Guide pratique de la Sécurité cloud pour les entreprises

Forcepoint

Brochure

Contenu :

Vue d'ensemble : Sécurité cloud et migration dans le cloud

Si pour vous le cloud semble devenir de plus en plus incontournable, sachez que votre impression est la bonne. Mais qu'est-ce qui motive cette accélération rapide et furieuse vers tout ce qui est cloud ? Rien d'autre que le consumérisme. Au format B2C.

La façon dont les personnes consomment le cloud chaque jour détermine la façon dont les entreprises adoptent et sécurisent le cloud.

La sécurité cloud est avant tout humaine.

Le cloud est d'accès instantané.

Et le cloud correspond à des attentes.

Permettant un accès constant au contenu, aux applications, aux appareils - tous connectés entre eux de manière transparente, tout le temps, sans interruption - le cloud est une partie inextricable de notre vie quotidienne. Profondément imprégné au cœur du tissu fonctionnel qu'une personne moderne utilise et opère inconsciemment. Ainsi, sur le lieu de travail, l'attente est la même. Vous voulez utiliser ce dont vous avez besoin, quand vous en avez besoin. Et vous voulez une expérience fluide qui n'entrave pas votre productivité, bien au contraire. Comment augmenter votre productivité avec le cloud ? Comment allez-vous faire plus avec moins ? Parce qu'en fait, le cloud n'est rien d'autre qu'un service. Mais c'est également une vulnérabilité.

En fin de compte, les employés sont des consommateurs. La manière dont les entreprises sécurisent leurs organisations, en protégeant leurs données et leurs personnes, doit correspondre à cette même attente et expérience que nous vivons chaque jour dans notre quotidien. Et la sécurité doit évoluer pour permettre cette fluidité, tout en sécurisant le paysage face à des menaces toujours plus étendues qui accompagnent cette liberté et l'utilisation de ce service.

C'est ainsi que l'on peut définir la culture générale du cloud. Mais quelles sont les circonstances spécifiques qui incitent à l'action et poussent les entreprises à repenser leur approche du cloud et de la sécurité dans son ensemble ? Cela inclut :

- Le parcours de la transformation numérique, à commencer par l'adoption et l'implémentation d'Office 365
- Déplacer les applications anciennes ou personnalisées vers le cloud, comme les systèmes EHR ou ERP
- Les personnes travaillant au-delà des limites d'un bureau, hors du réseau de l'entreprise ou derrière d'autres défenses
- Les entreprises mondiales opérant dans et à travers des environnements hautement distribués, englobant des sites qui ont besoin du même niveau de sécurité que le siège social – sans qu'il soit nécessaire de recréer une empreinte coûteuse en matériel à chaque endroit avec du trafic redirigé
- Les efforts d'optimisation – qu'il s'agisse de consolider les piles de sécurité, de rationaliser les flux de travail des équipes ou simplement de réduire les CapEx/OpEx.
- Déplacer les infrastructures vers les clouds publics comme AWS ou l'Azure

Le bon chemin vers le cloud

La sécurité dans le cloud a un sens différent selon les personnes. Et ce sens change constamment et rapidement. Alors, comment faire pour le suivre ? Comment vous assurer que votre approche est holistique et efficace ? Afin de protéger efficacement votre organisation, la sécurité cloud doit être globale.

Réfléchissons aux composantes clés du cloud :

Les données dans le cloud

Les utilisateurs dans le cloud

Les applications dans le cloud

La connectivité dans le cloud

L'infrastructure dans le cloud

La sécurité dans le cloud

C'est l'essence même de la sécurité cloud. Et tous les composants du cloud doivent être pris en charge et protégés afin d'éviter les failles de sécurité et de préserver la sécurité des utilisateurs et des données. Bien que la sécurité dans le cloud n'ait pas de définition statique, il existe une bonne façon d'aller dans le cloud.

Alors, à quoi cela ressemble-t-il ?

Pour se protéger et se connecter au cloud, les entreprises doivent :

- Sécuriser l'accès au contenu web et aux applications cloud pour tout utilisateur, où qu'il se trouve et sur n'importe quel appareil
- Avoir de la visibilité et un contrôle sur toute l'entreprise pour diriger une stratégie de sécurité cloud
- Préserver l'intégrité des données alors qu'elles transitent dans et vers le cloud.
- Permettre la connectivité directe au cloud pour les utilisateurs et les sites sans redirection du trafic
- Optimiser l'infrastructure et le flux de travail
- Protéger contre les menaces avancées, y compris les failles au jour zéro

