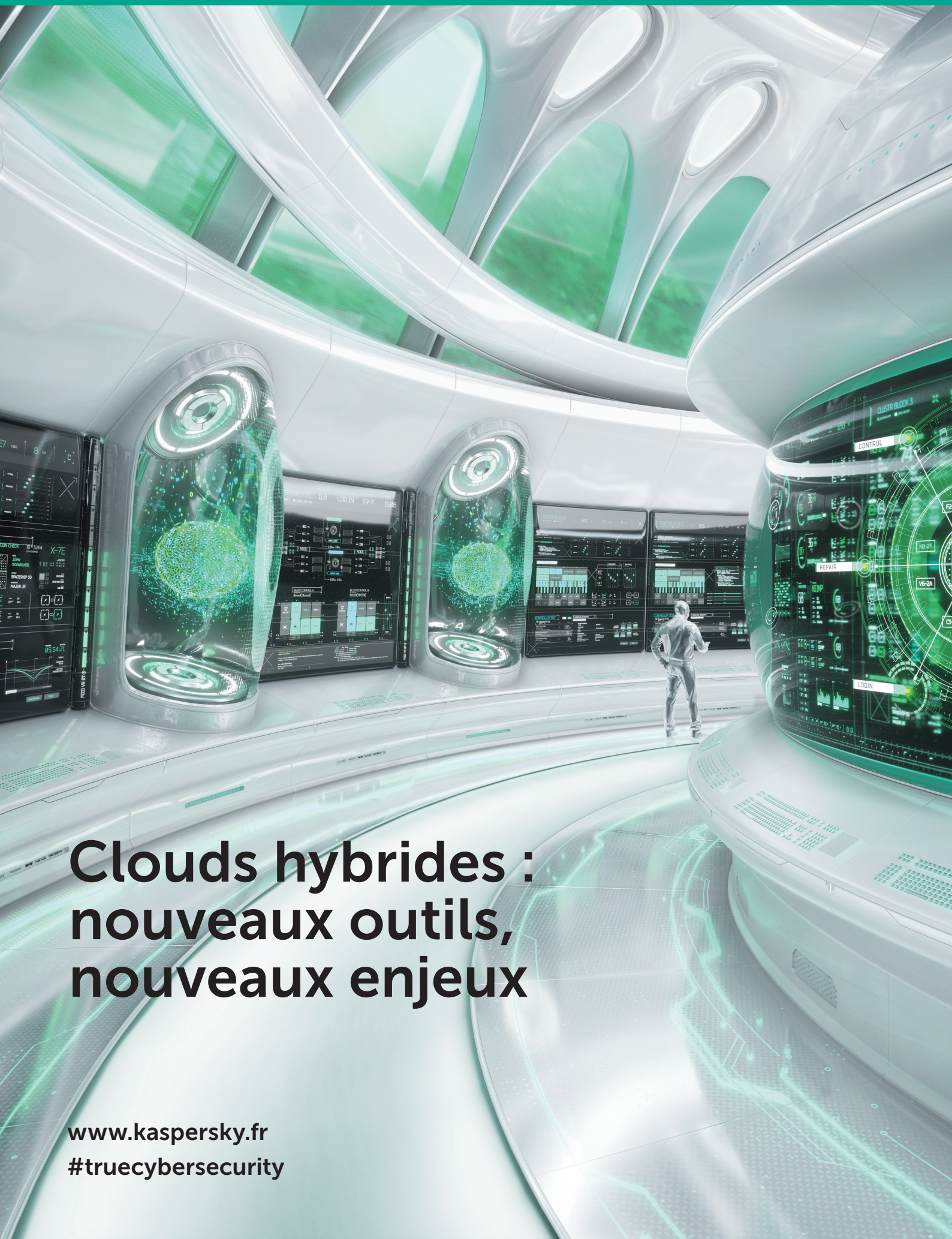
kaspersky



Clouds hybrides : nouveaux outils, nouveaux enjeux

www.kaspersky.fr
#truecybersecurity

« Votre transformation ne sera jamais terminée. Elle évoluera constamment. »

