**Sophos dévoile la nouvelle version de sa solution Endpoint Detection and Response (EDR)**

*Conçue pour les analystes de sécurité et les administrateurs informatiques, cette nouvelle version propose les fonctionnalités Live Discover et Live Response*

**Bruxelles, le 9 juin 2020** – [Sophos](https://www.sophos.com/en-us.aspx) dévoile la mise à jour de sa solution [Endpoint Detection and Response](https://www.sophos.com/fr-fr/products/endpoint-antivirus/edr.aspx) (EDR), première solution conçue à la fois pour les analystes de sécurité et les administrateurs informatiques, disponible avec [Sophos Intercept X Advanced](https://www.sophos.com/fr-fr/products/endpoint-antivirus.aspx) et [Intercept X Advanced for Server with EDR](https://www.sophos.com/fr-fr/products/server-security.aspx).

Les importantes évolutions et les nouvelles fonctionnalités de la solution permettent aux analystes de sécurité une identification et une neutralisation plus rapide et plus facile des menaces insidieuses tandis que les administrateurs informatiques peuvent désormais assurer de manière proactive le maintien de la sécurité des opérations informatiques afin de réduire les risques.

Comme le révèle l’étude Sophos *State of Ransomware 2020*, seules 23% des entreprises belges victimes d’un ransomware déclarent avoir pu détecter et arrêter l’intrusion avant le chiffrement des fichiers. Les nouvelles fonctionnalités de Sophos EDR permettent aux équipes de sécurité et à l’IT de détecter les menaces et les violations de sécurité dont la découverte prendrait généralement plusieurs mois. Sophos EDR répond à cette difficulté, en réduisant radicalement le temps nécessaire pour détecter les signes d’une violation de sécurité.

« Les enjeux sont de plus en plus élevés, les cybercriminels ne reculant devant rien pour tirer profit de l’étendue grandissante des surfaces d’attaque, liée à la migration croissante des entreprises vers le cloud et à l’accélération du travail à distance. La protection des serveurs et autres périphériques est insuffisante, ce qui créé des points d’entrée vulnérables que les attaquants n’ont plus qu’à exploiter », déclare Patrice Clair, Directeur Avant-Vente, Sophos France. « Sophos EDR permet d’identifier ces attaques, prévenant ainsi les violations de sécurité et mettant en lumière les zones d’ombre. Les fonctionnalités d’interrogation en temps réel *(Live Querying)* proposées par Sophos EDR avec Intercept X permettent aux entreprises de rechercher des indicateurs de compromission dans l’historique et de déterminer l’état du système en temps réel. Ce niveau de renseignement est déterminant pour mieux appréhender les changements de comportement des attaquants et réduire le temps qui s'écoule entre le début de la compromission et le déclenchement de l'attaque. »

Sophos EDR offre une visibilité exceptionnelle de l’ensemble du parc informatique de l’entreprise, permettant aux responsables de la sécurité et de l’informatique de répondre rapidement aux questions critiques en matière d’investigations sur les menaces*(Threat Hunting)* et d’opérations de sécurité informatique, et de réagir facilement.

Parmi les nouvelles fonctionnalités :

* **Live Discover** : contrairement aux autres solutions EDR, qui ne stockent les données que pendant une ou deux semaines, Sophos EDR offre 90 jours de rétention avec l’offre de base. Grâce aux requêtes SQL prêtes à l'emploi, les administrateurs peuvent répondre aux questions relatives au *Threat Hunting* et à l’IT, en s’appuyant sur une bibliothèque d'options prédéfinies et entièrement personnalisées par les utilisateurs. Ce moteur de requêtes flexible donne accès à des enregistrements d’activité parmi les plus granulaires et les plus détaillés, également enrichis de la technologie de *Deep Learning* de Sophos.
* **Live Response** : permet de répondre et d’accéder aux périphériques et aux serveurs à l’aide d’une interface de ligne de commande afin d’effectuer un examen approfondi des problèmes et de les résoudre, de facilement redémarrer les systèmes, d’installer et de désinstaller des logiciels, de mettre fin à des processus en cours, d’exécuter des scripts, de modifier des fichiers de configuration, d’exécuter des outils d’analyse, d’isoler des machines, etc.

Sophos EDR repose sur le réseau neuronal de *Deep Learning* de Sophos, entraîné sur des centaines de millions d’échantillons pour la recherche d’indicateurs de menaces. Les analystes de sécurité et les administrateurs informatiques bénéficient également d’un accès à la demande aux renseignements sur les menaces de SophosLabs, qui surveillent, décortiquent et analysent plus de 400 000 échantillons de malwares chaque jour. Disponible dès maintenant avec [Sophos Intercept X Advanced](https://www.sophos.com/fr-fr/products/endpoint-antivirus.aspx) et [Intercept X Advanced for Server with EDR](https://www.sophos.com/fr-fr/products/server-security.aspx) sans coût supplémentaire, Sophos EDR sera compatible avec Windows, MacOS et Linux. Les nouvelles fonctionnalités *Live Discover* et *Live Response* sont facilement gérées depuis le centre d’analyse des menaces de la plateforme cloud [Sophos Central](https://www.sophos.com/fr-fr/products/sophos-central.aspx) pour un partage en temps réel des informations avec toute la suite de solutions de cybersécurité Next-Gen de Sophos grâce à l’approche unique de [sécurité synchronisée](https://www.sophos.com/fr-fr/lp/synchronized-security.aspx) de Sophos. Sophos EDR est associé à Sophos [Managed Threat Response](https://www.sophos.com/fr-fr/products/managed-threat-response.aspx) (MTR), un service 100% managé de recherche, de détection et de réponse aux menaces, permettant aux entreprises de renforcer leurs capacités grâce à l'analyse humaine pour une approche encore plus avancée de la protection proactive de la sécurité.

**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, le phishing, et bien plus encore. Sophos Central, la 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 commercialise ses produits et services exclusivement par l’intermédiaire d’un réseau mondial regroupant plus de 53 000 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. 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.