LIVRE BLANC

Pourquoi le cloud doit avoir sa propre sécurité

Découvrez les avantages d'une plateforme d'analyse de sécurité dans le cloud

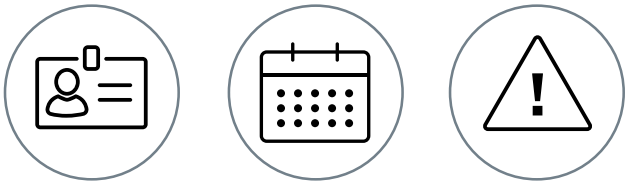
splunk> turn data into doing™

Les menaces de sécurité avancées deviennent de plus en plus difficiles à détecter en raison de la sophistication croissante des attaques des pirates informatiques. Parallèlement à cela, les outils utilisés pour se défendre contre les cyberattaques se multiplient et gagnent en complexité. Les entreprises sont également confrontées à une pénurie de personnel qualifié pour repousser les malfaiteurs.

Cybercriminels | **Menaces internes** | **États-nations**

C'est maintenant qu'il faut résoudre ces problèmes, et non pas au cœur d'une attaque avancée ou lors de l'investigation d'une faille potentielle. Le temps est une ressource rare que les équipes de sécurité ne peuvent se permettre de consacrer à acquérir du personnel qualifié, du matériel ou des capacités de déploiement, en particulier en pleine investigation sur une menace potentielle.

Pour prendre de l'avance sur les attaques sophistiquées et les malfaiteurs, les équipes de sécurité doivent pouvoir effectuer des analyses ad hoc sur l'ensemble de leurs données locales et cloud (réseau, points de terminaison, identités, informations sur les menaces et données de sécurité non traditionnelles) en quasi temps réel.



100 % des identifiants valides ont été utilisés

99 nombre moyen de jours avant détection

67 % des victimes notifiées par une entité externe

Les entreprises doivent également pouvoir superviser et analyser en temps réel les menaces, les attaques et autres activités anormales à partir de toutes les données de sécurité, en les replaçant dans leur contexte métier. Grâce aux analyses avancées, les clients parviennent à accélérer la détection des menaces et la réponse aux incidents sur tout l'écosystème de sécurité.

Adoptez le cloud

Heureusement, il y a quelques rayons de soleil dans cette époque souvent sombre. Les équipes de sécurité ont l'opportunité d'améliorer simultanément leurs opérations de sécurité et d'acquisition d'informations. Elles doivent adopter une solution de sécurité axée sur l'analyse et basée dans le cloud pour sécuriser leurs applicatifs cloud et leurs systèmes locaux existants dans le même temps.

Une solution de sécurité axée sur l'analyse est une plateforme qui donne aux entreprises les moyens de garder une longueur d'avance sur des cybermenaces en évolution constante et de corriger rapidement les failles lorsqu'elles se produisent, tout en étant capable de traiter les besoins métier essentiels.

La flexibilité du cloud met également les solutions de sécurité axées sur le cloud à la portée des entreprises de toute taille, grâce aux économies réalisées en évitant le recrutement de personnel supplémentaire et l'achat de matériel physique coûteux.

Une solution cloud de sécurité axée sur l'analyse évolue tout en sécurisant le parcours d'une entreprise vers le cloud. Elle offre également des informations détaillées sur les écosystèmes de sécurité et les applications cloud et hybrides. Elle permet souvent à l'entreprise de commencer à rentabiliser son passage au cloud en quelques heures.

Plus spécifiquement, une solution de sécurité axée sur l'analyse et basée dans le cloud peut détecter des malwares complexes, investiguer des menaces sophistiquées et réagir rapidement aux incidents. Une solution cloud aide aussi les entreprises à atteindre rapidement et à maintenir leur conformité tout en protégeant les IP sensibles et les actifs stratégiques.

Le cloud, avec des avantages de poids

Certains se demandent encore s'il est sûr d'exploiter une solution de sécurité dans le cloud. Mais une solution de sécurité dans le cloud ne se protège pas différemment de bien d'autres solutions de logiciels en tant que service (SaaS), sur lesquelles les entreprises s'appuient déjà au quotidien. Une solution de sécurité basée dans le cloud peut résoudre les problèmes rencontrés par de nombreuses entreprises en matière d'informations de sécurité.

Avant de rejeter l'option d'une sécurité basée sur le cloud, sachez que les pratiques et les technologies de sécurité de la plupart des grands services cloud peuvent être bien plus sophistiquées que celles d'une entreprise classique.

Le SaaS est déjà largement employé pour des systèmes stratégiques tels que la CRM, les RH, l'ERM et l'analyse commerciale. Le SaaS est également largement exploité pour délivrer des logiciels courants comme Microsoft Office 365, Salesforce.com, Okta, Box, ServiceNow, AWS et bien d'autres.

