) unterscheidet zwischen optionalen und erforderlichen Feldern.

Die zu übertragenden Daten sind auf das Mindestmaß beschränkt, das zur Erreichung des Übertragungszwecks erforderlich ist, und die Verwendung von Freitextfeldern wird vermieden.

- **Zweckbindung** - Der Zweck jedes Datenelements wird vor der Erfassung identifiziert, der spezifische Zweck jedes Datenelements wird dokumentiert, und Daten werden niemals „nur für den Fall“ gesammelt.
- **Datenrichtigkeit** - Validierungssteuerelemente sind vorhanden, um alte, inkonsistente, unvollständige oder ungenaue Daten herauszufiltern.
- **Speicherbegrenzung** - Dateninventurüberprüfung und Lösch- oder Archivierungsprozesse sind vorhanden. Aufbewahrungsfristen und Lösch-/Archivierungsauslöser wurden festgelegt.

## Datenverwaltung

Wir bemühen uns, Daten für einen rollierenden Zeitraum von fünfundzwanzig (25) Monaten zu speichern. Auf Anfrage erhalten Sie eine Datei mit Ihren Daten für die fünfundzwanzig (25) Monate vor dem Beendigungsdatum. Die Informationen werden im CSV-Format bereitgestellt, zusammen mit Anhängen im



jeweiligen Format. Dieses Anliegen muss innerhalb von dreißig (30) Tagen nach dem Wirksamkeitsdatum der Kündigung eines gekauften Dienstleistungsabonnements gestellt werden. Danach sind wir nicht verpflichtet, Ihre Daten zu speichern oder bereitzustellen, und können, sofern nicht gesetzlich untersagt, alle Ihre Daten in unserem Besitz oder unter unserer Kontrolle löschen. Wenn Sie längere Speicheranforderungen haben, können Vereinbarungen über Ihren Vertriebsleiter getroffen werden.

## Profile

Ein Profil ist wie eine Rolle in vielen Unternehmensanwendungen, außer dass jeder Benutzer nur ein Profil haben darf. Profile helfen bei der Verwaltung des Berechtigungsprozesses und ermöglichen es Ihnen, Benutzern nur den Zugriff zuzuweisen, den sie benötigen.

Jedes Profil enthält eine oder mehrere Berechtigungen, die festlegen, was ein Benutzer innerhalb von Shipping 360 tun kann. Diese Berechtigungen können global für alle Benutzer eingerichtet oder basierend auf Benutzerprofilen oder einzelnen Benutzern definiert werden.

Da Profile der erste Schritt zur Bestimmung von Autorisierungsrechten sind, sollten sie sorgfältig überprüft werden.

Wenn benutzerdefinierte Profile verwendet wurden, sollte jedes Profil überprüft werden, um festzustellen, welche Privilegien enthalten sind und welche Benutzer dem Profil zugewiesen wurden.

### Rollen

Rollen innerhalb von Shipping 360 beziehen sich nicht vollständig auf das traditionelle Konzept einer Rolle im rollenbasierten Zugriffskontrollsystem (RBAC). Stattdessen ist eine Rolle enger mit einem der beiden Typen verbunden: Benutzer oder Administrator. In jeder Rolle können Sie Berechtigungen steuern und Benutzer einfach hinzufügen oder entfernen oder Berechtigungen basierend auf Ihren Geschäftsanforderungen anpassen.

## Verschlüsselung

Verschlüsselung wird für Daten im Transit über HTTPS und TLS 1.2 verwendet. Dies stellt sicher, dass die neuesten branchenüblichen Kontrollen vorhanden sind. Es findet

keine Kommunikation zwischen Komponenten oder Systemen statt, außer über HTTPS. Dies beginnt direkt am Lastenausgleicher, der den gesamten HTTP-Verkehr ablehnt, bevor er überhaupt auf Systeme oder Anwendungen zugreifen kann. In der Plattform werden Daten von Ende zu Ende verschlüsselt, einschließlich in den Kubernetes-Clustern. Daten im Ruhezustand werden mit FIPS 140-2 validierten Verschlüsselungsgeräten verschlüsselt. Wo immer verfügbar, nutzt die Shipping 360-Plattform FIPS 140-2-konforme Endpunkte.

