LIVRE BLANC Kaseya®

Comment relever neuf défis importants dans la vente au détail

Kaseya®

Je vous mets au défi de citer une activité plus difficile que la vente au détail. Les marges sont très minces, la concurrence est plus féroce que lors d'une finale de coupe du monde de football et les goûts des clients changent constamment.

Sans parler du fait que les grands détaillants couvrent des centaines, voire des milliers de sites. Il existe également une myriade de points de terminaison différents : PC et ordinateurs portables, kiosques, systèmes de points de vente (POS) et de points de vente électroniques (ePOS), tablettes, et même smartphones.

Que doit donc faire un professionnel IT dans la vente au détail ? Nous allons étudier neuf des plus grandes difficultés dans ce secteur et la façon dont l'IT peut les atténuer.

1. La sécurité avant tout

Dans l'immobilier, on dit que l'emplacement passe avant tout. Dans la vente au détail, et dans la quasi-totalité de l'IT, c'est la sécurité qui passe avant tout.

La sécurité est une question très sérieuse. Les attaques dans la vente au détail comptent parmi les violations les plus médiatisées.

Qui n'a pas entendu parler de Target, dont 40 millions de dossiers client ont été volés, et chez qui la même attaque a ensuite compromis 70 millions de dossiers supplémentaires ? Ou de Home Depot, dont 56 millions de dossiers client ont été compromis ? Neiman Marcus et J. C. Penney ont été frappés de la même manière et ont eu mauvaise presse.

La vente au détail possède des besoins en sécurité particuliers et critiques. L'existence même d'un détaillant dépend du maintien en sécurité des données client. On pense en premier aux données des cartes de paiement. Elles sont effectivement cruciales. Cependant, les clients sont le plus souvent protégés de toute fraude par les entreprises des cartes de paiement. Les informations personnelles qui entourent le numéro de carte constituent un problème plus important : ces informations sont assez complètes pour permettre un vol d'identité, une fraude bien plus difficile à éviter.

Et n'allez pas croire que ces attaques ne ciblent que les plus grands détaillants.

L'e-book « Cybercriminals: Unmasking the Villians » de Kaspersky Lab indique aux PME qu'elles doivent prendre la sécurité au sérieux. « De nombreuses entreprises éprouvent un faux sentiment de sécurité concernant ce problème. Les grandes entreprises consolident souvent leurs propres mesures de sécurité IT, mais les petites et moyennes entreprises partent du principe, à tort, qu'elles ne sont pas des cibles pour les cybercriminels. En fait, presque n'importe quelle entreprise peut devenir une cible, et aucun secteur n'est à l'abri », peut-on lire dans cet e-book. « Le Département de la Sécurité intérieure des États-Unis a même indiqué que 31 % de toutes les cyber-attaques visaient les entreprises de moins de 250 employés. »

Solution : les détaillants doivent posséder une stratégie de défense approfondie dans laquelle tous les aspects des appareils et applications du réseau sont protégés. Il est tout aussi important de former les employés aux procédures de sécurité appropriées, comme utiliser des mots de passe sécurisés, mais aussi éviter les logiciels malveillants et détecter et arrêter les attaques d'ingénierie sociale.

2. Conformité PCI appropriée

Si vous êtes un détaillant qui utilise des cartes de paiement, ce qui est le cas de presque tout le monde (en dehors du stand de limonade du petit voisin), vous devez respecter les règles de la norme de sécurité de l'industrie des cartes de paiement (PCI DSS, Payment Card Industry Data Security Standard). Ces réglementations sont une cible mouvante. En avril dernier, les réglementations ont même été renforcées et requièrent désormais que les détaillants impliqués dans les transactions électroniques adoptent des mesures d'authentification plus solides. Le Conseil des normes de sécurité PCI, qui est responsable de la norme, a également recommandé que les chefs d'entreprise adoptent un rôle plus actif pour veiller à ce que la sécurité entourant les cartes de paiement soit complète.

