Document de présentation

pitney bowes

Expédition et traitement de courrier

Sécurisation de données grâce au noyau de communication Relay[MC]

Le noyau de communication Relay[MC] vous permet de modifier et d'améliorer vos communications papier et de vous préparer en vue de l'envoi de messages numériques. En outre, il minimise les perturbations, car il est compatible avec vos systèmes actuels.

Le noyau de communication Relay de Pitney Bowes est une application commerciale hébergée. Pitney Bowes offre d'héberger cette application afin d'en simplifier le déploiement, de libérer les ressources de TI du client, afin qu'elles puissent se concentrer sur les principaux objectifs commerciaux, et de permettre une mise en œuvre sans souci. De plus en plus d'entreprises emploient des applications hébergées plutôt que des logiciels installés sur place. Relay propose une solution supérieure offrant un haut niveau de protection et de confidentialité.

Le présent document traite de l'application hébergée, fait une présentation complète des fonctions de sécurisation et de protection de renseignements confidentiels inhérentes au noyau de communication Relay et présente un aperçu des composants de gestion et de suivi de la solution hébergée qu'offre l'équipe mondiale d'hébergement de Pitney Bowes.

Services d'hébergement de Pitney Bowes

Avantages considérables des services d'hébergement de Pitney Bowes :

- À lui seul, le noyau de communication Relay présente un dossier commercial avantageux, qui est rehaussé par la réduction des ressources de TI à l'interne et des contraintes budgétaires.
- Il est possible qu'une politique d'entreprise exige l'externalisation des applications ou l'utilisation de logiciels-services lorsque c'est possible.
- Il est possible que des restrictions relatives au coupe-feu de l'entreprise ou d'autres questions de sécurité rendent l'hébergement externe plus attrayant.

Pour obtenir de plus amples renseignements sur Relay, veuillez communiquer avec votre conseiller technique Pitney Bowes.

Architecture de sécurisation

L'architecture de sécurisation du noyau de communication Relay[MC] comprend à la fois la conception et la maintenance d'une plate-forme sécurisée et de politiques. Celles-ci ont été créées afin de protéger la confidentialité des clients directs et de l'ensemble des données. De plus, les fonctions de l'application respectent les politiques strictes de Pitney Bowes en matière de sécurisation et de confidentialité.

Sécurisation de la plate-forme

Le test de pénétration externe de Trustwave conclut que le noyau Relay présente peu de risques
Dans le cadre d'un abonnement aux services gérés de test de sécurité de Trustwave pour applications de niveau 3, Pitney Bowes a fait appel à SpiderLabs de Trustwave pour effectuer un test de pénétration annuel sur le noyau Relay. Le principal objectif de ce test était d'évaluer la résistance de l'application à diverses attaques lancées contre des surfaces vérifiées et non vérifiées. Trustwave a effectué le test entre le 5 et le 9 octobre 2015. Après un examen minutieux des systèmes et des niveaux d'accès visés par le test, Trustwave a jugé que le noyau Relay présentait peu de risques de compromission.

Sécurisation des installations d'hébergement et accès à celles-ci
L'application Relay de Pitney Bowes est hébergée dans des installations de calibre mondial. Ces installations sont gérées par Amazon Web Services (AWS) depuis Francfort, en Allemagne, dans le cas des déploiements en Europe et internationaux, et depuis la Virginie dans le cas des déploiements aux États-Unis. L'infrastructure de TI qu'AWS offre est conçue et gérée selon des pratiques exemplaires en matière de sécurisation, et elle répond à diverses normes de sécurité du secteur des TI, notamment les suivantes :

- SOC 1 / SSAE 16 / SAE 3402
- SOC 2
- SOC 3
- FISMA, DIACAP et FedRAMP
- PCI DSS de niveau 1
- ISO 27001
- ISO 9001
- ITAR
- FIPS 140-2

AWS offre des centres de données extrêmement sûrs, qui emploient des systèmes de contrôle d'accès électroniques et à facteurs multiples de pointe, dont ce qui suit :

- installations très sûres protégées par un gardien en tout temps, circuits fermés, portes protégées par un signal d'alarme et munies d'un dispositif d'accès à l'aide d'une carte-clé, lecteur biométrique et accès restreint à l'étage des données;
- alarmes de contrôle du bâtiment et de l'environnement, qui sont surveillées en tout temps.

