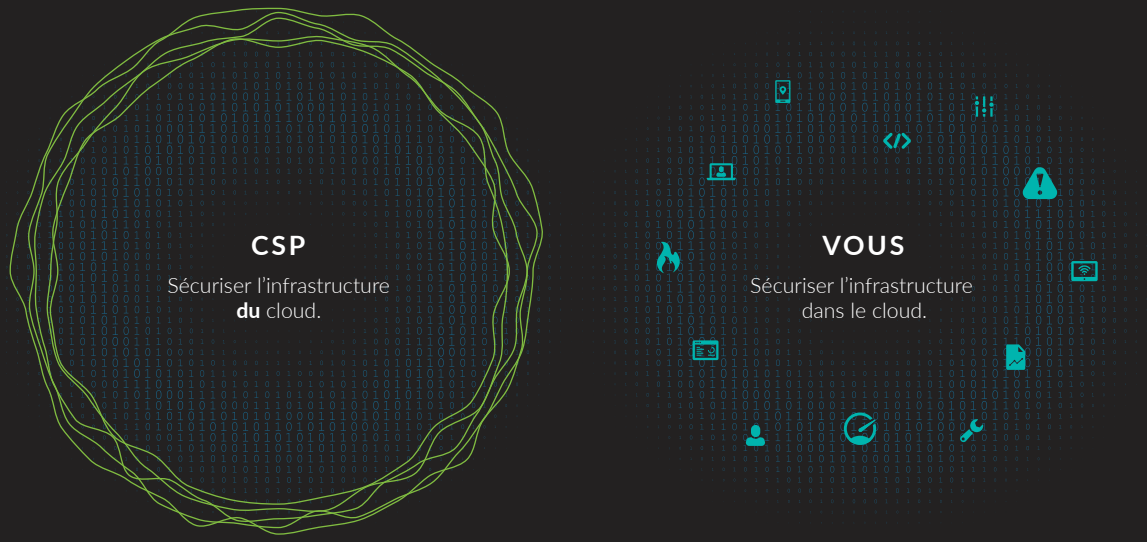
ExtraHop

Responsabilité partagée dans le cloud

COMPRENDRE LE RÔLE DE L'ENTREPRISE EN MATIÈRE DE SÉCURITÉ DANS LE CLOUD

En tout premier lieu, tous les clients du cloud doivent savoir qu'Amazon Web Services (AWS) et Microsoft Azure sont des fournisseurs de services cloud (CSP, pour « cloud service provider » en anglais). Ils ne vous vendent pas de la sécurité. C'est en grande partie pour cette raison qu'ils ont essayé de faire comprendre que leur sécurité et leur conformité étaient limitées. Pour permettre d'identifier exactement où la responsabilité du CSP s'arrête et où celle du client commence, AWS et Azure ont chacun développé des modèles de responsabilité partagée.



Qu'est-ce que ça veut dire ?

L'expression « responsabilité partagée » signifie que les CSP protègent leurs actifs (tout ce qui se trouve sous le contrôle de l'hyperviseur) et que le client protège les siens (tout ce qui se trouve au-dessus de l'hyperviseur)

Le modèle de responsabilité partagée ne vous protège pas

Jusqu'ici, aucune violation importante n'a été subie par les CSP. Comme leur personnel est composé de certains des meilleurs chercheurs mondiaux en matière de sécurité, leur niveau de sécurité va probablement continuer à s'améliorer au fil du temps. Il n'en va pas de même pour le client ordinaire du cloud. Gartner prévoit que d'ici 2022, au moins 95 % des défaillances de sécurité du cloud se seront produites dans la partie du modèle de responsabilité partagée qui dépend du client.

Ce chiffre peut surprendre, mais en disposant d'une meilleure compréhension de leur responsabilité et en détaillant les principaux vecteurs de menaces par le biais desquels ces défaillances sont susceptibles de se produire, les entreprises peuvent mieux comprendre ce qu'elles sont en mesure de faire pour remplir leur rôle au niveau de ces marchandages concernant la sécurité du cloud.