Forrester, The Sorry State of Digital Transformation in 2018 (Forrester, Le triste état de la transformation numérique en 2018)

« D'ici 2020, l'essentiel de l'activité de 50 % des 2 000 plus grandes entreprises mondiales dépendra de leur capacité à créer des produits, services et expériences numériquement améliorés. »

IDC, Preparing for the Digital Transformation Economy: The Tools Needed to Build a Digitally Native Enterprise (Se préparer à l'économie de la transformation numérique : les outils nécessaires à la création d'une entreprise « native du numérique »)

Selon une étude menée par IDC en 2017 :

« **L'efficacité médiane de la technologie dans le secteur de l'informatique d'entreprise ne dépasse pas les 50 %.** Ce manque d'efficacité est à la fois dû à une surdistribution en termes de redondance et de résilience et à une sous-utilisation permanente des capacités et des performances, ce qui se traduit par un grand nombre d'heures d'inactivité pendant lesquelles l'infrastructure n'est au service d'aucune application. »

Quantifying Datacenter Inefficiency: Making the Case for Composable Infrastructure (Quantifier l'inefficacité des data centers : sensibilisation à l'infrastructure composable - Parrainé par Hewlett Packard Enterprise), Ashish Nadkarni, mars 2017

« Le data center type doit prendre en charge un grand nombre de systèmes d'exploitation, de logiciels de bases de données et de middlewares. Ce qui complique l'administration et la maintenance des systèmes - et fait grimper les coûts. Quant à l'utilisation des serveurs, elle est souvent limitée, avec un trop grand nombre de processeurs inactifs ou presque. Cette mauvaise utilisation entraîne souvent une augmentation des exigences en termes de capacité des data centers, ainsi que des investissements matériels inutiles et de grosses factures d'électricité. »

Strategy& (anciennement Booz&Co) Keeping the Data Center Competitive: Six Levers for Boosting Performance, Reducing Costs and Preparing for an On-Demand World (Compétitivité des data centers : six leviers pour doper les performances, réduire les coûts et se familiariser avec un monde de services à la demande) (p. 5)

Transformation numérique - une fin sans fin

La transformation numérique n'a rien à voir avec les projets de gestion du changement traditionnels. Car elle est faite pour être sans fin.

Si les entreprises veulent gagner en efficacité pour pouvoir survivre aux décennies à venir, elles doivent impérativement aborder la transformation numérique comme une *attitude* permanente et durable, et non comme un projet. Une attitude qui aura un impact sur leur bilan - indéfiniment.

Tandis que l'objectif de la transformation numérique est le changement perpétuel, son fruit est plus concret puisqu'il s'agit du retour sur investissement. Une transformation numérique efficace élimine les obstacles qui entravent généralement l'efficacité des ressources et, par conséquent, l'évolutivité.

Une nouvelle forme d'agilité

Le terme *agilité* est tellement employé au sein des entreprises qu'il a fini par perdre un peu de son sens, probablement à cause de la familiarité que provoque la sur-utilisation. Pourtant, en matière de transformation numérique, *l'agilité* est un concept essentiel qui mérite d'être abordé avec un œil neuf.

Grâce à la transformation numérique (et en particulier à la migration vers le cloud), les entreprises bénéficient d'une toute nouvelle forme d'agilité que ne confèrera jamais aucun système hérité rigide ni aucune infrastructure interne coûteuse.

Pourquoi la migration vers le cloud n'est-elle que la première étape d'un voyage sans fin ?

La migration vers le Cloud est désormais incontournable. En fait, il s'agit de la première étape d'une transformation numérique sans fin devenue essentielle pour les entreprises du monde entier.