Le PCI possède un certain nombre d'exigences clés, comme l'installation et le maintien d'un pare-feu, l'abandon des mots de passe par défaut (en particulier ceux des fournisseurs, qui sont bien trop faciles à pirater), et le chiffrement des données du détenteur de la carte lorsqu'elles sont transmises par voie électronique.

De manière plus approfondie, les organisations doivent défendre leurs systèmes contre les logiciels malveillants et virus en mettant régulièrement à jour les outils de sécurité et en veillant à ce que les définitions de virus soient toujours à jour.

Les détaillants doivent posséder une stratégie de défense approfondie dans laquelle tous les aspects des appareils et applications du réseau sont protégés.

Dans le même temps, vous devez bénéficier d'un contrôle d'accès précis, comprenant, comme l'indique le conseil, la capacité à :

- Restreindre l'accès aux données du détenteur de la carte que l'entreprise doit connaître
- Identifier et authentifier l'accès aux composants du système
- Restreindre l'accès physique aux données du détenteur de la carte

Solution : le respect de la conformité PCI nécessite tout d'abord de comprendre les exigences. Lisez ces documents et assurez-vous de rester informé des nouvelles réglementations. Dressez la liste des étapes de protection que vous devez entreprendre, créez un budget et établissez un plan pour mettre en œuvre toutes ces initiatives.

3. Termes PCI DSS à respecter

Les nouvelles exigences, exposées dans un document de 139 pages, sont accompagnées de leur ensemble de bonnes pratiques, créées par le Conseil des normes de sécurité PCI.

Le point essentiel consiste à intégrer la conformité PCI à vos processus de routine.

Ainsi, elle devient une simple fonction normale des activités quotidiennes. Les activités de conformité comprennent la « surveillance des contrôles de sécurité, telles que les pare-feu, les systèmes de détection des intrusions/systèmes de prévention des intrusions (IDS/IPS), la surveillance d'intégrité de fichier (FIM), les antivirus, les contrôles d'accès, etc., afin de s'assurer qu'ils fonctionnent de manière efficace et tel que prévu », indique le conseil.

Pendant ce temps, votre position en matière de sécurité doit être mise à jour à chaque changement de système significatif. « Si un nouveau système est concerné par le PCI DSS, il doit être configuré selon les normes de configuration du système, dont la FIM, les antivirus, les correctifs, la consignation d'audit, etc. », indique le conseil.

Des pénalités sont appliquées en cas de non-conformité aux normes PCI, ainsi que pour les violations qui aboutissent. Les amendes de non-conformité vont de 5 000 $ (USD) à 500 000 $ (USD). Vos banques et organismes de carte de crédit peuvent prélever ces amendes directement.

Il existe également des pénalités pour violations, selon le site Web Focus on PCI. Voici comment il décrit les conséquences possibles liées aux violations, même pour une entreprise 100 % conforme PCI et validée :

- Amende de 50 à 90 $ par données de détenteur de carte compromises
- Suspension de l'acceptation de carte de crédit par le fournisseur de compte de carte de crédit d'un marchand
- Perte de réputation auprès des clients, fournisseurs et partenaires
- Litige civil possible auprès des clients en violation
- Perte de la confiance des clients, ce qui affecte les futures ventes

Solution : vous devez développer une politique de sécurité interne correspondant aux exigences du PCI. Toute l'équipe IT doit ne jurer que par la conformité PCI : les dommages et dégâts financiers causés à la réputation de votre entreprise ne valent pas la peine de contourner les règles.

4. Protection des POS et ePOS

Les systèmes de points de vente (POS) ont subi une amélioration spectaculaire ces dernières années.
On trouve désormais des systèmes de points de vente électroniques (ePOS) étroitement liés aux systèmes back-end de vente au détail, pour vérifier et mettre à jour l'inventaire en temps réel. Ils peuvent même accéder au site Web du détaillant pour vérifier les prix sur Internet, et souvent les envoyer par e-mail.