Capacité de défense du réseau
Les modules Relay ne conservent aucun renseignement au sujet de cartes de crédit ou de cartes d'approvisionnement, ni d'autres renseignements financiers, à moins que ces renseignements ne soient déjà publiquement accessibles au sein de l'entreprise.

Relay chiffrera tous les documents et les archivera pendant douze mois avant de les supprimer de façon sécurisée.

Essentiellement, les modules Relay utilisent et conservent seulement des renseignements auxquels le client donne déjà accès.

Certaines mesures sont prises afin de protéger les données contre les intrus, notamment les mesures suivantes :
- segments de coupe-feu redondants et tolérants aux pannes et sécurisation du trafic;
- certificat SSL (HTTPS);
- seuls des services de couche présentation se trouvent dans la zone démilitarisée (DMZ).

Évaluation préalable à l'installation
Avant de passer à l'étape de production, tous les systèmes subissent une évaluation de sécurité approfondie afin de trouver les vulnérabilités du système d'exploitation ou de l'application. Dans le cadre de cette évaluation, on vérifie les dix principales vulnérabilités d'OWASP, ainsi que d'autres vecteurs d'attaque courants. L'évaluation doit être effectuée avant le déploiement du logiciel.

Essais continus

Test de pénétration périodique
Un tiers effectue chaque année un test de pénétration afin qu'on puisse remédier aux vulnérabilités en matière de sécurité. On fait l'essai de tous les chemins d'entrée et de sortie, en se concentrant sur la sécurisation des données.

Évaluation continue des vulnérabilités du système d'exploitation
On fait une vérification de routine de tous les systèmes afin de détecter les virus et les autres formes d'intrusion et de protéger les systèmes contre ces attaques. De plus, on exécute des mises à jour de système d'exploitation critiques afin d'assurer la protection des systèmes contre les vulnérabilités récentes en matière de sécurité. On remédie aux vulnérabilités à l'aide d'outils automatisés dans l'ensemble de l'environnement.

Sécurisation des applications

Pitney Bowes intègre la sécurisation à toutes les étapes de ses procédés de développement de plate-forme. De la conception de logiciels et d'architectures au soutien postconception, en passant par l'architecture d'hébergement, on tient compte des questions de sécurisation.

En ce qui concerne les exigences, Relay respecte les lignes directrices de l'ENISA et du FFIEC. Ces lignes directrices ont été appliquées au développement des produits et aux exigences relatives au déploiement.

On a passé en revue l'architecture de sécurisation et la conception afin de s'assurer que des contrôles de sécurité appropriés seraient appliqués au système en ce qui concerne ces spécifications. Il y a notamment des contrôles relatifs :

- aux données au repos;
- aux données en transit;
- à la connectivité;
- à la planification de la reprise des activités;
- à la stratégie de correction;
- à la logique applicative.

On a élaboré et exécuté un plan de vérification de la sécurité afin de s'assurer que les mesures de contrôle fonctionnaient comme prévu.

Capacité de défense
Pitney Bowes suit les pratiques exemplaires standards de l'industrie en matière de capacité de défense des logiciels. Tous les ordinateurs de Pitney Bowes sont protégés par un logiciel de détection de virus au niveau de l'entreprise.

En outre, les mises à jour de système d'exploitation sont surveillées par un système à gestion centrale et exécutées chaque semaine. Tout ordinateur relié aux réseaux d'entreprise et hébergés de Pitney Bowes qui n'est pas doté des logiciels antivirus et de gestion nécessaires est désactivé par les administrateurs locaux et retiré du réseau ou de l'établissement.