Seul le Cloud offre l'évolutivité, la fiabilité et la disponibilité dont les entreprises ont besoin si elles ne veulent pas se contenter de survivre. *Seul le Cloud* offre la flexibilité qui permet aux organisations de « reculer pour mieux sauter », et de rebondir de façon décisive et précise chaque fois que cela s'avère nécessaire. *Seul le Cloud* offre une véritable agilité, avec sa capacité à répondre, instantanément et en permanence, aux besoins d'un horizon de données en constante évolution.

Mais il y a clouds et clouds

La plupart des organisations disposent déjà d'au moins une charge de travail dans le Cloud. Ce qui ne veut pas forcément dire qu'elles ont opéré leur transformation numérique.

Le degré d'adoption du Cloud varie considérablement d'une région, d'un secteur et d'une organisation à l'autre. Et, stricto sensu, il n'existe pas de solution Cloud unique :

Il y a mieux que la solution unique :

Le modèle de Cloud hybride est une solution *universelle*.

Le modèle de Cloud hybride permet aux organisations de configurer des orchestrations sur mesure, avec les avantages des deux mondes, qui s'adaptent et répondent à l'évolution de leurs exigences numériques spécifiques. La capacité de traitement est toujours prête (même sans préavis) à répondre à ces exigences sans que les entreprises aient besoin de payer des serveurs inactifs en veille, tels onze footballeurs remplaçants trépignant d'impatience sur le banc de touche.

L'efficacité des ressources des Clouds hybrides est telle qu'ils éclipsent d'un seul coup les révolutions qu'ont représenté l'externalisation des data centers et les services d'infrastructure.

L'élégante synergie qu'offre le modèle hybride entre Cloud privé et Cloud public montre que le rêve de transformation numérique durable est enfin une réalité. *Totalement libérées des limites de l'infrastructure interne et des solutions externalisées rigides,* rien n'empêche désormais les entreprises d'atteindre des sommets en matière d'efficacité des ressources et d'agilité.

Nouvelle liberté, nouvelles responsabilités

La liberté d'évolution et de transformation offerte par les Clouds hybrides s'accompagne d'une série de cyberdéfis et de responsabilités en matière de sécurité.

Tous ces défis tournent autour d'un constat essentiel :

Le Cloud hybride ne ressemble à rien de ce qui existait jusqu'à présent. Par conséquent, les anciens outils n'ont plus lieu d'être.

Les entreprises disposaient jusqu'à présent de « portefeuilles » de services de données, principalement composés des éléments suivants :

- Infrastructure / équipements internes
- Externalisation des data centers
- IaaS
- Clouds privés
- Clouds publics, tels qu'AWS et Microsoft Azure

Il existe une énorme différence entre l'assemblage d'un portefeuille de services sur mesure et la migration vers un modèle de Cloud hybride.

Le portefeuille est un ensemble de services disparates, chacun répondant à un besoin spécifique. Et ces services ne travaillent pas nécessairement de concert.

À l'inverse, le Cloud hybride est une solution entièrement intégrée, holistique, *heuristique* et dynamique qui repose principalement sur des *flux*.

« Des transformations numériques sont en cours dans plus de la moitié des entreprises, mais rares sont celles qui sont passées à l'étape supérieure pour optimiser des fonctions ou des canaux individuels. Le capital politique privilégiant l'analogique et orienté silo continue de favoriser l'inertie. »

Forrester: The Future of Organizations (L'avenir des organisations), p. 4

Les Clouds hybrides et l'ère des *flux*

La frontière entre Cloud public et Cloud privé est floue, presque invisible : non pas parce qu'elle n'existe pas, mais parce qu'il est désormais très facile pour les organisations de permettre à leurs données de *circuler* en toute transparence entre les deux. La véritable beauté de ces flux de données vient du fait qu'ils varient *en fonction de l'orchestration du Cloud hybride unique* que chaque entreprise configure pour répondre à la perfection à ses besoins (évolutifs).

Selon un rapport d'IDC, les flux font partie des besoins changeants qui accompagnent l'adoption du Cloud hybride. Ils y sont décrits comme « un tout nouveau monde en termes de besoins de sécurité dans la mesure où les données circulent librement d'un bout à l'autre du Cloud ».