Les systèmes ePOS étant principalement des PC spécialisés, les logiciels peuvent offrir davantage de fonctions, telles que :

- Messagerie instantanée entre les employés de la vente au détail et les emplacements d'ePOS
- Enregistrement et gestion de la présence
- Partage de documents
- Outils de comptabilité
- Marketing par e-mail et suivi des clients
- Gestion des fournisseurs

Presque tous les éléments qui s'exécutent sur un PC peuvent potentiellement s'exécuter sur certains appareils POS, en particulier s'ils ne sont pas verrouillés en termes d'installation et d'utilisation d'applications.

Le respect de la conformité PCI nécessite tout d'abord de comprendre les exigences. Lisez ces documents et assurez-vous de rester informé des nouvelles réglementations.

Kaseya®

Le PC est un grand avantage pour les opérations, mais un gros inconvénient pour la sécurité. Les PC constituent toujours le plus large vecteur d'attaque pour les logiciels malveillants et violations, et représentent un conduit majeur pour les attaques d'IT en vente au détail.

Les appareils POS sont également vulnérables car ils sont souvent utilisés pour de nombreuses actions, parfois trop, et peuvent être très visibles sur Internet. Bien que cette exposition soit vraie pour les grands comme pour les petits détaillants, les organisations plus petites mettent souvent en place des protections et politiques moins strictes. « Dans les petites entreprises, l'environnement de POS peut avoir une population propre, avec des paiements à traitement informatique isolés et une communication sur le processeur de paiement. Cet appareil peut également (malheureusement) être utilisé pour consulter les e-mails personnels, pour les violations sur les réseaux sociaux et d'autres activités sur Internet qui introduisent plus de risques pour une application POS isolée, sans antivirus ni pare-feu basé sur un hôte avec lequel communiquer », selon le rapport Verizon 2016 Data Breach Investigation Report.

Autre problème : les appareils POS sont placés au même endroit que les clients, c'est-à-dire loin du chemin établi par le réseau LAN. Il est donc un peu plus difficile de les surveiller et gérer correctement. De nos jours, de nombreux appareils POS sont sans fil, ce qui les rend vulnérables aux piratages Wi-Fi. Les logiciels de gestion de points de terminaison ont également plus de difficultés à exercer un contrôle complet.

Solution : ces appareils à distance peuvent être observés, sécurisés et réparés de manière rapprochée grâce à la gestion de point de terminaison. Grâce à ce type de solution, les appareils POS sont à jour et bénéficient des derniers correctifs ; ils sont surveillés en temps réel afin que tous les problèmes puissent être détectés et réparés immédiatement.

5. Vos appareils non gérés sont vulnérables

En raison de tous ces facteurs, les appareils POS et ePOS sont l'une des cibles les plus courantes des attaques à distance, selon Verizon. Verizon a découvert 534 incidents liés à des attaques de POS l'année passée, et dans la plus grande majorité de ces cas (525 pour être exacts), une exposition des données a été confirmée.

Les types d'attaque comprennent :

- L'utilisation d'identifiants volés
- Le RAM scraping (grâce à cette technique, les attaquants accèdent à des données censées être chiffrées, mais qui sont encore sous forme de texte en clair dans la RAM)
- L'utilisation de logiciels malveillants d'enregistrement de frappe
- Les séries (dans lesquelles un seul acteur fait de nombreuses victimes)
- Et toutes sortes d'attaques automatisées

Le fil conducteur des attaques les plus réussies : les logiciels malveillants. Et que recherchent principalement les attaquants ? Les données de carte de paiement et les renseignements personnels connexes. C'est pourquoi le segment vertical de la vente au détail est l'un des principaux domaines d'attaques dans tous les secteurs.

