L'adoption du cloud stimule la productivité, mais complique la réglementation des données. Nous sommes là pour vous aider.

Garantissez la sécurité de vos données tout en facilitant l'adoption du cloud

kaspersky BRING ON THE FUTURE

Introduction

Les organisations accélèrent depuis longtemps l'adoption du cloud pour renforcer la cohésion et stimuler la productivité. Cependant, depuis le début de la pandémie, cette tendance s'est emballée. La sécurité a été laissée de côté, et les entreprises le découvrent à leurs dépens.

Aujourd'hui, près de la moitié de toutes les violations de données[1] se produisent dans le cloud. Ce constat ne devrait pas surprendre, étant donné que les entreprises s'appuient sur un nombre important de fournisseurs de services dans le cloud dont la maturité informatique dépasse de loin la leur. Mais même si le fournisseur peut avoir tout sous contrôle de son côté, il ne s'agit là que de la moitié du travail.

La sécurisation de vos données au niveau de votre organisation est la clé d'une adoption sûre du cloud, et ce résultat ne peut être atteint que grâce à la visibilité. Peu d'organisations sont en mesure de classer toutes leurs données. Et faute de visibilité, vous risquez de vous retrouver en situation de non-conformité, ou pire, de faire face à des violations qui pourraient entraîner des amendes, des atteintes à votre réputation ou même une perte d'activité.

Pourtant, il est possible de procéder autrement et de faire de l'adoption du cloud un jeu d'enfant. En portant une attention particulière aux données de votre entreprise, il est plus facile de les classer, de les suivre et de les protéger, ce qui vous permet d'accélérer sans crainte votre migration vers le cloud.

Dans cet article, nous aborderons les risques liés à l'adoption du cloud, nous examinerons les origines de la faiblesse de la sécurité des données et, enfin, nous vous aiderons à reprendre le contrôle du cloud.

La hausse de l'adoption du cloud

Des avantages comme l'évolutivité, l'économie et la portée encouragent les entreprises à migrer vers le cloud ainsi qu'à adopter la transformation numérique. Ce phénomène s'est accéléré depuis le début de la pandémie, les entreprises cherchant à stimuler leur collaboration et leur productivité tout en étant géographiquement dispersées. La ruée pour faciliter la généralisation du télétravail distance était telle que Microsoft a connu deux ans de transformation numérique en deux mois seulement[2], et qu'aujourd'hui, 90 % des entreprises[3] passent plus de temps dans le cloud.

Les PME gèrent des charges de travail moins importantes que les grandes entreprises, mais elles sont en fait celles qui adoptent le plus rapidement le cloud[4]. Dans leur volonté de faciliter le télétravail, 53 % d'entre elles dépassent désormais 1,2 million de dollars par an[5] pour l'informatique dans le cloud. Les avantages sont bien sûr nombreux. Capital One, par exemple, a réduit le temps de création de l'environnement de développement[6] de plusieurs mois à quelques minutes en procédant à une migration vers le cloud ; AppLovin a réduit de 25 % la latence[7] de sa plateforme d'enchères, et J.B. Hunt a augmenté de 10 % la satisfaction de ses utilisateurs[8].

Cependant, certaines entreprises sont méfiantes et pensent qu'il est plus sûr de conserver les opérations informatiques sur place que de les externaliser. Bien qu'il ne soit pas facile de renoncer à votre contrôle technologique, un tiers peut protéger vos données mieux que vous ne le pensez, surtout si vous choisissez le partenaire approprié.

Public ou privé : l'histoire de deux clouds

Tous les clouds ne sont pas égaux. Le **modèle de cloud privé** est essentiellement un hébergement de données privé : un cloud pour une organisation et aucune ressource partagée. Il est particulièrement apprécié dans les secteurs où les réglementations en matière de données sont les plus strictes, comme les gouvernements, les services de santé et le secteur financier, où le coût d'une violation peut se chiffrer en millions de dollars.

Cloud privé

Avantages	Inconvénients
Sécurité	Prix
Sur mesure	Gourmand en ressources
Optimisé	Difficile à faire évoluer
	Accès à distance limité

Le **modèle de cloud public** consiste à mettre des éléments numériques à la disposition du public sur Internet. Ces services sont généralement des services d'abonnement (par exemple, un logiciel en tant que service (SaaS)), et le fournisseur de services dans le cloud (CSP) s'occupe du matériel, des logiciels ainsi que de l'infrastructure correspondante. Les principaux acteurs dans ce domaine sont Amazon Web Services (AWS), Google Cloud Platform (GCP) et Microsoft Azure.