IDC White Paper: The Power of Hybrid Cloud (Livre blanc IDC : La puissance du cloud hybride - Parrainé par Dell)

Ces flux, propres aux Clouds hybrides, ne ressemblent à rien de ce qui a existé dans l'histoire de l'évolution numérique.

Car ce sont eux qui garantissent l'efficacité des ressources et la flexibilité des Clouds hybrides. C'est la raison pour laquelle le Cloud hybride n'a pas plus de points communs avec les systèmes de données antérieurs que la mécanique quantique n'en a avec la théorie de Newton.

« Le Cloud hybride ne consiste pas simplement à connecter un data center local à un Cloud public et à déplacer les charges de travail entre les deux. Les Clouds interne et externe doivent être orchestrés pour travailler ensemble comme un système unique. »

IDC White Paper: Journey to the Cloud (Livre blanc IDC : Voyage vers le cloud - Parrainé par VMware)

Il va de soi que la protection et la facilitation de ces flux avantageux doivent être en tête de la liste des priorités des entreprises qui, après avoir opéré l'essentiel de leur migration vers le Cloud hybride, peuvent maintenant espérer dégager un retour sur investissement sans précédent.

De la même manière, toute perturbation de ces flux peut avoir de graves conséquences. En fait, toute interruption des flux des Clouds hybrides reviendrait à *réduire à néant les bienfaits de la transformation numérique*.

Nouveau monde, nouveaux outils

Comme vous le dira n'importe quel bijoutier, vous ne pouvez pas travailler l'or avec des outils faits pour l'acier.

Tout comme l'or, le Cloud hybride s'accompagne de nouvelles exigences et de nouveaux défis. Pour protéger les *flux*, les organisations doivent mettre en œuvre des réponses à la fois éprouvées et taillées sur mesure pour les infrastructures hybrides. Il est désormais plus important que jamais de se doter d'une sécurité adéquate.

Une entreprise doit respecter trois conditions pour assurer le retour sur investissement de son Cloud hybride :

1) Identifier le profil de risque et de menace unique qui s'applique aux Clouds hybrides
2) Comprendre les limites de la « responsabilité partagée »
3) Répondre de façon appropriée aux deux conditions précédentes

Examinons de plus près chacun de ces trois points.

« L'hybride est probablement l'avenir du Cloud. »

Forrester: Hybrid Cloud: An Obvious Reality Or A Conservative Strategy? (Cloud hybride : une réalité évidente ou une stratégie conservatrice ?)

Identifier le profil de risque et de menace unique qui s'applique aux Clouds hybrides

Au premier abord, on peut penser que la sécurité du Cloud hybride se gère comme une guerre sur plusieurs fronts. Et, par extension, que le théâtre de cette guerre (électronique) est un véritable chaos, où la défense (à condition qu'elle soit possible) est épuisante en termes de ressources.

Certes, l'implication de multiples ressources et de multiples couches nécessite une évaluation *pluraliste* du risque et de la menace. Dans une certaine mesure, le Cloud hybride peut être comparé à une chaîne de données dans laquelle les entreprises ne peuvent pas tolérer le moindre maillon faible.

L'important déploiement de ressources qu'implique la « micro-surveillance » de chacun des maillons de cette chaîne peut considérablement freiner l'adoption du Cloud et nuire à la productivité. Lorsqu'une telle approche est adoptée (souvent, hélas, par défaut plutôt qu'à dessein), les entreprises ont encore plus de mal à profiter des avantages de la transformation numérique.

Mais ce n'est que la partie émergée de l'iceberg.

Les vrais problèmes causés par la micro-surveillance sont bien plus profonds. Le recours à une multiplication anarchique d'outils de sécurité peut être tellement lourd à gérer qu'il peut *augmenter la probabilité* d'incursions de cybermenaces.

Une armée épuisée ne gagne jamais.