Les appareils POS détiennent de nombreuses données de carte de paiement, y compris celles qu'ils collectent via des lecteurs magnétiques et auxquelles ils ont accès grâce à leurs connexions fréquentes aux données transactionnelles, à l'échelle de l'entreprise.

Au fur et à mesure que les attaquants de POS deviennent plus sophistiqués, les techniques plus anciennes restent efficaces contre les systèmes mal défendus. Verizon nomme ce type d'approche cambriolage de POS. Voici son fonctionnement. « 1) Le serveur POS est visible sur Internet, 2) le POS possède une connexion par défaut, 3) l'attaquant profite des points 1) et 2) pour installer un logiciel malveillant et 4) le logiciel malveillant s'empare des données de carte de paiement lors de leur traitement », indique le rapport Verizon.

Solution : il est conseillé aux professionnels de l'IT en vente au détail de se défendre aussi bien contre les anciennes attaques que contre les nouvelles. Tout en haut de la liste de sécurité, on retrouve le fait de vérifier que vos systèmes antivirus/anti-malware sont toujours bien à jour.

6. Obtenir une authentification efficace

Au début du PCI, l'authentification à deux facteurs (TFA) était requise pour ceux qui traitaient directement les données des détenteurs de carte. Selon les dernières règles, la TFA est obligatoire pour toutes les personnes bénéficiant d'un accès au réseau qui pourrait les mettre en contact avec les données de paiement.

Cela signifie que beaucoup plus de personnes ont désormais besoin de la TFA.

Verizon a découvert 534 incidents liés à des attaques de POS l'année passée, et dans la plus grande majorité de ces cas (525 pour être exacts), une exposition des données a été confirmée.

Kaseya®

Solution : Verizon conseille à tous les détaillants de mettre en place une authentification solide. « L'authentification unique statique est un point faible fréquemment exploité par les attaquants. Si possible, améliorez ce point grâce à un deuxième facteur, comme un jeton matériel ou une application mobile, et surveillez les activités de connexion pour détecter les schémas inhabituels », conseille Verizon.

7. Restez informé des activités grâce à une gestion de point de terminaison qui fonctionne à distance

Les systèmes de POS sont généralement distribués à grande échelle, sauf dans le cas d'un détaillant situé à un seul endroit. De plus, il s'agit davantage d'ordinateurs que de simples appareils de POS. Ils doivent être protégés, gérés et réparés.

La majorité des organisations IT de vente au détail doivent mener des visites sur site pour maintenir, mettre à jour et réparer les appareils. Elles perdent un temps précieux à se rendre aux emplacements éloignés où se trouvent ces appareils.

La situation est dangereuse et non viable. Les appareils sur le terrain ne doivent pas rester non protégés ou en panne : cela pourrait forcer la fermeture d'une caisse, voire rendre inopérable un kiosque situé à un emplacement lointain, jusqu'à l'arrivée d'un technicien. Mais demander à l'équipe IT de gérer tout ce travail en temps et en heure n'est pas une solution efficace, ni même possible. Cette solution ne devrait même pas être testée. Mieux vaut mettre en place des outils qui faciliteront la tâche, sans nécessiter un déplacement pour chaque appareil et machine nécessitant une intervention.

Solution : la gestion de point de terminaison automatise toutes ces fonctions et élimine les visites sur site. Ces solutions peuvent également mettre en œuvre un contrôle précis. Par exemple, les professionnels de l'IT peuvent établir des seuils de performances. Lorsqu'ils sont dépassés, les administrateurs reçoivent une alerte pour pouvoir agir enconséquence. Ainsi, les problèmes peuvent être réparés avant de s'aggraver, et avant que les utilisateurs finaux ne se doutent de quoi que ce soit.

Les correctifs et mises à jour peuvent être testés de manière centralisée, puis envoyés à toutes les machines ou à certains groupes une fois qu'ils ont été déterminés comme étant sûrs.