Cloud public

Avantages	Inconvénients
Évolutif	Doutes sur la conformité
Rentable	Moins de sécurité
Fiabilité	Effort de migration
Peu d'efforts	

O'Reilly a constaté que deux tiers des organisations[3] se servent d'un cloud public, ce qui est plus que celles qui utilisent une infrastructure sur site (55 %) ou un cloud privé (45 %). La plupart de ces organisations ont également déclaré faire appel à plusieurs fournisseurs de services dans le cloud, ce qui complique de plus en plus la question de la sécurité des données.

Il est important de choisir le modèle qui convient à la fois aux fonctions existantes de votre entreprise et à son potentiel de croissance, tout comme il est essentiel de disposer d'une visibilité sur les données que vous contrôlez.

Ce que l'adoption croissante du cloud signifie pour la sécurité des données

Près de la moitié de toutes les violations de données[1] se produisent désormais dans le cloud. La vitesse à laquelle nous avons évolué (la plupart d'entre nous poussés par la pandémie) a laissé la sécurité jouer les seconds rôles, et la moitié de tous les acteurs qui ont adopté le cloud[9] sont concernés. Neuf utilisateurs sur dix[10] stockent des données confidentielles dans le cloud (public ou privé), et les 10 % qui ne le font pas ont fait part de leurs préoccupations en matière de conformité et de contrôle. Bien que ces préoccupations puissent être abordées avec le bon soutien technologique (ce dont nous parlerons sous peu), elles ne sont pas disproportionnées : 45 % des organisations[11] ont déjà été confrontées à une violation des données dans le cloud ou ont échoué à un audit impliquant des données dans le cloud. Cela prouve que même les données que vous considérez comme étant sécurisées peuvent devenir problématiques si les contrôles appropriés ne sont pas mis en place.

Risques de sécurité des données dans le cloud public

Lorsque vous utilisez un cloud public, trois parties sont généralement impliquées : votre organisation, vos clients et le fournisseur de services cloud. En cas de violation des données, votre organisation est considérée comme le propriétaire des données, vos clients comme la personne concernée et votre fournisseur de services cloud comme le détenteur des données. (Si des secrets d'entreprise comme des bilans sont divulgués, alors votre organisation est également la personne concernée.)

Lors d'une violation, le responsable du traitement des données (c'est-à-dire vous) est souvent pointé du doigt. Toutefois, dans le bon contexte **et avec les bonnes preuves à votre disposition**, il est possible que le détenteur des données (ici le fournisseur de services) soit tenu pour responsable. Cela pourrait vous faire gagner du temps, de l'argent et de la crédibilité.

Il est essentiel d'avoir une visibilité sur vos données afin de pouvoir classer vos informations (pensez aux bases de données clients) et gérer les risques associés. Vous devriez poser les questions suivantes dès que possible au cours de votre migration vers le cloud :

- Disposez-vous de l'expertise et/ou des ressources nécessaires pour maintenir des normes de sécurité élevées pour le cloud ?
- À quelle industrie ou réglementation gouvernementale devez-vous vous conformer ?
- Quelles données sont sous votre contrôle ?
- Qui peut accéder à ces données ?

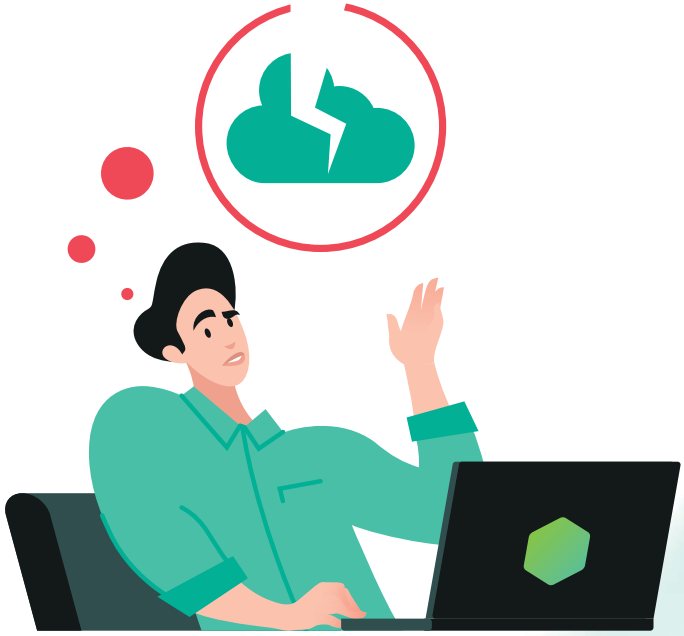
Avant de discuter davantage de la visibilité des données, examinons le rôle d'un acteur clé de la sécurité des données dans le cloud : votre personnel.