Voici certaines des pratiques exemplaires suivies lors du développement de solutions logicielles :

- Communication confidentielle avec des serveurs à l'aide du protocole SSL
- Formation de sensibilisation à la sécurité à l'intention des développeurs logiciels
- Test de pénétration et analyse de codes automatisés
- Examens de projet et évaluations par les pairs avec vérification de codes
- Formation sur le piratage contrôlé
- Logiciel à signature numérique

Protocoles HTTPS et FTP sécurisé
Pitney Bowes emploie le protocole HTTPS pour le transfert sécurisé de fichiers entre vos utilisateurs et nos centres de données hébergés. Nous offrons également une solution FTP sécurisée qui permet aux clients d'envoyer des fichiers à des installations d'impression de tiers ou de récupérer des fichiers à partir de celles-ci. Les dossiers des clients sont privés, séparés et verrouillés à l'aide d'un nom d'utilisateur propre à chaque client. On vérifie si les fichiers ne comportent pas de virus après leur téléversement et avant leur transfert vers le serveur d'applications aux fins de traitement.

Suivi de la situation relative à l'état et à la sécurité

On surveille constamment l'utilisation de l'unité centrale, l'espace disque libre, la défaillance de composants matériels, la disponibilité du réseau, la disponibilité des applications et d'autres éléments à l'aide des divers outils décrits ci-dessous. La solution Relay emploie une journalisation et une analytique consolidées afin de détecter les anomalies en matière de sécurité et d'envoyer des alertes à l'équipe de soutien.

Amazon CloudWatch
Amazon CloudWatch offre la surveillance d'indices clés au niveau des serveurs. Si l'un de ces attributs dépasse un seuil prédéfini, des alertes sont déclenchées, ce qui génère ensuite des demandes dans Remedy. Ces demandes sont traitées par le centre d'exploitation du réseau, qui diagnostique et trie le problème, comme l'indique la section « Alertes » ci-dessous. Voici certains des attributs de rendement des serveurs que les services CloudWatch surveillent :

- Unité centrale
- Utilisation du disque
- Mémoire
- Bande passante du réseau
- Pagination par le système d'exploitation
- Services en cours d'exécution
- Journaux d'événements

AppDynamics
AppDynamics sert à surveiller le rendement des divers composants de la solution. Ce logiciel prévient tôt le personnel de soutien de problèmes éventuels. Le personnel est informé lorsque des opérations entre les divers niveaux de la solution ne s'effectuent pas selon la base de référence. Lorsque des seuils ne sont pas respectés, des alertes sont déclenchées, ce qui génère ensuite des demandes dans Remedy. Ces demandes sont reçues par le centre d'exploitation du réseau, qui diagnostique et trie le problème, comme l'indique la section « Alertes » ci-dessous.

KeyNote
KeyNote est déployé afin de surveiller l'expérience utilisateur qu'offre la solution Relay. Cela se fait en exécutant des opérations synthétiques relatives au service depuis de multiples endroits dans le monde. (Remarque : Cela élimine les fausses alarmes causées par des problèmes sur le réseau local d'un seul site de surveillance de KeyNote.)

KeyNote établit une base de référence relative au rendement de la solution dans le cadre d'un fonctionnement normal et émet des alertes si des seuils de rendement ne sont pas respectés. De plus, KeyNote permet à Pitney Bowes de produire des rapports sur le rendement des applications par rapport au contrat de niveau de service à partir d'une source indépendante.

Alertes
Les alertes sont consignées automatiquement dans le système de suivi de problèmes de Pitney Bowes. Selon le niveau de gravité de l'alerte, on communique automatiquement avec les premiers répondants appropriés. Dans le cas de chaque application hébergée par Pitney Bowes, on désigne une équipe d'intervention d'urgence (EIU), avec laquelle il est possible de communiquer immédiatement au moyen d'un pont téléphonique spécialisé, selon le type d'alerte déclenchée. Les EIU sont composées de gestionnaires de projets, de responsables d'application technique, d'administrateurs de matériel, d'administrateurs de réseau, d'administrateurs de base de données et de gestionnaires de TI.