8. Complexité du réseau et du système

Les réseaux de vente au détail, sauf si vous n'avez qu'un seul emplacement, sont complexes par définition, avec de nombreux points de terminaison éparpillés et diversifiés, ainsi que des problèmes sur des zones étendues et le réseau sans fil. Ces systèmes étant très complexes, il existe davantage de points de défaillance ; il est donc plus difficile de trouver les causes d'un échec et la résolution du problème prend plus de temps.

Les détaillants doivent conserver les opérations IT en état de marche, en permanence. Le temps d'indisponibilité est synonyme de pertes de revenus, et surtout de perte de confiance. Cela signifie que l'IT doit comprendre ce qui se passe dans les systèmes placés sous sa responsabilité. La surveillance est essentielle. « Découvrez les options de surveillance disponibles pour votre environnement de POS et validez leur mise en œuvre. Suivez les connexions à distance et vérifiez que toutes respectent la norme », suggère le rapport de Verizon. Naturellement, la surveillance doit être appliquée à tous les appareils à distance, et pas seulement aux POS.

Claranet, un MSP installé en Europe, indique que, même si les détaillants souhaitaient auparavant acquérir principalement une bande passante supérieure, leur priorité est désormais de gérer la complexité des réseaux qu'ils ont mis des années à construire. Cela est dû en partie à une grande augmentation du nombre d'appareils connectés à Internet, ainsi qu'à une hausse semblable dans les services cloud.

« Les vingt dernières années de développement réseau ont complètement changé la façon dont les entreprises interagissent avec Internet et l'utilisent. La disponibilité de la bande passante augmente constamment et les coûts ont diminué : les entreprises ont ainsi bénéficié d'une capacité inédite, qui leur a permis de prendre en charge différents services à partir d'emplacements variés. Cependant, face à la prolifération des appareils et des applications orientées cloud, il est de plus en plus important de gérer et de surveiller le flux de données, en s'assurant que la disponibilité, les performances et la sécurité sont optimales », explique Michel Robert, Directeur Général de Claranet.

Cela ne signifie pas que toutes les constructions de réseau sont réussies. Vodat International indique que les détaillants du Royaume-Uni ne peuvent pas fournir une expérience client optimale, car leurs réseaux sont trop lents et la couverture Wi-Fi est incomplète.

Ces systèmes étant très complexes, il existe davantage de points de défaillance ; il est donc plus difficile de trouver les causes d'un échec et la résolution du problème prend plus de temps.

Kaseya®

Par exemple, le problème du Wi-Fi est critique, car les acheteurs au Royaume-Uni ont l'habitude de faire du shopping avec leur smartphone. D'ailleurs, 60 % de ces clients utilisent leur téléphone de cette façon. Le fait étrange est que les trois quarts des acheteurs ont rencontré des problèmes de réseau l'année passée. Près de 40 % des acheteurs ont connu des lenteurs du Wi-Fi et un tiers ont rencontré des problèmes avec des paiements en libre-service ou des automates offrant de mauvaises performances.

Suite à ces problèmes, un quart de ces clients deviennent moins fidèles envers le détaillant et 20 % sont moins susceptibles de retourner dans le magasin concerné, a indiqué Vodat.

Solution : des clouds privés et hybrides, une infrastructure virtualisée et une infrastructure de réseau distribué multiplient les difficultés liées à la surveillance, même lorsque les clients exigent des niveaux de service supérieurs. Vous devez surveiller votre réseau, le LAN, le sans fil et les connexions WAN que vous possédez sur le cloud ou au siège. Il n'est plus possible de surveiller ces composants et réseaux à l'aide de produits en silo pour déterminer la cause racine de la dégradation de l'application. Recherchez une solution pouvant vous présenter toute l'infrastructure et vous aider à comprendre rapidement la cause des problèmes de performances.