L'intervention sur plusieurs fronts de cybermenaces n'est pas pour autant une bataille perdue d'avance. Au contraire, si vous êtes conscient que la cyberbataille du Cloud hybride se déroule sur plusieurs fronts, vous avez déjà remporté la moitié de cette bataille.

Comprendre les limites de la « responsabilité partagée »

On considère souvent que le modèle de sécurité dans le cloud hybride repose sur la « responsabilité partagée ». C'est à la fois vrai et faux. Dans une certaine mesure, les Clouds publics comme AWS et Microsoft Azure disposent de leur propre sécurité native qu'ils partagent avec leurs clients.

Cela dit, la sécurité native de ce type de Clouds publics offre uniquement une protection contre les menaces externes. Elle n'est pas équipée pour faire face aux menaces provenant des machines virtuelles (ou introduites par celles-ci) et de l'intérieur du Cloud hybride. Sachant que les environnements de démonstration sont eux-mêmes vulnérables aux programmes malveillants, se reposer sur ses lauriers (ou sur ceux d'un fournisseur de Cloud public) n'est pas une option viable.

Les fuites constituent un risque majeur pour les organisations, pour leur réputation, mais aussi financièrement et juridiquement, de sorte qu'il est absolument essentiel que chaque entreprise aborde la sécurité en tenant compte de ses intérêts spécifiques.

« C'est à vous de veiller à ce que toutes les infrastructures internes et externes fournissent une protection cohérente. »

Forrester: Unlock the Value of Cloud: Spotlight on IT Executives (Libérer la valeur du cloud : pleins feux sur les cadres informatiques)

Rappelons que la fuite de données personnelles de 198 millions d'Américains (25 téraoctets) survenue en 2017 était due à une mauvaise configuration des seaux d'AWS. (Source : Forbes). En fait, PWC a nommément désigné les modèles de responsabilité partagée mal définis comme « responsables de failles dans les processus métier qui peuvent ensuite se traduire par des atteintes à la sécurité ». Source

« Les entreprises qui transfèrent des données vers le Cloud n'ont souvent que peu de visibilité sur les processus et procédures des fournisseurs de services Cloud (y compris sur les mises à jour techniques et les pratiques d'embauche) et n'ont donc qu'une vague notion des risques de sécurité auxquels le fournisseur est lui-même confronté. »

PWC : Cloud Computing: An Information Security Perspective (Cloud computing : un point de vue sur la sécurité des informations)

« Au bout du compte, la sécurité dans le Cloud doit être replacée dans le contexte du programme global de sécurité des informations de chaque entreprise, notamment en termes de gestion des risques, de gestion des incidents, de planification du maintien de l'activité et de gouvernance. Cela exigera des efforts de la part de tous ceux qui ont intérêt à assurer la sécurité des données transférées vers le Cloud. »

PWC : Cloud Computing: An Information Security Perspective (Cloud computing : un point de vue sur la sécurité des informations)

« Les entreprises doivent comprendre que le Cloud est un lieu à part où les données distribuées dictent une nouvelle façon d'envisager la sécurité. Une meilleure visibilité (en sachant où se trouvent vos données et qui y a accès) est essentielle. »

PWC : Cloud Security: How to Manage Six Common Pitfalls (Sécurité dans le cloud : comment éviter six pièges communs)

Une fois la migration (souvent complexe) vers le Cloud hybride effectuée, les organisations se doivent de saisir toutes les opportunités d'accroître l'efficacité de leurs ressources, et de poursuivre la réduction du coût et de l'encombrement de leur infrastructure.

« Les problèmes de sécurité sont en tête de la liste des défis liés au Cloud hybride. Pour développer un Cloud hybride sûr et fiable, les entreprises doivent commencer par établir de solides fondations de sécurité à l'aide de technologies connues et éprouvées. »

Forrester: Unlock the Value of the Cloud: a Spotlight on IT Executives (Libérer la valeur du Cloud : pleins feux sur les cadres informatiques)

« Les déploiements de Clouds hybrides requièrent une approche holistique de la sécurité. »

Three Must-Haves for Hybrid Cloud Security (Trois incontournables pour la sécurité dans le cloud hybride - CSO - IDG)

La sécurité native des fournisseurs de services de Cloud public tiers n'est pas suffisante pour protéger les entreprises du nombre croissant de cybermenaces, connues et inconnues.