ExtraHop

RESPONSABILITÉ PARTAGÉE SUR LE CLOUD

APPLICATIONS ET CONTENU

Les événements du Azure Security Center enrichissent la détection des menaces sur le réseau grâce à l'activité intégrée (journalisation désactivée, processus suspects, exécution de fichiers suspects)

Décodage TLS 1.3 complet et analyse de la charge utile des transactions en temps réel, pour le repérage des menaces et l'évaluation des risques, même dans le cadre de déploiements PFS

SÉCURITÉ RÉSEAU

- Visibilité sur l'accès à l'infrastructure cloud via une connexion réseau privée pour suivre les mouvements latéraux
- Responsabilité concernant l'accès à distance

INVENTAIRE ET CONFIGURATION

- Détection et catégorisation automatiques de l'ensemble des actifs du cloud
- Suivre les instances malveillantes même si la journalisation est désactivée
- Marquez instantanément les ressources exposées (exposition d'Azure Blob Storage à Internet)

SÉCURITÉ DES DONNÉES

- Disposer d'un support complet pour les bases de données Azure SQL et les protocoles Azure Blob Storage est synonyme de visibilité en ce qui concerne le comportement, et pas seulement les activités
- Le machine learning au niveau de la couche applicative permet une détection immédiate de toute activité d'exfiltration

CONTRÔLE D'ACCÈS

- L'intégration avec Azure Activity Monitoring permet un suivi granulaire des manipulations des privilèges
- L'analyse des charges utiles d'Active Directory permet au machine learning de signaler tout comportement suspect (collecte d'identifiants, attaque par force brute)

Sécurité native du cloud par rapport à la sécurité adaptée au cloud

Malgré les efforts visant à faire une distinction claire entre leur responsabilité et celle du client, AWS et Azure continuent à proposer des solutions de sécurité natives du cloud à leurs clients. Pour de nombreuses entreprises – en particulier celles qui sont nouvelles dans le cloud – ces solutions offrent des avantages immédiats, notamment une console avec laquelle elles sont familières, une accélération du temps de commercialisation et une disponibilité clé en main.

ExtraHop propose un machine learning dans le cloud, ce qui offre beaucoup plus de puissance pour alimenter les détecteurs. Toutefois, toutes les solutions de sécurité natives du cloud, comme AWS Guard Duty, AWS CloudWatch ou Azure Monitor, mettent en œuvre leur machine learning en se basant sur les données de journaux de flux. Comme les solutions AWS et Azure reposent sur les journaux, il s'agit essentiellement d'informations superficielles, qui ne sont pas basées sur des modèles de comportement. Elles ne vont pas tout détecter – en particulier les instances malveillantes non signalées. Un équilibreur de charge ELB ne vous indiquera que ce qu'il enregistre en votre nom, et ne vous donnera pas un compte rendu détaillé sur son comportement.

COMMENT EXTRAHOP PEUT VOUS AIDER

En intégrant et en contextualisant les événements du cloud avec d'autres activités de l'infrastructure afin de créer un environnement d'analyse et d'investigation unifié pour les équipes SOC, Reveal(x) pour Azure et AWS offre une analyse permanente de la couche applicative sur l'ensemble de la surface d'attaque hybride. Avec un machine learning appliqué à plus de 4 700 paramètres, Reveal(x) détecte les activités d'attaque en phase tardive avec un niveau de certitude élevé, en les présentant dans leur contexte pour que les équipes de sécurité du cloud puissent procéder à une investigation immédiate.

À PROPOS D'EXTRAHOP NETWORKS

ExtraHop propose une cyberanalyse d'entreprise qui assure sécurité et performance de bout en bout. Notre approche révolutionnaire permet d'analyser l'intégralité des interactions réseau et s'appuie sur le machine learning avancé pour vous offrir une visibilité totale, une détection en temps réel et une investigation guidée. Nous aidons ainsi les plus grandes entreprises du monde à prendre du recul par rapport aux alertes, aux silos organisationnels et aux technologies à durée de vie limitée. Que vous analysiez des menaces, vous assuriez de la disponibilité d'applications stratégiques ou sécurisiez votre investissement sur le cloud, ExtraHop vous aide à protéger votre entreprise et à donner un nouvel élan à votre activité.

ExtraHop

520 Pike Street, Suite 1600
Seattle, WA 98101
877-333-9872 (téléphone)
206-274-6393 (fax)
info@extrahop.com
www.extrahop.com