9. Trouver du temps pour les nouvelles technologies et les exploiter

Les professionnels de l'IT de la vente au détail gèrent des situations d'urgence liées à des opérations étendues, en assurant le bon fonctionnement de réseaux complexes et en répondant aux nouvelles demandes des chefs d'entreprise. Ces professionnels sont véritablement débordés ; ils ont des difficultés à accueillir les nouvelles technologies qui révolutionnent l'IT de la vente au détail. Celles-ci incluent :

Activation mobile : le mobile est désormais régulièrement utilisé pour le paiement. Pendant ce temps, les clients bénéficient de plus en plus d'un accès sans fil, et les applications de ventes peuvent proposer des offres spéciales aux clients intéressés, voire même mettre en œuvre un système de suivi afin de savoir où se trouve le client dans le magasin et de le cibler par rapport à son emplacement.

Expérience client : les détaillants doivent interagir avec les clients de nombreuses façons, avec un message toujours cohérent. Cela inclut les applications, e-mails, réseaux sociaux et la vente au détail en ligne.

Intégration des systèmes : de nombreux systèmes ont été ajoutés de manière morcelée et ne sont pas entièrement intégrés. La gestion des commandes, l'e-commerce et les POS ont tous été rassemblés, synchronisés et conçus pour alimenter les transactions et les back-ends du Big Data.

Solution: la bonne solution de gestion des systèmes IT, avec des fonctionnalités à distance puissantes et des fonctionnalités de gestion des politiques, peut faire économiser de nombreuses heures de travail à l'IT de la vente au détail et diminuer radicalement les coûts de support. Dans l'ensemble, ces fonctionnalités offrent aux responsables IT de la vente au détail le temps et le budget nécessaires pour se concentrer sur des technologies plus stratégiques, qui vont plus loin.

Solutions Kaseya – Un kit d'outils IT essentiel pour la vente au détail

Kaseya possède un certain nombre de solutions qui facilitent la tâche des professionnels IT de la vente au détail. Il en existe trois en particulier que nous souhaiterions mettre en avant.

Kaseya VSA

Kaseya VSA est une solution de système IT et de gestion de point de terminaison pour l'IT. Dans le cadre de la vente au détail, VSA peut augmenter le temps de fonctionnement, les performances et la sécurité des appareils, dont les kiosques, ePOS, tablettes, serveurs et PC de tous les types.

VSA prend en charge la gestion à distance de vos appareils grâce à une seule console : l'affichage unique.

Avec Kaseya VSA, les professionnels IT de la vente au détail peuvent :

- **Découvrir, auditer, répertorier et surveiller les clients, les serveurs et le réseau**

  Ainsi, l'équipe IT sait qu'elle bénéficie d'une visibilité complète sur son réseau et tous les appareils associés (dont les appareils ePOS), et qu'elle peut connaître le statut en temps réel sur tous les détails de fonctionnement de ces appareils. Tous les écarts ou problèmes par rapport aux conditions de fonctionnement normales peuvent être identifiés par VSA, avec le déploiement d'une correction appropriée et/ou l'envoi d'alertes à l'équipe IT.

Les professionnels de l'IT de la vente au détail gèrent des situations d'urgence liées à des opérations étendues, en assurant le bon fonctionnement de réseaux complexes et en répondant aux nouvelles demandes des chefs d'entreprise.

Kaseya®

- **Gestion des correctifs**
  De nombreux appareils de POS sont basés sur PC ; les plus vulnérables aux attaques sont ceux qui n'ont pas de correctifs. Le POS étant en contact direct avec le client et détenant beaucoup de données ne doit pas être compromis.

- **Surveiller les points de terminaison pour détecter les performances ou d'éventuels problèmes**
  Mieux vaut éviter les longues files d'attente à la caisse ; de plus, les clients sont découragés par les systèmes lents. Un réseau toujours réactif est l'une des clés du succès auprès des clients.