Le facteur humain

Il existe plusieurs façons pour une partie non autorisée d'accéder à vos données confidentielles dans le cloud, mais vos employés sont les premiers à pouvoir le faire. Neuf PME sur dix[12] qui ont subi une violation des données touchant leur infrastructure de cloud public ont déclaré que l'ingénierie sociale avait joué un rôle dans l'attaque. Les trois principaux types de données volées étaient les informations personnellement identifiables (PII), les informations de paiement des clients et les identifiants d'authentification des utilisateurs. Ils sont tous annonciateurs d'ennuis, pourtant leur compromission découle souvent d'incidents a priori anodins, notamment :

- Un employé qui laisse un ordinateur portable sans surveillance dans un café
- Un spécialiste du marketing qui partage les détails de son compte avec une agence tierce
- Un ingénieur fatigué qui fait des concessions au détriment de la sécurité des fichiers

Vous pouvez minimiser le risque d'attaques par ingénierie sociale en utilisant une solution de sécurité des terminaux qui protège les serveurs de messagerie, les clients ainsi que les navigateurs. Toutefois, de nombreux produits effectuent cette tâche seuls et ne parviennent pas à assurer la surveillance nécessaire au suivi des données sur les plateformes dans le cloud. Et vous ne pouvez pas protéger ce que vous ne pouvez pas voir.



Cet écart entre l'efficacité perçue des contrôles de sécurité des fournisseurs de services cloud et la confiance dans les capacités des organisations à protéger les données confidentielles dans le cloud pourrait être dû à la différence de ressources de sécurité lorsque l'on compare les fournisseurs de services et les utilisateurs du cloud. De même, cette situation souligne le besoin des organisations de mettre en place des mesures de sécurité supplémentaires au-delà des fonctionnalités de sécurité intégrées des fournisseurs de services dans le cloud.

– The Cloud Security Alliance,
« Les données sensibles dans le cloud »

Les organisations manquent de confiance

Selon la Cloud Security Alliance[10], la plupart des entreprises estiment que les contrôles de sécurité de leur fournisseur de services cloud sont efficaces, mais elles **manquent de confiance dans leur propre capacité** à protéger les données confidentielles dans le cloud. (Seul un quart des entreprises font plus que « modérément confiance » à leur capacité à protéger les données confidentielles dans le cloud.) Cette incertitude va de pair avec l'inaction : 43 % des entreprises[1] n'ont pas encore commencé à appliquer des pratiques de sécurité à leur environnement cloud ou n'en sont qu'aux premiers stades de cette initiative.

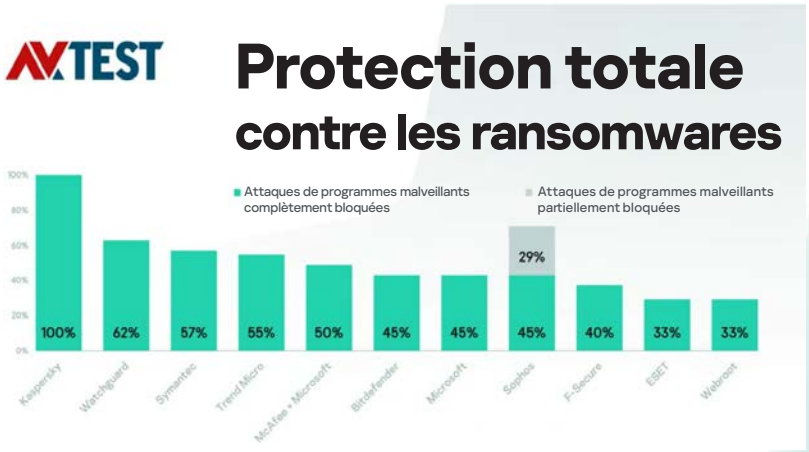
Étant donné que votre organisation est plus susceptible d'être victime d'une violation à la suite d'une ingénierie sociale que d'une erreur de votre fournisseur de services cloud, il est important d'établir des mesures qui protègent vos terminaux et assurent la visibilité des données dans vos environnements cloud. À l'heure actuelle, 22 % des organisations[11] ne peuvent classer que très peu de leurs données, et un quart seulement peut les classer toutes. Une mauvaise gestion de ces données peut entraîner des violations qui coûtent aux PME des millions de dollars par an.