Par conséquent, la « responsabilité partagée » ne doit pas être interprétée comme une responsabilité égale. Tandis que des éléments de sécurité natifs du Cloud prennent en charge certains fronts, la lutte globale doit être sous le commandement en chef de chaque organisation.

Comme toujours dans le monde des affaires, personne ne se soucie autant de votre bénéfice net que vous.

Répondre de façon appropriée

Les flux possibles au sein des Clouds hybrides doivent toujours rester sous le strict contrôle de l'entreprise qui les a configurés, et qui est désormais aux commandes.

Pour cela, l'entreprise doit bénéficier en temps réel d'une visibilité totale et panoramique sur les données de l'ensemble du Cloud hybride. Aucune bataille ne peut se gagner sans visibilité, et la cybersécurité ne fait pas exception à cette règle.

Dans le cas des Clouds hybrides, la visibilité doit être sans frontières, et la facilité de gestion est un compagnon indispensable. Les entreprises doivent savoir où se trouvent leurs charges de travail, et connaître l'état de celles-ci en temps réel.

Pour rendre cette visibilité panoramique et cette facilité de gestion encore plus performantes, efficaces et adaptées aux environnements des Clouds hybrides, la fonctionnalité de protection automatisée doit être activée, via les API natives du Cloud.

À chaque étape, la sécurité du Cloud hybride doit mettre l'accent sur la visibilité et la facilité de gestion, sans sacrifier ni l'une ni l'autre.

Les différents composants de l'architecture d'un Cloud hybride ne peuvent pas être assemblés n'importe comment - il ne s'agit pas d'un patchwork (ni des puzzles de données fragmentées et disparates d'autrefois).

Par nature, le Cloud hybride est transparent.

Notamment parce qu'il a été conçu à dessein, et non par hasard. De plus, les différents composants de chaque Cloud hybride ont été conçus pour évoluer (et continuer d'évoluer) les uns avec les autres, en parfaite symbiose.

Sans cette évolution symbiotique, les flux au sein des Clouds hybrides seraient impossibles.

Cela signifie que la sécurité doit être abordée via une approche holistique et symbiotique similaire.

Chacune des charges de travail du Cloud, sur l'ensemble du parc informatique, doit être protégée. Faute d'adopter cette approche, des problèmes d'alignement catastrophiques peuvent survenir entre la sécurité et l'infrastructure, exposant le Cloud hybride aux risques suivants :

- Violation de données
- Fuites de données
- Perte de données
- Absence d'intégrité critique
- Applications indésirables introduisant une vulnérabilité

En conclusion, une réponse appropriée au profil de risque et de menace unique inhérent à l'utilisation du Cloud hybride doit être :

1) holistique,
2) unifiée,
3) agile et capable d'évoluer parallèlement aux environnements de Clouds hybrides,
4) sous le contrôle de l'organisation dont les données (et les activités) sont en jeu.

« Ne vous lancez pas seul... Les bons partenaires hybrides prennent en charge une partie de la complexité liée à l'intégration multi-Cloud et vous permettent d'étendre votre utilisation du Cloud hybride en toute confiance. »

Forrester: Unlock the Value of the Cloud: Spotlight on IT Executives (Libérer la valeur du cloud : pleins feux sur les cadres informatiques)

« Le principal frein au succès de l'hybride est la présence d'une multitude d'outils de gestion déconnectés et de plateformes Cloud incohérentes. La complexité tue l'efficacité. »

Forrester: Unlock the Value of the Cloud: A Spotlight on IT Executives (Libérer la valeur du cloud : pleins feux sur les cadres informatiques)