- **Résoudre les problèmes, y compris les pannes de disque dur**
  Tout système de vente au détail en panne, notamment les POS ou kiosques, est synonyme de perte d'argent. L'idéal est de les remettre en état de marche le plus rapidement possible, en utilisant l'outil de gestion de point de terminaison adapté.

- **Maintenir et exécuter des outils d'antivirus/anti-malware**
  Les logiciels malveillants restent la première cause de compromission des systèmes de vente au détail. Les antivirus/anti-malware à jour sont la meilleure ligne de défense.

- **Rapports en temps réel pour faciliter les audits de PCI**
  VSA veille à ce que tous les systèmes soient surveillés et conformes, permettant ainsi d'exécuter rapidement et facilement des rapports d'audit en temps réel, selon le besoin.

La bonne nouvelle est que tous ces avantages peuvent être automatisés, d'après des politiques prédéfinies que vous définissez et gérez selon les besoins de votre entreprise. Par exemple, les mises à jour de correctif peuvent être automatiquement téléchargées et installées selon des politiques de correctif prédéfinies et des calendriers qui minimisent l'impact sur le réseau. L'IT peut ainsi gagner du temps et de l'argent, et ces processus se déroulent dans les temps.

Découvrez plus d'informations sur Kaseya VSA ou obtenez un essai gratuit. **Cliquez ici**

Authentification multi-facteurs AuthAnvil

Les règles d'authentification PCI se sont fortement renforcées ; toutes les personnes qui PEUVENT être en contact avec les données des détenteurs de carte de crédit DOIVENT avoir une authentification à deux facteurs. Et pas uniquement les personnes qui sont directement et régulièrement impliquées.

Kaseya AuthAnvil fournit une authentification à deux facteurs et multi-facteurs, ainsi que la capacité à chiffrer tous les mots de passe utilisateur et les données lors de la transmission.

Il existe deux autres couches de protection pour l'authentification. AuthAnvil comprend l'authentification unique (SSO) qui permet aux utilisateurs finaux de se connecter plus facilement à plusieurs services, de manière sécurisée. La gestion des mots de passe applique des mesures essentielles, comme la définition de mots de passe sécurisés, leur changement fréquent et leur désactivation lors du départ d'un employé.

Pour en savoir plus sur l'authentification multi-facteurs Kaseya AuthAnvil : **cliquez ici**
Pour plus de détails sur l'authentification unique Kaseya AuthAnvil : **cliquez ici**

Surveillance transversale du réseau et du cloud

Peu de réseaux et d'applications sont tous en interne ou sur site de nos jours. Beaucoup d'entre eux sont dans le cloud ou une association hybride d'installation sur site et dans le cloud. Les systèmes de vente au détail ne font pas exception. Souvent, les problèmes de performances qui découragent les clients sont liés à l'infrastructure du cloud, hybride ou virtuelle. Lorsque vous possédez un cloud hybride, vous devez gérer deux composants : le cloud interne privé et le cloud public, sans oublier les interfaces entre les deux. Si vous possédez un cloud privé, vous devez suivre et gérer l'infrastructure virtuelle qui permet son fonctionnement.

Kaseya Traverse est une solution de surveillance de réseau complète qui s'exécute sur les différentes infrastructures sur site, cloud ou hybrides. Elle peut surveiller les performances, afin que le réseau et tous les services qu'il offre respectent les niveaux de service requis.

Avec Traverse, l'équipe IT peut afficher cette infrastructure complexe grâce à des vues de service. Par exemple, tous les composants de réseau et de centre de données qui prennent en charge le service « Paiement » peuvent être affichés de manière holistique, même si les composants sont dispersés dans l'infrastructure. Cette vue orientée service permet de générer

La bonne solution de gestion des systèmes IT, avec des fonctionnalités à distance puissantes et des fonctionnalités de gestion des politiques, peut faire économiser de nombreuses heures de travail à l'IT de la vente au détail et diminuer radicalement les coûts de support.

