White paper

pitney bowes

Shipping & Mailing

Relay™ communications hub data security

The Relay™ communications hub lets you modify and improve your print communications as well as getting you ready for sending digital communications. Minimize disruption by working seamlessly with your existing systems.

The Relay communications hub by Pitney Bowes is offered as a hosted business application. Pitney Bowes offers hosting of this application in order to simplify deployment, free customer IT resources to focus on core business objectives and to provide worry-free implementation. More and more businesses are using hosted versus on premise software. Relay offers a superior solution with a high degree of security and privacy.

This document discusses the hosted offering, a comprehensive introduction to the inherent security and privacy features of the Relay communications hub as well as an overview of the management and monitoring components of the hosting solution being provided by the Pitney Bowes Global Hosting team.

Pitney Bowes hosting services

Notable benefits for choosing a Pitney Bowes hosting service include:

- The Relay communications hub, alone, may provide a beneficial business case, and is enhanced further by reducing the in-house IT resource and budget constraints.
- Corporate policy may call for applications to be outsourced or to use software as a service (SaaS) whenever possible.
- Corporate firewall restrictions and/or other security issues may make external hosting a more attractive option.

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

Security architecture

The Relay™ communications hub security architecture includes both the design and maintenance of a secure platform and policies. They have been created to protect the privacy of direct customers and all data, as well as application features which implement stringent Pitney Bowes' security and privacy policies.

Platform security

Trustwave external penetration test concludes Relay hub is low risk
As part of a tier 3 application enrollment in Trustwave's Managed Security Testing (MST) services, Pitney Bowes engaged Trustwave SpiderLabs to perform an annual penetration test of the Relay hub application. The primary objective of this test was to gauge the resiliency of the application to various attacks launched against both authenticated and unauthenticated surfaces. Trustwave conducted the test between the dates of October 5–9, 2015. After careful review of the systems and access levels included in this test, Trustwave feels that the Relay hub application is at a low risk of compromise.

Hosting facility security and access
Pitney Bowes Relay is hosted in world-class hosting facilities. These facilities are managed by Amazon Web Services (AWS) located in Frankfurt in Germany for the European and International deployments and Virginia for the USA deployment. 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:

- 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
- Building and environmental control alarms which are constantly monitored.

Network defensibility
The Relay modules do not maintain any credit card, procurement card, or other financial information unless it is already publicly available within the organization.

Relay will encrypt and archive all documents for twelve months prior to their secure deletion.

Essentially, Relay modules only use and/or store information that is already available from the customer.

A number of approaches are taken to protect against intruders, including:
- Redundant, fault-tolerant firewalls segment and secure traffic
- SSL Certificate (HTTPS)
- Only presentation layer services are present in the DMZ

Pre-installation assessment
Before being accepted into production, all systems undergo a thorough security assessment to scan for operating system or application vulnerabilities. The assessment checks for the OWASP Top Ten vulnerabilities as well as other common attack vectors. The assessment must be passed before the software is deployed into production.

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 recently published security vulnerability. Vulnerabilities are patched using automated tools across the entire environment.

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, Relay 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
- Data in transit
- Connectivity
- Business continuity planning
- Patching strategy
- Business logic.

A security test plan was put in place and executed to ensure the controls functioned as expected.

Defensibility
Pitney Bowes follows industry standard best practices for software defensibility. All computers within Pitney Bowes are protected by enterprise level virus scanning software.

Additionally, operating system updates are monitored by a centrally managed system and applied on a weekly basis. Any computers found on the Pitney Bowes corporate and hosted networks without the required antivirus and management software are disabled by local administrators and removed from the network or the facility.

The following lists some of the best practices followed when developing software solutions:

- Sensitive communication to servers utilize SSL
- Security awareness training for software developers
- Automated penetration testing and code analysis
- Design and peer reviews with code auditing
- 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. We also offer a secure FTP solution for customers to send or retrieve files to/from third party print facilities. Customer folders are private, separated and locked down to each customer's login ID. All files are scanned for virus after being uploaded before transferring them to the application server for processing.

Health and security status monitoring

CPU utilization, available disk space, hardware component failure, network availability, application availability and more are monitored constantly using the various tools described below. The Relay solution uses consolidated logging and analytics to look for security anomalies and generate 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 below. Server performance attributes that are monitored via the CloudWatch services include:

- CPU
- Disk Utilization
- Memory
- Network Bandwidth
- OS Paging
- Services Running
- Event Logs

AppDynamics
Appdynamics is used to monitor performance of the various solution components. This provides support staff 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 below.

KeyNote
KeyNote is deployed to monitor user experience of the Relay 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 allows 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) which 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:
- Deployment Group
- Operations
- Call Center
- Customer

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

In summary:
The Relay™ communications hub allows users to modify and improve your print streams. Pitney Bowes offers hosting in order to simplify deployment and free customer IT resources to focus on core business tasks.

Pitney Bowes Relay is hosted in world-class hosting facilities. These facilities are managed by Amazon Web Services located in Frankfurt Germany and Virginia USA.

The Relay communications hub is reported as a low risk of compromise — Trustwave, October 2015.

More and more businesses are using hosted versus on premise software and Relay offers a superior solution with a high degree of security and privacy.

Glossary

AWS Amazon Web Services.

CPU Central Processing Unit.

DIACAP Department of Defense Information Assurance Certification and Accreditation Process.

DMZ DeMilitarised 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 27001 International Organization for Standardization. ISO/IEC 27001 is an internationally recognized best practice framework for an information security management system.

ISO 9001 is a certified quality management system (QMS) for organizations 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

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

SOC 3 This report is 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).

SSO Single Sign On.

United States
3001 Summer Street
Stamford, CT 06926-0700
800 327 8627

United Kingdom
Building 5, Trident Place
Hatfield Business Park
Mosquito Way
Hatfield
Hertfordshire AL10 9UJ
08444 992 992
ukenquiries@pb.com

Ireland
Unit E5, Calmount Park
Calmount Road
Ballymount
Dublin 12
+353 (0) 1 4608700
ibuenquiries@pb.com

France
Immeuble Le Triangle
9 rue Paul Lafargue
93456 Saint Denis la Plaine cedex
0825 850 825

Germany
Poststraße 4-6
64293 Darmstadt
contact.de@pb.com
06151 5202 0

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

New Zealand
72 Apollo Drive, Building B
Units 2 & 3, Rosedale
Auckland 0632
0800 748 639

For more information, visit us online: pitneybowes.com

15SMB10156_ANZ