Maintenant que vous savez ce que vous avez à faire, comment y parvenir ? De nombreuses entreprises peuvent déjà avoir des produits capables d'exécuter certaines fonctions clés, ou demander à des équipes responsables de certains éléments de la sécurité de s'occuper également du cloud. Mais ce que toute entreprise veut éviter, c'est de submerger ses équipes de sécurité déjà surchargées en travaillant avec des produits à entrées multiples qui ne sont pas intégrés et qui ne se parlent pas entre eux. Ce dont les entreprises ont réellement besoin, c'est d'une solution unique, et non d'une concoction de produits divers. Des nécessités existent, comme le besoin de visibilité pour avoir le contrôle ou la nécessité de migrer la sécurité web sur site vers le cloud afin de protéger les utilisateurs hors réseau. Dans son état optimal, la sécurité cloud est une solution unifiée qui s'articule autour des données, de l'accès au web, de l'accès et du traitement des données dans le cloud et de la connectivité. Elle permet d'atténuer tous les secteurs douloureux au sein de votre équipe et d'éviter les lacunes en matière de sécurité. Que ce soit atteint avec un ou trois prestataires, les entreprises doivent s'assurer que les lignes directrices de ce qu'elles ont, de ce qu'elles veulent et d'où elles veulent être s'alignent, pour de bons résultats opérationnels.

Répondre aux problématiques du cloud+

Le transfert de données vers le cloud est un projet important – et si vous ressentez une certaine anxiété à ce sujet, vous n'êtes pas seul. Comment maintenir la propriété et le contrôle ? Comment faites-vous pour continuer à tenir à distance les menaces ? Comment assurer de bonnes performances ?

Résolvons certains des points d'interrogation les plus courants.

Latence

Une bonne couverture est critique pour réduire la latence. Une empreinte étendue avec de nombreux terminaux à travers le monde offrira une faible latence ainsi que d'autres avantages stimulant la productivité, comme la localisation de contenu. **Les réseaux Tier 1 et les centres de données Tier 4** contribuent à garantir un niveau élevé de portée, de redondance, de connectivité et de qualité, idéal pour les applications sensibles à la latence.

Visibilité

Vous ne pouvez pas protéger contre les menaces que vous ne voyez pas. Et vous ne pouvez pas faire de changements ou définir de politique sans savoir ce qu'elle va affecter. Le couplage d'une **passerelle à sites web** avec un **firewall** offre une visibilité et une application cohérentes pour tous les utilisateurs et tous les emplacements, y compris pour l'application des politiques et le contrôle de la "Shadow IT". Et la fonctionnalité **CASB** aide à sécuriser les entreprises en offrant une visibilité sur ce que les utilisateurs des applications, autorisées ou non, font dans le cloud pour comprendre les risques et protéger les utilisateurs et les données.

Conformité

Des programmes de certifications de confiance – et non des tests de conformité auto-administrés. Les normes adéquates pour votre entreprise incluent probablement :

- **ISO 27018**, qui régit les informations personnelles identifiables (PII)
- **ISO 27001**, une certification multisites pour le développement, l'assurance qualité, le déploiement et les opérations de soutien
- **CSA**, qui régit la sécurité des logiciels et les opérations interfonctionnelles dans un contexte d'informatique dématérialisée (et qui est basé sur le code de conduite du RGPD)
- **SOC2**, qui se concentre sur les contrôles des rapports non financiers relatifs à la sécurité, la disponibilité, l'intégrité du traitement, la confidentialité et la vie privée, en plus des tests des centres de données et de l'efficacité opérationnelle

Souveraineté des données

Bien que le cloud en lui-même n'a pas de limites concrètes, il n'est pas exempt des conséquences juridiques des frontières et des limites géographiques. Les données numériques sont soumises aux lois qui régissent le lieu de résidence de ces données. L'utilisation **de centres de données cloud situés dans les régions où votre entreprise opère** est essentielle pour la conformité aux lois et réglementations locales, ainsi que pour les performances.

Pertes de données

Une approche unifiée est l'approche ayant le plus de réussite. Avec des **solutions intégrées de protection de données**, vous pouvez étendre vos mesures de sécurité depuis votre site jusque dans le web, dans les courriels, le réseau et le cloud. Tirez parti de vos politiques existantes pour protéger les données au repos dans le cloud et les données en transit.

PAP

La main-d'œuvre d'aujourd'hui s'appuie sur une multitude d'applications cloud autorisées ou non, sur des appareils gérés et non gérés. Lorsqu'il s'agit de sécuriser les utilisateurs distants et itinérants, les défenses du périmètre du réseau et la protection des terminaux ne suffisent pas. Vous devez faire la distinction entre les dispositifs gérés et les BYOD, en utilisant des **politiques de sécurité granulaires** pour donner aux salariés la possibilité d'utiliser leurs propres appareils sans poser de risques supplémentaires. **Des contrôles élargis** donnent de la sécurité aux utilisateurs à distance qui utilisent les appareils de l'entreprise à la fois pour leur travail et pour leur usage personnel.