« Selon IDC, la sécurité restera l'une des principales préoccupations liées à la migration et à l'utilisation du Cloud à mesure que les organisations transfèreront des applications de plus en plus complexes et/ou stratégiques vers le Cloud. Par conséquent, l'interopérabilité et la standardisation entre les environnements de Clouds internes et externes constituent les principaux enjeux en matière de portabilité des applications. Et pour les types d'environnements informatiques diversifiés, il s'agit de fondations qui facilitent la transition vers le Cloud d'une entreprise. »

IDC White Paper: Hybrid Cloud Defined (Définition du cloud hybride)

La solution Kaspersky Lab

La bonne nouvelle est que, même si les Clouds hybrides sont complexes, la sécurité ne doit pas nécessairement l'être.

Kaspersky Hybrid Cloud Security est une solution unifiée tournée vers l'avenir qui est aussi flexible que votre orchestration de Cloud hybride unique, assurant ainsi une protection éprouvée sur les différentes infrastructures.

Les contrôles intuitifs de la solution Kaspersky Hybrid Cloud Security garantissent une protection sans frontières aux environnements de Clouds hybrides. Grâce à une console d'administration de la sécurité au niveau de l'entreprise, Kaspersky Lab rend la gestion, la flexibilité et la visibilité au sein des infrastructures évolutives des Clouds hybrides plus simples que jamais.

Plutôt que d'aborder la cybersécurité de manière fragmentée, ou comme un « jeu de taupe » sans fin, les entreprises peuvent désormais compter sur la solution de Kaspersky Lab pour profiter des avantages suivants :

- **Augmentation du retour sur investissement** grâce à la transformation numérique et aux stratégies de migration vers le Cloud
- **Atténuation** des risques de cybersécurité grâce à des techniques primées et brevetées de sécurité des données, à la distribution automatisée et à la protection basée sur le ML
- **Économies** sur les coûts administratifs, avec une efficacité des ressources sans précédent dans tout l'environnement de Cloud hybride
- **Intégration** à des fonctionnalités majeures via des API natives (pour Microsoft Azure et AWS)
- **Fortification et compensation** pour les limites du modèle de responsabilité partagée de la sécurité dans le Cloud hybride
- **Flexibilité**, avec le pouvoir de transformer et de répondre aux flux ininterrompus de la transformation numérique
- **Confiance** permettant d'évoluer de façon transparente, avec une protection sans frontières éprouvée sur les infrastructures physiques, virtuelles et Cloud

Ainsi, même si le rythme de la transformation numérique dans l'ère du Cloud hybride est parfois très soutenu, les entreprises disposent désormais d'une solution simple pour faire face (rapidement) aux nouvelles cybermenaces et relever les défis uniques du modèle de responsabilité partagée.

Avec son architecture réactive, la solution Kaspersky Hybrid Cloud Security est conçue pour répondre à l'évolution constante des besoins de sécurité des Clouds hybrides, offrant une protection sans frontières primée aux entreprises du monde entier.

Avancez en toute sécurité vers le nouvel horizon de données sans frontières avec la cybersécurité tournée vers l'avenir de Kaspersky Lab.

DEMANDE D'ESSAI GRATUIT DE 30 JOURS

« Les limites d'évolutivité des Clouds privés finiront par inciter les entreprises à adopter des modèles hybrides avec des éléments de Clouds privés et publics »

Larry Lange, rapport PWC, https://www.pwcaccelerator.com/pwcsaccelerator/docs/future-it-outsourcing-cloud-computing.pdf

La puissance et l'interopérabilité des plateformes basées dans le Cloud permettent aux organisations de synthétiser un éventail de technologies synergiques https://www.pwc.fr/fr/assets/images/2016/10/gsis/GSISS-2017-report-cybersecurity-privacy-safeguards.pdf

Kaspersky pour les entreprises :
https://www.kaspersky.fr/enterprise-security
Actualités des cybermenaces : **www.viruslist.fr**
Actualités de la sécurité informatique :
https://www.kaspersky.fr/blog//

#truecybersecurity
#HuMachine

www.kaspersky.fr