Kaseya®

une analyse rapide de la cause première ; ainsi, les problèmes de réseau et de service sont résolus rapidement et n'empêchent pas le bon déroulement des opérations de vente au détail.

Découvrez plus d'informations sur Kaseya Traverse. **Cliquez ici**

Étude de cas :

Redbox maintient des milliers de kiosques en activité grâce à la gestion de point de terminaison à distance

Si vous êtes déjà allé dans un supermarché ou même un McDonald's aux États-Unis, vous avez sans doute croisé un kiosque de location de DVD Redbox. Il en existe des milliers dans le pays, et chacun doit être conservé en état de marche afin que les clients ne soient pas déçus. C'est pour cela que Redbox a défini un objectif de temps de fonctionnement de 99,5 % pour les unités basées sur PC.

Redbox a mis en place des superviseurs régionaux qui approvisionnent les kiosques en DVD. Pendant un temps, ces mêmes superviseurs étaient responsables de l'entretien des unités.

Ils devaient donc se déplacer pour mettre à jour la machine ou la réparer.

« Malgré le nombre de superviseurs régionaux engagés, nous rencontrions toujours un délai entre le moment où un système tombait en panne et celui où quelqu'un se déplaçait pour diagnostiquer le problème et le remettre en ligne », explique Eric Hoersten, vice-président IT de Redbox.

Redbox avait besoin d'une meilleure méthode et a adopté le logiciel de gestion de point de terminaison de Kaseya.

Aujourd'hui, les milliers de kiosques Redbox sont tous gérés de manière centralisée ; les opérations comprennent l'installation de correctifs et mises à jour Windows, la mise à jour du logiciel propriétaire utilisé par les kiosques, ainsi que la surveillance et la réparation des systèmes à distance.

Une conformité complète

De nombreux kiosques Redbox acceptent les cartes de paiement et doivent donc être conformes à la norme de sécurité de l'industrie des cartes de paiement (PCI DSS, Payment Card Industry Data Security Standard).

La solution de gestion des systèmes à distance Kaseya maintient tout ce matériel à jour grâce aux correctifs, et le protège des attaques. Si un audit de conformité PCI se profile, Kaseya produit des journaux et rapports exhaustifs pour prouver la conformité des appareils.

Pour plus d'informations, vous pouvez lire l'étude de cas complète **ici.**

« Kaseya VSA a immédiatement modifié le mode de gestion de nos kiosques. VSA nous permet de diagnostiquer et de dépanner à distance tous les problèmes qui se produisent. Il nous a permis de passer d'une gestion réactive à une gestion proactive. Désormais, nous pouvons éliminer les problèmes avant qu'ils ne se produisent, pour une disponibilité continue. »

Eric Hoersten
Vice-président IT
Redbox

À PROPOS DE KASEYA

Kaseya® est leader dans l'apport de solutions complètes de gestion IT destinées aux MSP et PME. Kaseya permet aux organisations de gérer et de sécuriser efficacement l'IT en vue de propulser les services informatiques et le succès des entreprises. Proposées aussi bien en tant que solution de pointe en matière de cloud que logiciels sur site, les solutions Kaseya permettent aux entreprises de contrôler tout leur système informatique de manière centralisée, de gérer aisément les environnements distants et distribués, et d'automatiser les fonctions de gestion informatique dans leur ensemble. À l'heure actuelle, les solutions Kaseya gèrent plus de 10 millions de points de terminaison dans le monde et sont utilisées par des clients de nombreux secteurs d'activité, notamment le commerce au détail, l'industrie manufacturière, la santé, l'éducation, l'administration, les médias, la technologie, les finances et autres. Kaseya, dont le siège social se trouve à Dublin (Irlande) est une société privée présente dans plus de 20 pays. Pour en savoir plus, rendez-vous sur le site **www.kaseya.com**

Rév. 070716

Kaseya®