Se contenter du minimum

Désireuses de devenir plus agiles, plus efficaces, etc., les entreprises adoptent souvent une approche “on verra plus tard” lorsqu'elles abordent le cloud. Mais le simple fait de cocher des cases sacrifie souvent la sécurité et l'efficacité. Par exemple, le filtrage d'URL seul n'est pas une sécurité - de la même manière qu'une solution DNS récursive ne remplace pas une passerelle web complète. Vous ne pouvez pas obtenir une protection intégrale si vous n'avez qu'une seule partie de la solution. De plus, l'approche “strict minimum” place la sécurité en position de réaction, plutôt que d'agir de façon proactive. Assurez-vous que **la sécurité et le réseau fonctionnent bien ensemble et font partie de l'équation** alors que votre entreprise crée sa feuille de route pour la transformation numérique – ainsi, ces éléments fonctionneront conjointement avec vos objectifs commerciaux, sans prendre de retard.

Atteindre le succès dans un monde connecté au cloud

Nous avons déterminé en préambule que la sécurité cloud est avant tout humaine. Et c'est pour cela qu'elle doit privilégier le facteur humain.

Grâce au cloud, **les personnes sont les nouveaux périmètres.**

Pendant que les usagers, les partenaires et les clients accèdent aux données de votre entreprise depuis n'importe quel endroit du monde, le mur artificiel qui protège les données ne suffit plus.

La sécurité historique, centrée sur l'infrastructure en regroupant les utilisateurs de confiance à l'intérieur et qui laissant les autres à l'extérieur, n'est plus pertinente.

La confiance inhérente ne peut pas faire partie de votre doctrine de sécurité.

Et votre doctrine de sécurité est une partie intégrante - et non optionnelle - de votre transformation numérique.

Pour l'accélérer et la préserver, voici quelques principes fondamentaux à garder à l'esprit :

Avancez à votre rythme

Rome ne s'est pas construite en un jour. Et votre migration vers le cloud ne va pas se faire en une soirée.La plupart des entreprises opèrent dans des environnements informatiques hybrides/multi-cloud et continueront à le faire dans un futur proche. Assurez-vous que votre passerelle web sécurisée dispose d'options de déploiement flexibles qui vous permettent de migrer en fonction de ce qui convient à votre organisation aujourd'hui et dans le futur. Cela vous permettra de migrer à vos propres conditions, lorsque vous serez prêt, tout en maintenant une sécurité d'ensemble.

Augmentez votre portée opérationnelle en même temps que la croissance de votre périmètre

Sécurisez votre cloud, votre réseau et vos terminaux pour répondre à l'évolution de votre entreprise. Une plate-forme convergente à faible empreinte matérielle, à capacités de sécurité modulaires, offre aux organisations hautement distribuées l'extensibilité et l'agilité dont elles ont besoin pour tirer parti des nouvelles avancées techniques, pour boucher les angles morts et pour se connecter d'un endroit à l'autre, de manière sûre et contrôlée.

Connaissance absolue pour Zero Trust

Le principe “Ne jamais faire confiance et toujours vérifier” est un élément clé du cadre de travail Zero Trust – ce qui signifie que la façon de protéger les données de votre entreprise consiste à évaluer l'accès à ces données tout au long de l'interaction entre l'utilisateur et l'appareil.Cela vous aide à comprendre le “qui” et le “comment” C'est en comprenant le “pourquoi” que vous pourrez aller au-delà de la sensibilisation et passer à la prévention. L'analyse comportementale pour aider à comprendre l'intention.

Êtes-vous prêt à découvrir l'étape suivante de votre sécurité cloud évolutive ?

› Lisez notre livre électronique“Protéger le personnel partout, en permanence”.

Forcepoint

forcepoint.com/contact

À propos de Forcepoint

Forcepoint est l'entreprise leader en cybersécurité pour la protection des utilisateurs et des données, dont l'objectif est de protéger les entreprises tout en stimulant la transformation et la croissance numériques. Les solutions personnalisées de Forcepoint s'adaptent en temps réel à la façon dont les personnes interagissent avec les données, et offrent un accès sécurisé tout en permettant aux employés de créer de la valeur. Basé à Austin, au Texas, Forcepoint crée des environnements sûrs et fiables pour des milliers de clients dans le monde entier.