Prenez le contrôle de vos données avec Kaspersky Endpoint Security Cloud

Nous pouvons vous aider à prendre le contrôle de la sécurité et de la conformité de vos données, où que vous soyez dans votre migration vers le cloud. Vous n'avez pas besoin de dépenser des sommes colossales pour suivre le rythme de sécurité imposé par les fournisseurs de services cloud. **Kaspersky Endpoint Security Cloud**, notre principale offre pour les PME, fournit la protection simple et abordable dont vous avez besoin pour vous mettre à la page et éviter les violations de données. Mieux encore, vous serez prêt en quelques minutes, grâce à une configuration facile directement depuis le cloud.

Première ligne de défense

Kaspersky Endpoint Security Cloud offre des fonctionnalités étendues de sécurité des données dans le cloud, mais assure également une protection de base en vous protégeant contre les menaces connues et avancées, les ransomwares (protection à 100 %[13]) ainsi que le phishing – la cause première de nombreuses violations. De plus, nous détecterons et corrigerons les vulnérabilités présentes dans vos systèmes afin que vous puissiez vous concentrer sur ce que vous faites le mieux.



Data Discovery (et protection des données)

Vous pouvez faire de l'utilisation inappropriée d'applications dans le cloud un problème du passé grâce à Cloud Discovery, un outil qui vous aide à trouver puis à restreindre l'utilisation de ressources dans le cloud inappropriées ou non autorisées. Les sources de violation potentielle de données sont rapidement suivies et éliminées, vous aidant ainsi à maintenir la confiance et la conformité.

Les modèles pré-configurés vous permettent d'identifier facilement les informations confidentielles et sensibles liées aux DPI* ainsi qu'aux données de paiement. Vous serez informé des partages sur Teams, OneDrive, SharePoint (**presque tous les services Microsoft Office 365**) ce qui vous permettra d'appliquer des mesures correctives pour préserver l'intégrité des données et répondre aux critères de conformité.

Et même si un appareil est perdu ou volé, vous pouvez protéger vos données grâce aux mécanismes de chiffrement à distance.

AV-TEST

Informations d'identification personnelles
Protection : données sensibles
Test de découverte.

En savoir plus

Consultez la liste complète de nos services pour Data Discovery.

Confiance en la conformité

Nous comprenons que les règlements locaux comme le Règlement général sur la protection des données (RGPD) peuvent être intimidants lorsque vous cherchez à migrer vers le cloud. Des dizaines d'articles doivent être respectés, et cette tâche peut vite devenir accablante. Cependant, Kaspersky Endpoint Security Cloud vous donnera la confiance et les outils nécessaires pour vous mettre en conformité.

Par exemple, selon l'article 32 du RGPD « Sécurité du traitement », vous avez l'obligation de garantir un niveau de sécurité des données correspondant au niveau de risque présenté par les données personnelles traitées, ainsi que de veiller à ce que quiconque bénéficiant d'un accès aux données personnelles ne traite pas celles-ci (sauf sur vos instructions et conformément aux exigences légales).

C'est toute une déclaration. Voici comment nous la simplifions :

Vos conditions	Notre solution
Vérifiez où vous stockez vos données	**Data Discovery** vous permet de détecter le traitement et le stockage de données personnelles dans les services accessibles par des tiers, susceptibles d'entraîner une violation de données
Déterminez pourquoi vous stockez vos données et pour combien de temps	**Data Discovery** vous permet de détecter des données stockées plus longtemps que nécessaire (ou que la durée spécifiée par votre politique de conservation des données)
Trouvez des moyens de contrôler l'accès des utilisateurs aux données	**Le contrôle des appareils** empêche les utilisateurs de connecter des appareils externes et amovibles (autres que ceux approuvés par le service informatique) à leur ordinateur afin de déplacer des données
Implémentez des mécanismes de protection des données comme le chiffrement des appareils mobiles	**La gestion du chiffrement** protège les données en cas de perte ou de vol d'un appareil, quel que soit l'endroit où il se trouve
Évaluez vos niveaux de risque en matière de sécurité des données	Une visibilité totale au fur et à mesure de votre croissance

Nos recherches ont révélé qu'une PME ne détient en moyenne qu'environ 160 fichiers contenant des données sensibles dans son stockage dans le cloud, et que seulement 15 % d'entre eux (environ 24 fichiers) sont partagés à l'extérieur de l'entreprise. Les rapports continus de Kaspersky Endpoint Security Cloud et la résolution manuelle occasionnelle d'un partage risqué sont tout ce dont vous avez besoin pour rester en conformité.