Différents groupes peuvent recevoir des alertes ou diagnostiquer des problèmes :
- Groupe responsable du déploiement
- Exploitation
- Centre d'appels
- Client

La solution génère plusieurs types d'alerte. Les alertes peuvent être liées à l'infrastructure, aux applications ou à la sécurité.

En résumé :
Le noyau de communication Relay[MC] permet aux utilisateurs de modifier et d'améliorer leurs files d'impression. Pitney Bowes héberge la solution, afin de simplifier le déploiement et de libérer les ressources de TI des clients, pour leur permettre de se concentrer sur les principales tâches commerciales.

L'application Relay de Pitney Bowes est hébergée dans des installations de calibre mondial. Ces installations sont gérées par Amazon Web Services (AWS) depuis Francfort, en Allemagne, et la Virginie, aux États-Unis.

Trustwave a établi en octobre 2015 que le noyau de communication Relay présentait peu de risques de compromission.

De plus en plus d'entreprises emploient des applications hébergées plutôt que des logiciels installés sur place, et Relay propose une solution supérieure offrant un haut niveau de protection et de confidentialité.

Glossaire

AWS Amazon Web Services

UC Unité centrale

DIACAP Department of Defense Information Assurance Certification and Accreditation Process

DMZ Zone démilitarisée

ENISA Agence de l'Union européenne, chargée de la sécurité des réseaux et de l'information

EIU Équipe d'intervention d'urgence

FedRAMP Federal Risk and Authorization Management Program

FFIEC Federal Financial Institutions Examination Council

FIPS 140-2 La publication 140-2 des Federal Information Processing Standards (FIPS) est une norme de sécurité informatique du gouvernement des États-Unis utilisée pour accréditer des modules cryptographiques.

FISMA Federal Information Security Management Act

FTP Protocole de transfert de fichiers

ISO 27001 Organisation internationale de normalisation. ISO/IEC 27001 est un cadre de travail exemplaire reconnu à l'échelle internationale relativement aux systèmes de gestion de la sécurité de l'information.

ISO 9001 Système de gestion de la qualité (SGQ) certifié pour les entreprises qui souhaitent prouver leur capacité à offrir invariablement des produits et services qui répondent aux besoins de leurs clients et d'autres parties prenantes pertinentes

ITAR International Traffic in Arms Regulations

TI Technologies de l'information

Pagination par le système d'exploitation Système d'exploitation

OWASP Open Web Application Security Project

PB Pitney Bowes

PCI DSS de niveau 1 Norme de sécurisation de données au sein de l'industrie des cartes de paiement

(I)SAE 3402 Norme internationale en matière de missions d'assurance

SOC 1 Rapport (rapport de contrôle d'une entreprise de service) sur les contrôles en place dans une entreprise de service relatifs au contrôle interne des entités d'utilisateurs en ce qui concerne les rapports financiers

