**COMMUNIQUE DE PRESSE**

**Sophos est le premier éditeur à proposer un chiffrement « always-on » pour les données partagées entre les plates-formes Windows, Mac, iOS et Android**

* *Le chiffrement « always-on » suit les fichiers où qu’ils soient*
* *Les utilisateurs collaborent facilement sur les fichiers chiffrés, que ce soit à partir de Windows, Mac, iOS ou Android*
* *Le chiffrement aide les entreprises à se conformer au nouveau règlement européen sur la protection des données personnelles (RGPD)*
* *Sophos SafeGuard 8 bénéficie d’une communication directe avec la protection Endpoint,   
  dans le cadre d’une stratégie de sécurité synchronisée*

**Bruxelles, 8 août 2016 –** [Sophos](http://www.sophos.fr/) (LSE: SOPH), leader mondial de la [sécurité des réseaux et des systèmes](https://www.sophos.com/fr-fr/security-news-trends/reports/gartner.aspx), annonce aujourd’hui la disponibilité de [Sophos SafeGuard Encryption 8](https://www.sophos.com/fr-fr/products/safeguard-encryption.aspx), une nouvelle solution de chiffrement synchronisée qui protège les données contre les vols par des malwares, des attaques ou suite à des pertes accidentelles. Toutes les organisations peuvent maintenant choisir d’adopter la bonne pratique d’un chiffrement « always-on », actif en permanence pour protéger les données accessibles sur les mobiles, les portables, les réseaux locaux et les services de partage de fichiers dans le Cloud. Sophos est le premier éditeur à fournir une solution de chiffrement persistante, transparente et proactive pour protéger les fichiers, opérationnelle aussi bien sur les plates-formes Windows et Mac que iOS ou Android.

Jusqu’à aujourd’hui, la mise en œuvre du chiffrement était considérée comme trop complexe et faisait l’objet d’une diffusion restreinte. D’après un sondage réalisé par Sophos, [The State of Encryption Today](https://secure2.sophos.com/en-us/security-news-trends/whitepapers/gated-wp/state-of-encryption-today.aspx), seulement 29% des responsables informatiques déclarent chiffrer systématiquement les smartphones et uniquement 43% les systèmes Mac, ce qui laisse une majorité d’organisations largement exposées.

« *Le chiffrement intégral à lui seul protège seulement les données en cas de vol ou de perte de mobile ou de portable. Mais les données voyagent partout - il est extrêmement difficile d’assurer une protection complète et cohérente des données quand elles sont accessibles à travers des périphériques multiples et des applications de collaboration à travers le Cloud*. » déclare Dan Schiappa, Senior Vice President et General Manager du Groupe Enduser Security de Sophos. « *Nous avons complètement repensé SafeGuard Encryption 8 pour chiffrer par défaut chaque fichier individuellement, en évaluant en permanence les droits d’accès des utilisateurs, des applications et des périphériques, afin d’assurer une collaboration sécurisée. Nous permettons aussi de fournir des fichiers protégés par mots de passe à des destinataires externes, afin de permettre les échanges sécurisés de fichiers chiffrés. Quand la protection des données est simple et transparente, les utilisateurs sont plus enclins à l’accepter, ce qui augmente la sécurité de votre organisation et sa conformité aux exigences réglementaires en matière de protection des données personnelles.* »

Un chiffrement complet et simple à gérer à grande échelle devrait figurer en bonne place dans l’agenda des responsables informatiques, dans une période de réactualisation des stratégies de protection de données pour se conformer aux nouvelles règlementations. Quand le nouveau [règlement européen sur la protection des données personnelles](https://blogs.sophos.com/2016/04/15/eu-parliament-passes-the-general-data-protection-regulation-why-its-a-good-thing/) (RGDP) entrera pleinement en vigueur le 25 mai 2018, les organisations détenant des données personnelles sur les citoyens de l’Union européenne s’exposeront à des amendes pouvant aller jusqu’à 4% de leur revenu annuel mondial en cas d’atteinte aux données personnelles, s’ils ne respectent pas les exigences du règlement. Ceci concerne non seulement les entreprises de l’Union européenne, mais toute organisation détenant des données sur les citoyens de la zone.

