White paper

pitney bowes

Shipping & Mailing
Inbound Package Management

Maximise your data security.

SendSuite Tracking Online from Pitney Bowes is a SaaS-based solution that streamlines the logging, tracking and managing of all packages and mail. With it, you'll gain better visibility on what comes into your organisation – and where it goes – making the entire process more accurate and efficient.

A superior solution with a high degree of security and privacy. SendSuite Tracking Online is offered as a hosted business application. More and more businesses are using hosted versus on premise software. Pitney Bowes offers hosting of this application in order to:

- Simplify deployment.
- Free customer IT resources to focus on core business objectives.
- Provide worry-free implementation.

White paper features

- Understanding the benefits of our hosted offering
- A comprehensive introduction to the inherent security and privacy features of SendSuite Tracking Online.
- An overview of the management and monitoring components of the hosting solution

Why choose a Pitney Bowes hosting service:

SendSuite Tracking Online provides a beneficial business case on its own. This is enhanced further by its ability to reduce in-house IT resource and mitigate against budget constraints that may exist.

- Corporate policy may call for applications to be outsourced or to use software as a service (SaaS).
- Corporate firewall restrictions and/or other security make external hosting the preferred option.

Security architecture

The SendSuite Tracking Online security architecture includes both design and maintenance of a secure platform. It has been created to protect the privacy of direct customers and all data. The application's features implement stringent Pitney Bowes security and privacy policies.

SendSuite Tracking Online is deployed on dedicated Amazon Web Services (AWS) instances. It includes encryption in transit and at rest via EBS volume encryption and SSL communication between the application servers and the database. SSL certificates are deployed on Amazon's load balancer layer, and all logs are stored with the Pitney Bowes data retention policies applied. The application servers have hardened Operating Systems to eliminate any potential vulnerabilities.

Platform security

Hosting facility security and access

Pitney Bowes SendSuite Tracking Online is hosted in world-class hosting facilities. These facilities are managed by Amazon Web Services (AWS) located in Ireland for the European and International deployments.

The IT infrastructure that AWS provides is designed and managed in alignment with best security practices and meets 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 9001
- ITAR
- FIPS 140-2

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 24x7 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

Network defensibility

A number of approaches are taken to protect against intruders, including:

- Redundant, fault-tolerant firewalls segment and secure traffic
- SSL Certificate (HTTPS)
- Presentation layer services are solely present in the DMZ

Pre-installation assessment

Before being accepted into production, all systems undergo a thorough security vulnerability assessment. If required, an executive summary of the Application Security assessment can be shared.

Shared responsibility for deployment of application in AWS

AWS responsibilities:

01. Network security
02. Data Center security
03. Enablement for DR and BCP

Application-specific responsibilities of Pitney Bowes:

01. VA scans of application to be deployed
02. Pen testing of the application
03. Security reviews of the AWS Infrastructure deployed
04. Static code analysis of the application code

For more information on SSTO, contact your Pitney Bowes technical consultant.

Application security

Pitney Bowes incorporates security into its platform development processes at all stages. From the software design and architecture, to hosting architecture, to post-release support; security considerations are included.

From a requirements perspective, SendSuite Tracking Online incorporated guidelines from ENISA and FFIEC. These were translated into product development and deployment requirements.

The security architecture and design was reviewed to ensure that appropriate security controls would be applied to the system with consideration to these specifications. This includes controls for data at rest as well as data in transit.

Continuous testing

Periodic penetration testing
Third party penetration testing is conducted on an annual basis to make sure security vulnerabilities are remediated. All input and output pathways are exercised along with a focus on data security.

Continuous assessment of operating system vulnerabilities
All systems are routinely scanned to detect and protect against viruses or other forms of intrusion. Critical operating system updates are also applied to ensure protection against any recent security vulnerability.

Vulnerabilities are patched using automated deployments and upgrades throughout the cloud infrastructure across the entire environment, including:

- Connectivity
- Business continuity planning
- Business logic
- Upgrade strategy

Defensibility
Pitney Bowes follows industry standard best practices for software defensibility. All computers within Pitney Bowes are protected by enterprise-level virus scanning software. The following lists some of the best practices followed by Pitney Bowes when developing software solutions:

- Sensitive communication to servers utilize TLS
- Security awareness training for software developers
- Automated penetration testing and code analysis
- Design and peer reviews with code review
- Ethical hacker training
- Digitally signed software

HTTPS and secure FTP
Pitney Bowes offer HTTPS for the secure transfer of files to/from your users to our hosted data centres.

Employee and Staff Security

Authentication

The authentication methodology utilized for SendSuite Tracking Online is where user IDs are stored in the application database to coincide with the customer's specific MyPB account. Passwords are never transmitted or stored in plain text.