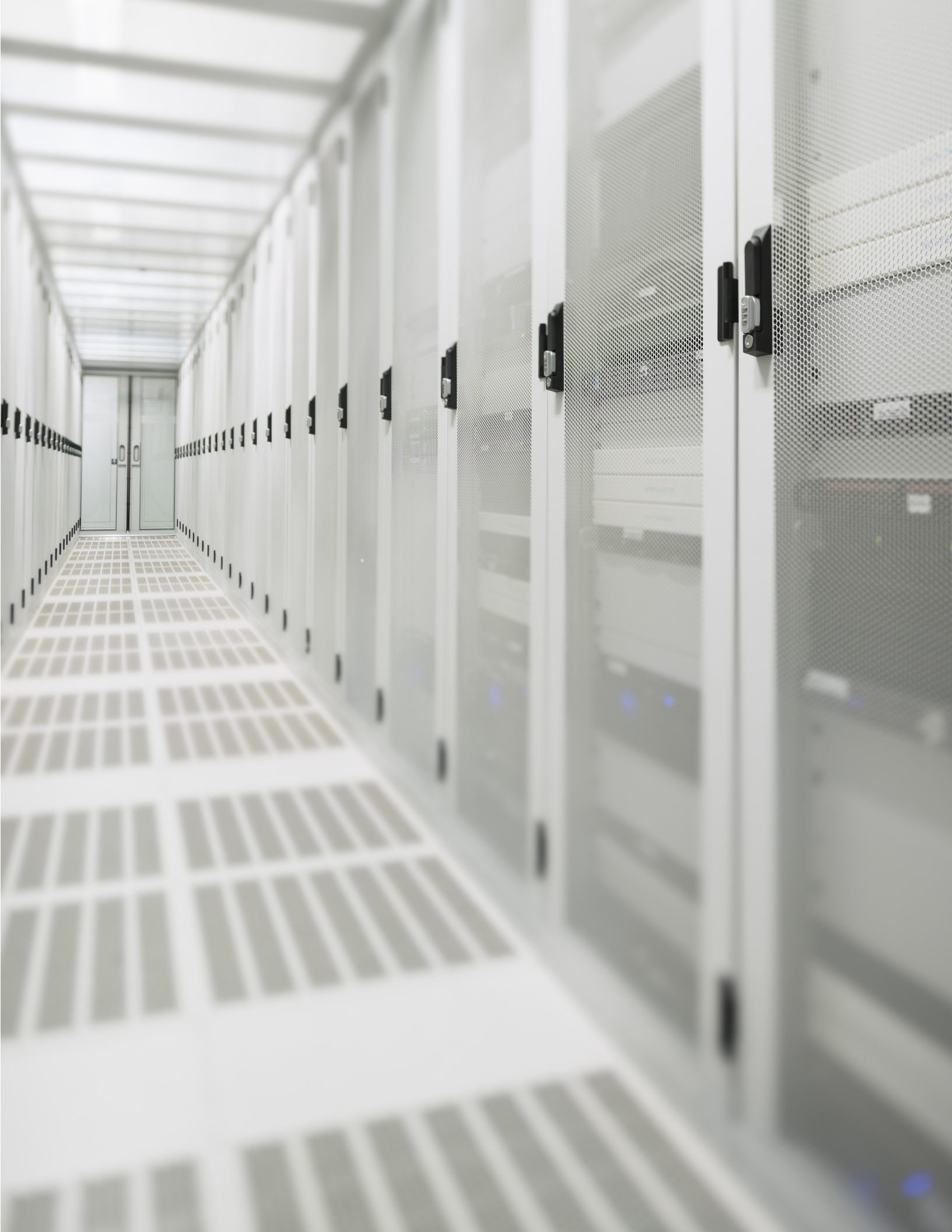
SOC 2 Ce rapport est axé sur les mesures de contrôle non financières d'une entreprise qui sont liées à la sécurité, à la disponibilité, à l'intégrité de traitement, à la confidentialité et à la protection des renseignements confidentiels d'un système.

SOC 3 Ce rapport général indique uniquement si le système a satisfait ou non les critères des services Trust selon le vérificateur.

SSAE 16 Énoncé sur les normes en matière de missions d'attestation n° 16, portant sur les contrôles au sein d'une entreprise de service

SSL Le protocole « Secure Sockets Layer » est la technologie de sécurisation de référence pour établir un lien chiffré entre un serveur Web et un navigateur (sécurisé).

SSO Single Sign On.



pitney bowes

États-Unis
3001 Summer Street
Stamford, CT 06926-0700
800 327-8627

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

Irlande
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

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

Canada
5500 Explorer Drive
Mississauga, ON L4W5C7
855 619-7974

Australie / Asie-Pacifique
Level 1, 68 Waterloo Road
Macquarie Park NSW 2113
+61 2 9475 3500
pb.apac@pb.com

Pour obtenir de plus amples renseignements, composez le 855 619-7974
ou visitez notre site Internet : pitneybowes.com/ca

VEUILLEZ RECYCLER
recycleplease.org

15SMB09800_FRCA