« *Des législations sur la protection des données personnelles sont promulguées partout dans le monde, et les organisations de toutes tailles devraient revoir leur stratégie en matière de protection des données avant de devoir faire face à des conséquences qui se durcissent. Toute société faisant du commerce avec des pays disposant de lois sur la protection des données personnelles est tenue de respecter ces législations locales*. » ajoute **Dan Schiappa**. « *Le chiffrement est largement reconnu comme étant la meilleure mesure de protection disponible pour les données. Déployer Sophos SafeGuard Encryption est une étape simple à gérer permettant à toute entreprise de mettre en œuvre une bonne pratique pour la sécurité des données, aussi bien pour protéger les informations sensibles ou propriétaires que pour* [*assurer la conformité aux législations telles que le nouveau règlement européen*](https://www.sophos.com/fr-fr/lp/compliancecheck.aspx)*.* »

Dans le cadre de la stratégie de sécurité synchronisée de Sophos, SafeGuard Encryption 8 peut automatiquement répondre aux incidents de sécurité grâce à sa connexion en temps réel avec la protection Endpoint de Sophos. Lors de la détection d’une infection active sur un système, Sophos SafeGuard Encryption peut temporairement révoquer les clés de chiffrement sur ce système pour protéger les données. Les utilisateurs pourront automatiquement récupérer leurs clés une fois l’incident résolu. Sophos SafeGuard Encryption synchronise également ses clés avec Sophos Mobile Control afin de fournir un accès fluide et transparent aux utilisateurs habilités, à partir de leurs smartphones et tablettes, chaque document chiffré étant accessible d’une manière sécurisée à travers l’application Secure Work Space.

« *Il y a quatre raisons principales de s’intéresser au chiffrement pour les entreprises. La première et la plus importante est la protection des données sensibles contre les attaques ciblant le vol de données. La seconde est la diffusion accidentelle de données, suite par exemple à l’oubli d’un mobile ou d’une clé USB dans un taxi ou l’envoi d’un courriel incluant des documents sensibles à la mauvaise personne, ce qui arrive malheureusement bien trop souvent. La troisième est la conformité aux lois telles que le nouveau règlement européen RGDP, afin de réduire les risques d’amendes de plus en plus substantielles. Enfin, la transition croissante vers des services Cloud présente des risques pour la sécurité des données, que le chiffrement peut aider à maîtriser*. » déclare **Duncan Brown, Directeur de Recherche en Pratique Européenne de Sécurité chez IDC.** *« Pour que le chiffrement soit efficace dans ces quatre cas de figure, il doit être simple à gérer pour le responsable IT, transparent pour les utilisateurs et fonctionner avec des plates-formes et des types de fichiers multiples. Sophos remplit toutes ces conditions avec SafeGuard Encryption, permettant aux entreprises de rapidement adopter le chiffrement comme mesure de sécurité indispensable*. »

**Connectez-vous avec Sophos**[Twitter](http://soph.so/CfuKd)

[LinkedIn](http://soph.so/Cfv36)

[Facebook](http://soph.so/CfvaA)

[Google+](https://plus.google.com/+sophos)

[Spiceworks](http://soph.so/Cgbwa%20)

[YouTube](http://www.youtube.com/user/sophoslabs)

[Naked Security News](http://nakedsecurity.sophos.com/)

[Sophos Blog](http://blogs.sophos.com/)

[Blog Sophos France](http://www.sophosfranceblog.fr)

**A propos de Sophos**Plus de 100 millions d’utilisateurs dans 150 pays font confiance à [Sophos](http://www.sophos.fr/) en tant que meilleure protection contre les menaces complexes et les pertes de données. Sophos propose des solutions de protection simples à administrer, déployer et utiliser pour le [Web](http://www.sophos.com/fr-fr/products/web.aspx), les [courriers électroniques](http://www.sophos.com/fr-fr/products/email.aspx), les [mobiles](http://www.sophos.com/fr-fr/products/mobile.aspx), les [données avec le chiffrement](http://www.sophos.com/fr-fr/products/encryption.aspx), les [systèmes](http://www.sophos.com/fr-fr/products/endpoint.aspx) et les [réseaux](http://www.sophos.com/fr-fr/products/network.aspx), qui s’appuient sur les SophosLabs, réseau mondial de centres d’analyse des menaces.

**Contacts Presse**

Square Egg, Sandra Van Hauwaert, GSM 0032 497251816, [Sandra@square-egg.be](mailto:Sandra@square-egg.be)