Health and security status monitoring

CPU utilisation, available disk space, hardware component failure, network availability, application availability and more are monitored constantly using the various tools described below. The SendSuite Tracking Online solution uses consolidated logging and analytics to look for security anomalies and generate real-time alerts to the support team.

Amazon CloudWatch
Amazon CloudWatch provides server level monitoring of key metrics. Should any of these attributes exceed a predefined threshold, alerts are created which, in turn, generate remedy tickets. These tickets are actioned by the Network Operations Center who diagnose and triage the issue as discussed in the Alerts section. Some of the server performance attributes that are monitored via the CloudWatch services include:

- CPU
- Memory
- Network bandwidth

AppDynamics
AppDynamics is used to monitor performance of the various solution components. This provides our support staff an early warning of possible problems. They are alerted when transactions between the various tiers of the solution are not performing to baseline. When thresholds are breached, alerts are generated which, in turn, generate remedy tickets. These tickets are received by the Network Operations Center who diagnose and triage the issue as discussed in the Alerts section.

Keynote
Keynote is deployed to monitor user experience of the SendSuite Tracking Online solution. This is performed via the execution of synthetic transactions against the service from multiple points around the globe (Note: This eliminates false alarms due to local network problems at a single keynote monitoring site).

Keynote baselines the performance of the solution during normal operation and alerts if performance thresholds are breached. Keynote also enables Pitney Bowes to provide reports of application performance against SLA from an independent source.

Alerts
Alerts are automatically logged into the Pitney Bowes Issue Tracking System Solution. Depending on the severity level of the alert, appropriate first responders are automatically contacted. Each Pitney Bowes hosted application has a designated Emergency Response Team (ERT) that can be immediately convened over a dedicated phone bridge depending on the type of alert that is escalated. ERT's are composed of project managers, technical application leads, hardware administrators, network administrators, database administrators and IT management.

Different groups can receive alerts or identify issues, including:
- Deployment Group
- Operations
- Call Centre
- Customer

There are several types of alerts generated by the solution. They range from infrastructure, to application to security.

In summary
SendSuite Tracking Online allows users to modify and improve both parcel and asset control streams. Pitney Bowes offers hosting in order to simplify deployment and free customer IT resources to focus on core business tasks.

For more information on SSTO, contact your Pitney Bowes technical consultant.

Glossary

AWS Amazon Web Services.

CPU Central Processing Unit.

DIACAP Department of Defense Information Assurance Certification and Accreditation Process.

DMZ Demilitarized Zone.

ENISA European Union Agency for Network and Information Security, originally European Network and Information Security Agency.

ERT Emergency Response Team.

FedRAMP Federal Risk and Authorization Management Program.

FFIEC Federal Financial Institutions Examination Council.

FIPS 140-2 The Federal Information Processing Standard (FIPS) Publication 140-2, is a U.S. government computer security standard used to accredit cryptographic modules.

FISMA Federal Information Security Management Act.

FTP File Transfer Protocol.

ID Identification.

ISO 9001 A certified quality management system (QMS) for organisations who want to prove their ability to consistently provide products and services that meet the needs of their customers and other relevant stakeholders.

ITAR International Traffic in Arms Regulations.

IT Information Technology.

OS Paging Operating System.

OWASP Open Web Application Security Project.

PB Pitney Bowes.

PCI DSS Level 1 Payment Card Industry Data Security Standard.

(I)SAE 3402 (International) Standard on Assurance Engagements.

SLA Service Level Agreement.

SOC 1 A report (Service Organization Controls Report) on controls at a service organization which are relevant to user entities' internal control over financial reporting.

SOC 2 A report focused on a business's non-financial reporting controls as they relate to security, availability, processing integrity, confidentiality, and privacy of a system.

SOC 3 A general-use report that provides only the auditor's report on whether the system achieved the trust services criteria.

SSAE 16 Statement on Standards for Attestation Engagements (SSAE) No. 16, Reporting on Controls at a Service Organization.

SSL Secure Sockets Layer, is the standard security technology for establishing an encrypted link between a web server and a browser (secure).

United States
3001 Summer Street
Stamford, CT 06926-0700
800 327 8627
pbsoftware.sales@pb.com

Europe/United Kingdom
The Smith Centre
The Fairmile
Henley-on-Thames
Oxfordshire RG9 6AB
0800 840 0001
pbsoftware.emea@pb.com

Canada
5500 Explorer Drive
Mississauga, ON L4W5C7
800 268 3282
pbsoftware.canada.sales@pb.com

Australia/Asia Pacific
Level 1, 68 Waterloo Road
Macquarie Park NSW 2113
+61 2 9475 3500
pb.apac@pb.com

For more information,
visit us online: pitneybowes.com/uk

16ECM09047_UK