Conclusions

Votre adoption du cloud s'accélère-t-elle ? Il est temps de mettre vos données en lumière pour que vous puissiez en profiter sans avoir à surveiller vos arrières. Dans ce document, nous avons fait le point sur l'adoption croissante et les immenses avantages de l'utilisation du cloud, tout en mettant en évidence vos sujets de préoccupation. Grâce à nous, vous pouvez minimiser le risque de violation des données dans le cloud, respecter les réglementations et protéger votre entreprise des menaces habituelles, le tout via un navigateur Web.

Kaspersky Endpoint Security Cloud se décline en trois versions et est proposé par appareil, ce qui signifie que vous payez uniquement pour ce dont vous avez besoin.

Il est temps de se tourner vers l'avenir.
Obtenez votre essai gratuit de 30 jours dès aujourd'hui.

À propos de Kaspersky

Kaspersky protège plus de 400 millions d'utilisateurs et 240 000 entreprises. Est. 1997.

Nous sommes une entreprise internationale privée dont la société holding est établie au Royaume-Uni.

Nous transformons nos renseignements de sécurité de pointe en une protection réelle pour nos clients. Nous vous donnons les moyens d'utiliser les technologies au quotidien et au travail en toute sécurité et en toute confiance.

Plus de 25 ans

d'expérience dans le secteur de la cybersécurité

Plus de 400 millions

de clients utilisent nos produits dans le monde entier

Plus de 200

pays tirent parti de nos solutions

Bibliographie

1. IBM. (2022). Rapport sur le coût d'une violation de données. IBM.
2. Spataro, J. (2020, 30 avril). Deux ans de transformation numérique en deux mois. Microsoft.
3. Loukides, M (2021, 7 décembre). Le cloud en 2021 : l'adoption se poursuit. O'Reilly.
4. Grand View Research. (2021). Rapport sur la taille du marché de l'informatique dans le cloud. Grand View Research.
5. Flexera. (2022). Rapport sur l'état du Cloud. Flexera.
6. Amazon AWS. (2020). Capital One achève la migration de ses data centers vers AWS et devient la première banque américaine à annoncer qu'elle se tourne entièrement vers le cloud. Amazon AWS.
7. Mehta, N & Birnbaum, J. (2021, 23 juillet). AppLovin s'appuie sur Google Cloud pour transformer le marketing mobile. Google Cloud
8. Google Cloud. (2021). J.B. Hunt effectue une migration rapide et transparente de cloud à cloud. Google Cloud
9. Nutanix. (2021). 4e indice annuel Nutanix Enterprise Cloud. Nutanix.
10. Cloud Security Alliance. (2022, 7 décembre). Données sensibles dans le cloud. Cloud Security Alliance.
11. Thales. (2022). Étude de Thales sur la sécurité du cloud de 2022. Thales.
12. Kaspersky. (2019). Comprendre la sécurité du cloud. Kaspersky.
13. Kaspersky. (2022, 19 juillet). AV-TEST constate que les solutions de sécurité Kaspersky pour les entreprises offrent une protection à 100 % contre les ransomwares. Kaspersky Lab.

Actualités sur les cybermenaces : www.securelist.com
Actualités dédiées à la sécurité informatique : business.kaspersky.fr
Sécurité informatique pour les PME : kaspersky.fr/small-to-medium-business-security
Sécurité informatique pour les entreprises : kaspersky.fr/enterprise-security
Portail de Threat Intelligence : opentip.kaspersky.com
Catalogue produits pour les entreprises : https://media.kaspersky.com/fr/business-security/enterprise/KL-Enterprise-Catalogue.pdf

www.kaspersky.fr

Reconnu. Indépendant. Transparent. Nous nous engageons à construire un monde plus sûr, dans lequel la technologie améliore notre vie. C'est pourquoi nous la sécurisons, afin que le monde entier dispose des possibilités infinies qu'elle nous offre. Adoptez la cybersécurité pour un avenir plus sûr.

Pour en savoir plus, rendez-vous sur kaspersky.fr/about/transparency

Proven.
Transparent.
Independent.