Les mêmes raisons qui font du SaaS une option judicieuse pour les applications d'entreprise (rapidité, déploiement facile, faibles coûts, mises à jour automatiques, facturation à l'utilisation, infrastructure évolutive et renforcée) expliquent que le cloud soit idéal pour la sécurité.

Les solutions de sécurité cloud offrent la possibilité d'utiliser un large éventail de groupes de données provenant d'installations locales comme du cloud. À l'heure actuelle, les entreprises déplacent leurs applicatifs vers l'infrastructure en tant que service (IaaS), les plateformes en tant que service (PaaS) et le SaaS. Dans ce contexte, sa simplicité d'intégration avec les systèmes tiers rend une approche cloud de la sécurité encore plus pertinente.

Les avantages stratégiques d'une solution cloud de sécurité axée sur l'analyse sont nombreux : souplesse d'une architecture hybride, mises à jour automatiques et configuration simplifiée des logiciels, infrastructure instantanée et évolutive, contrôles étroits et haute disponibilité.

Une architecture hybride et flexible

L'utilisation de services cloud en entreprise gagne du terrain et beaucoup d'organisations exploitent désormais un environnement hybride, qui abrite des données et des applications dans le cloud et sur des machines locales. Par conséquent, où que soit déployée la solution de sécurité, elle doit être capable de recueillir les données des deux environnements.

En effet, un récent rapport a révélé que les décideurs IT considéraient le cloud et le SaaS comme la deuxième technologie la plus disruptive des 3 à 5 prochaines années. C'est pourquoi un tiers de ces décideurs prévoient également d'augmenter les dépenses dans le cloud au cours de l'année à venir. Parallèlement à cela, l'industrie prévoit de réduire les dépenses en matériel et en systèmes hérités l'année prochaine.

Opter pour une solution de sécurité dans le cloud apporte également de la flexibilité aux entreprises. Dans le cas d'un environnement cloud hybride, une solution de sécurité peut être déployée dans le datacenter privé de l'entreprise et agréger les données des machines locales et des services cloud, tout en jouant le rôle de service cloud capable d'importer les données de sécurité de n'importe quelle source.

Une infrastructure robuste et évolutive

De plus, la mise en place et l'exploitation d'une infrastructure hébergeant une solution de sécurité cloud locale demande du temps et des efforts de mise en œuvre.

Les systèmes de sécurité doivent s'adapter à la fois à la croissance des données et à la diversité des sources. Une solution de sécurité axée sur l'analyse et basée dans le cloud permet de la déployer instantanément et de la faire évoluer facilement en fonction des besoins. Réunir toutes les informations de sécurité utiles dans un même dépôt, en veillant à ce qu'elles soient protégées, indexées et sécurisées, est le meilleur moyen d'améliorer la prise de décisions de sécurité.

Des contrôles étroits et une haute disponibilité

Les services pour entreprise doivent répondre à des préoccupations courantes concernant la sécurité, les contrôles et les performances des services cloud. Ces questions portent sur plusieurs thèmes.

La sécurité des données et du système : les fournisseurs de SaaS s'appuient souvent sur l'une des grandes plateformes IaaS que sont AWS, Google Cloud ou Microsoft Azure. Ces grands fournisseurs d'infrastructure cloud exploitent des datacenters sécurisés régis par des politiques de sécurité répondant aux certifications SOC 2 Type II et ISO 27001.

Une bonne pratique consiste à séparer logiquement les données du client en les affectant à des serveurs virtuels et à des espaces de stockage délimités et dédiés. Les données des clients doivent être chiffrées par SSL lorsqu'elles sont en transit, et l'être aussi éventuellement au repos par AES-256, avec des clés uniques régulièrement renouvelées.

Les exigences relatives à la souveraineté et la résidence des données : l'architecture cloud hybride représente une bonne option pour les solutions de sécurité car elle permet de conserver sur place (ou dans la région concernée) les données soumises à des exigences de confidentialité, de traitement ou réglementaires spécifiques et locales. En hébergeant leur solution auprès d'un fournisseur IaaS majeur, les entreprises ont la possibilité de la déployer dans différentes régions du monde. AWS propose même une région certifiée FedRAMP pour les utilisateurs fédéraux américains avec AWS GovCloud (US).

Le contrôle et la personnalisation des services : passer au cloud ne doit pas se traduire par une perte de contrôle sur les paramètres importants des applications et les politiques de sécurité. Une solution de sécurité cloud doit offrir à ses utilisateurs un contrôle sur la gouvernance

à l'échelle de l'application, tout en les isolant des informations au niveau de l'infrastructure. Elle permet en outre aux entreprises de garder le contrôle nécessaire pour satisfaire leurs obligations internes et externes.

