 **Les améliorations apportées à Sophos Cloud Optix simplifient la sécurité du Cloud**

*Les nouvelles fonctionnalités et options seront présentées lors de l’événement AWS re:Invent 2019*

**LAS VEGAS**  – 03 Déc, 2019 – [Sophos (](https://www.sophos.com/fr-fr.aspx)LSE: SOPH),leader mondial en solutions de cybersécurité Next-Gen, dévoile aujourd'hui les améliorations apportées à Sophos Cloud Optix qui automatisent et simplifient la détection et la réponse aux vulnérabilités de sécurité et aux erreurs de configuration dans le Cloud, afin de réduire l'exposition aux risques.

Cloud Optix est facilement managé à partir de la plateforme unifiée Sophos Central, basée dans le Cloud, en parallèle de toute la gamme de solutions de cybersécurité Next-Gen de Sophos, comme notamment les produits Sophos endpoint, network, mobile, Wi-Fi, email et encryption. Le partage d'informations en temps réel et la réponse aux menaces depuis Sophos Central permettent aux entreprises d'améliorer leurs délais de détection et de réponse, simplifiant ainsi les investigations et minimisant l'impact des menaces.

Cloud Optix répond à un besoin critique du marché en matière de sécurité du Cloud grâce à une visibilité inégalée des angles morts. En utilisant l'intelligence artificielle pour automatiser la détection des vulnérabilités et des mauvaises configurations au sein de l'architecture Cloud, les équipes de sécurité bénéficient d'une visibilité complète sur l’ensemble de leurs actifs dans le Cloud, et se voient ainsi dotées d’une capacité de réponse et de remédiation des risques de sécurité, et ce en quelques minutes seulement. Disponible dans AWS Marketplace, Cloud Optix permet de détecter automatiquement les actifs d’une entreprise dans des environnements Amazon Web Services (AWS) et multi-cloud.

Découvrez ci-dessous un aperçu des nouvelles fonctionnalités et options innovantes présentées sur le stand #1032 lors de l’événement AWS re:Invent 2019 :

* **L’accélération des investigations sur les menaces** : Cloud Optix transforme la visualisation de l'infrastructure AWS afin que les entreprises puissent identifier et éliminer les menaces de sécurité cachées. Cloud Optix étend désormais son support à Amazon Detective, récemment lancé, avec des données interactives et intuitives concernant les menaces potentielles, telles que les tentatives de connexion infructueuses et les appels d'API suspects au niveau des workloads AWS.
* **L’identification des vulnérabilités de sécurité Kubernetes** : Cloud Optix assure désormais le suivi des clusters Amazon EKS (Amazon Elastic Kubernetes Service) et des déploiements Kubernetes natifs, offrant ainsi une liste complète et une visualisation des clusters, des nœuds, des groupes de nœuds, des pods, des conteneurs, etc. De nouvelles vérifications de sécurité par comparaison permettent aux entreprises d'évaluer en permanence leur posture en matière de cybersécurité concernant leur plateforme d'orchestration de conteneurs.
* **La détection des anomalies liées aux coûts dans le Cloud** : les nouvelles fonctionnalités de sécurité, permettant la surveillance des coûts dans le Cloud, signalent les anomalies inattendues pouvant provenir d’actes malveillants, afin que les entreprises puissent agir en conséquence. Cloud Optix surveille les coûts de manière quotidienne dans le Cloud et identifie les activités inhabituelles, se focalisant sur les principaux environnements et services par type de coût, avec la mise en place d’alertes personnalisables lorsqu’un seuil est atteint.
* **La détection des accès publics ou inter-comptes non souhaités** : l'intégration du nouvel analyseur d'accès d'AWS Identity and Access Management (IAM) fournit les détails et le contexte nécessaires pour déterminer rapidement si les politiques en matière de ressources ont été mal configurées, permettant ainsi un accès public ou inter-comptes non souhaité.
* **Un trafic Cloud sécurisé** : en étendant la sécurité au réseau, la prise en charge par Sophos UTM du nouveau routage des entrées au niveau d’Amazon Virtual Private Cloud (VPC) garantit la sécurité du trafic entrant et sortant au niveau des VPC et des autres appliances virtuelles. Avec la nouvelle possibilité de limiter le trafic nord-sud, Sophos offre une couche de protection supplémentaire pour sécuriser l’infrastructure Cloud.

Lors de l’événement AWS re:Invent 2019, Sophos animera une session sur la création de solutions de sécurité à l'aide du service Amazon Elasticsearch. Le jeudi 4 décembre, de 17h30 à 18h30 (heure PST), Key Vaidya, Sophos Distinguished Cloud Engineer, et Dennis Griffin, Senior Director MDR Platforms, partageront leurs meilleures pratiques en matière de conception pour des déploiements à grande échelle, en se basant sur leurs expériences dans le développement de systèmes de surveillance et d’alerte de sécurité exploitant Amazon Elasticsearch Service ainsi que d’autres composants.

Les participants seront invités à se rendre sur le stand #1032 de Sophos pour bénéficier d’une évaluation gratuite de la sécurité du Cloud, qui permettra de mettre en évidence les risques encourus et de lister les actions prioritaires à lancer afin d’apporter des améliorations immédiates et significatives.

**À propos de Sophos**

En tant que leader mondial en solutions de cybersécurité Next-Gen, Sophos protège plus de 400 000 entreprises, de toutes tailles et dans plus de 150 pays, contre les cybermenaces actuelles les plus avancées. Développées par les SophosLabs, une équipe présente dans le monde entier et spécialisée dans le renseignement sur les menaces et la science des données, les solutions Cloud-Native et basées sur l'IA de Sophos protègent les systèmes endpoint (les ordinateurs portables, les serveurs et les périphériques mobiles) ainsi que les réseaux contre les techniques de cyberattaque évolutives, notamment les ransomwares, les malwares, les exploits, l'exfiltration de données, les violations par adversaire-actif, le phishing, et bien plus encore. Sophos Central, une plateforme de management Cloud-Native, intègre l'ensemble des produits Next-Gen de Sophos, y compris la solution Intercept X endpoint et le pare-feu XG Next-Gen, via un système unique de «sécurité synchronisée» accessible via un ensemble d'API. Sophos a favorisé la transition vers une cybersécurité moderne en exploitant des fonctionnalités avancées au niveau du Cloud, de l'apprentissage automatique, des API, de l'automatisation, du service MTR (Managed Threat Response), entre autres, afin d’offrir une protection de niveau professionnel à toutes les entreprises. Sophos commercialise ses produits et services exclusivement par l’intermédiaire d’un réseau mondial regroupant plus de 47 000 partenaires et fournisseurs de services gérés (MSP : Managed Service Provider). Sophos met également ses technologies commerciales innovantes à la disposition des particuliers via Sophos Home. Le siège de l’entreprise est basé à Oxford, au Royaume-Uni, et Sophos est cotée à la Bourse de Londres sous le symbole «SOPH». Plus d'informations sont disponibles sur [www.sophos.com](http://www.sophos.com).

**Contact presse :**Square Egg Communications, Sandra Van Hauwaert, [sandra@square-egg.be](mailto:sandra@square-egg.be), GSM 0497251816.