## Sicherheitsüberwachung

Pitney Bowes betreibt ein SOC, das rund um die Uhr besetzt ist und die Sicherheit und Integrität der Plattform kontinuierlich überwacht. Pitney Bowes führt jährliche Penetrationstests an allen Komponenten der SendPro 360-Plattformen durch. Darüber hinaus nutzen wir unser SIEM, um die Sicherheitslage der Plattform zu überwachen. In der Plattform wird der Perimeter durch mehrere Firewalls geschützt; die Infrastruktur wird kontinuierlich von branchenüblichen Infrastruktur-Scanning-Tools gescannt; die Betriebssysteme werden kontinuierlich auf Schwachstellen gescannt; wir nutzen branchenübliche Container-Schwachstellen-Scans. Pitney Bowes pflegt Eindringungserkennungswerkzeuge am Perimeter, innerhalb der Infrastruktur, innerhalb des Betriebssystems und schließlich auf Container-Ebene, um sicherzustellen, dass selbst die fortschrittlichsten Angriffsstrategien letztendlich erkannt und behoben werden.

## Empfehlungen

Die Shipping 360 Web-App und Client-Apps werden auf den Betriebssystemen Apple und Windows validiert und laufen auf Google Chrome, Microsoft Edge und Safari. Es wird immer empfohlen, dass Benutzer die neueste Version des von ihnen verwendeten Browsers mit den neuesten Betriebssystemupdates und aktueller Virensoftware haben. Unabhängig davon, wie sicher unsere Systeme in der Cloud sind, ist es ebenso wichtig, dass die Systeme, die darauf zugreifen, aktuell sind und sichere Prozesse anwenden.

## Notfallwiederherstellung

Shipping 360 wird sowohl aus einem primären als auch aus einem sekundären Rechenzentrum bereitgestellt, die mithilfe von SQL-Verfügbarkeitsgruppen gespiegelt sind.



Darüber hinaus stellen nächtliche Backups sicher, dass wir im Falle eines Disasters Ihre Informationen zu jedem Zeitpunkt wiederherstellen können.

## Für Regierungskunden

Es stehen zwei Optionen für Regierungskunden zur Verfügung. Es steht eine vollständig FedRAMP-mäßig zertifizierte Plattform für Bundes- und Landesbehörden zur Verfügung. Darüber hinaus entspricht die kommerzielle Lösung allen NASPO-Vereinbarungen der Bundesstaaten.

### FedRAMP-Konformität

Für die Bundesregierung verfügbar, ist FedRAMP ein Regierungsprogramm, das die Annahme sicherer Cloud-Dienste in der gesamten Bundesregierung fördert, indem es einen standardisierten Ansatz für Sicherheits- und Risikobewertung für Cloud-Technologien und Bundesbehörden bereitstellt. Der Sicherheitsstatus von Shipping 360 befindet sich [hier](#).

## Zusammenfassung

Shipping 360 ist darauf ausgelegt, eine sichere Umgebung für den Versand und andere Transportfunktionen bereitzustellen. Unsere cloudbasierte Lösung skaliert problemlos in Ihrer Organisation und ermöglicht es den Mitarbeitern, Frachtversandetiketten zu erstellen und Porto zu drucken, unabhängig vom Standort. Darüber hinaus bieten Echtzeitdaten bessere Einblicke und Sichtbarkeit in Ihre Versandaktivitäten, was Ihnen hilft, Zeit und Geld bei jedem versendeten Paket zu sparen.

### Deutschland

Poststr. 4-6  
64293 Darmstadt  
contact.de@pb.com  
06151 5202 0  
pitneybowes.de

### Australien

Ebene 1, 68 Waterloo Road  
Macquarie Park NSW 2113  
13 23 63

### Neuseeland

Gebäude B, Einheit 2 & 3  
72 Apollo Drive  
Rosedale  
Auckland 0632  
0800 748 639  
pitneybowes.com/nz

### Indien

Einheit Nr. 015  
Erdgeschoss  
Time Tower Gebäude  
M G Road Gurgaon  
Haryana - 122002  
pitneybowes.com/in