La performance et la disponibilité des applications : l'hébergement chez un fournisseur IaaS majeur comme AWS permet de garantir au service de sécurité une disponibilité haut de gamme à un prix raisonnable. Par exemple, le service peut être conçu de manière à couvrir plusieurs zones ou régions de disponibilité cloud, ce qui permet de maintenir un service en ligne même si un datacenter s'arrête.

Splunk entre en jeu

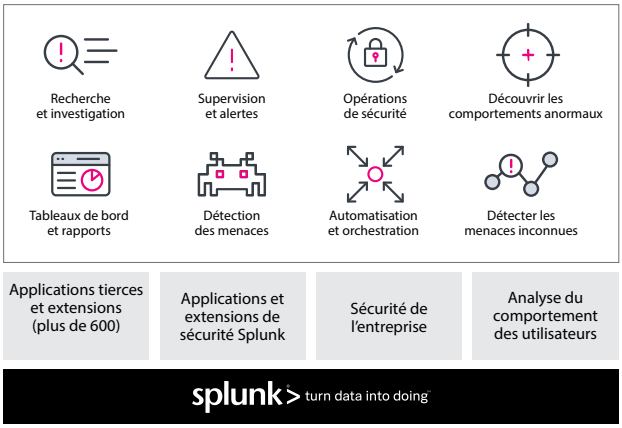
Le portefeuille cloud de sécurité axée sur l'analyse de Splunk comprend **Splunk Enterprise** (et sa version logiciel en tant que service, Splunk Cloud), **Splunk Enterprise Security** (ES) et Splunk UBA, qui se combinent pour réunir différents domaines de l'IT pour faciliter la collaboration et la mise en œuvre des bonnes pratiques, et relever les défis des cybermenaces modernes.

Splunk Enterprise **est déployé** sur Amazon Web Services (AWS). La solution est autonome et peut être facilement déployée sur n'importe quelle instance EC2, elle peut aussi évoluer horizontalement, ce qui la rend idéale pour un déploiement AWS.

En utilisant la plateforme Splunk comme centre névralgique, les équipes de sécurité peuvent exploiter des analyses statistiques, visuelles, comportementales et exploratoires afin d'obtenir des informations et de prendre des décisions et des mesures.

La puissance de l'analyse des big data et de la sécurité cloud

Exécuter votre solution de sécurité dans le cloud offre de nombreux avantages, mais en l'associant à une plateforme d'analyse big data comme Splunk, vous obtiendrez des analyses des logs et des rapports sur tous les indicateurs des systèmes et des applications. Une telle combinaison symbolique délivre des fonctions de supervision des applications de bout en bout, de résolution des problèmes et d'analyse de sécurité, en plus d'une solution complète de sécurité axée sur l'analyse.



Les meilleures plateformes d'analyse de sécurité sont conçues pour importer, collecter et interpréter les enregistrements de log de myriades de systèmes et ont été éprouvées dans des entreprises de toute taille. Ces plateformes offrent des fonctions de collecte des données en temps réel, d'interrogation des données à l'aide d'un langage de requête riche, de visualisation des données et d'analyse statistique pouvant informer des tableaux de bord en temps réel.

Combiner une solution de sécurité à une plateforme big data capable d'extraire les données de n'importe quel système permet aux entreprises d'obtenir une vue unifiée des métriques les plus importantes concernant les opérations, les performances des applications et la sécurité. Déployée en tant que service cloud, les entreprises en tirent immédiatement une valeur sans configuration longue, courbes d'apprentissage ni investissement massif, et peuvent recueillir et analyser les données de tous les systèmes, aussi bien cloud que locaux.

Face à l'augmentation exponentielle des sources d'informations de sécurité utiles et du volume des données en général, un service cloud est la solution idéale pour les déploiements de sécurité. En appuyant votre plateforme de sécurité sur une plateforme éprouvée d'agrégation et d'analyse des données comme Splunk, il devient possible de mettre au service de la gestion de la sécurité les riches fonctionnalités conçues pour améliorer les opérations IT.

Essayez Splunk Enterprise Security dès maintenant. Découvrez la puissance de Splunk Enterprise Security sans téléchargement, sans machine et sans configuration. La sandbox en ligne Splunk Enterprise Security est un environnement cloud d'évaluation de sept jours contenant des données pré-remplies qui vous permet d'interroger, visualiser et analyser les données, et d'étudier des incidents de manière détaillée sur un large éventail de scénarios de sécurité. Vous pouvez également suivre un tutoriel pas à pas qui vous guidera dans les analyses et les visualisations puissantes que permet le logiciel Splunk. **En savoir plus.**

splunk>

En savoir plus : www.splunk.com/asksales

www.splunk.com

20-16126-Why You Should Take Security in the Cloud-A4-102-WP