SOPHOS

CYBERSECURITY EVOLVED : LES BÉNÉFICES DE LA SÉCURITÉ SYNCHRONISÉE DE SOPHOS

Une quantification des bénéfices concrets du système de cybersécurité de Sophos en termes de protection et de gain de temps à travers cinq témoignages clients.

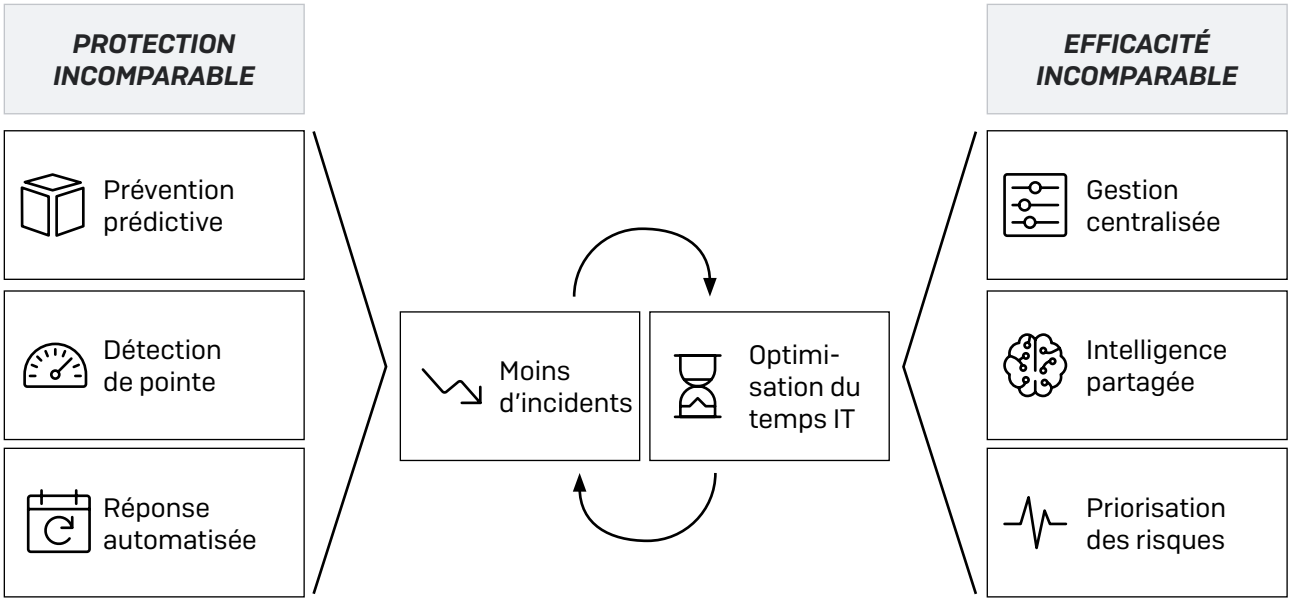
Livre blanc Sophos Juin 2020

Introduction

Lorsque vous choisissez Sophos pour votre cyber protection, vous profitez du système de cybersécurité original, et de loin le meilleur sur le marché : la Sécurité Synchronisée.

- **Portefeuille complet de produits et services Next-Gen.** Nous répondons à tous vos besoins en matière de cybersécurité : protection des postes, mobiles et serveurs, EDR, pare-feu Next-Gen, messagerie, solution UEM (Unified Endpoint Management) et bien plus encore. Que votre environnement soit déployé dans le Cloud, sur site ou dans une architecture hybride, nous avons ce qu'il vous faut.
- **Protection inégalée.** Tirez profit à la fois des toutes dernières technologies de protection et de l'expertise de nos SophosLabs et de nos équipes de haut vol spécialisées en science des données et en recherche des menaces. La détection haut de gamme bloque les attaques avancées d'aujourd'hui tandis que les réseaux neuronaux artificiels du Deep Learning bloquent de manière prédictive les menaces inédites. Les produits Sophos fonctionnent ensemble en temps réel pour consolider votre protection. Ils discutent entre eux et partagent des informations sur les menaces et l'état de sécurité, et répondent automatiquement aux incidents.
- **Une seule plateforme d'administration.** Administrez toutes vos solutions Sophos dans Sophos Central, notre plateforme d'administration basée dans le Cloud. Elle exploite les données partagées pour livrer et hiérarchiser les informations sur les risques, et vous guide dans vos investigations grâce à des actions recommandées pour chaque scénario.

Le système de cybersécurité Sophos **augmente votre protection** tout en **réduisant votre coût total de possession (TCO).** Il y parvient en créant un cercle vertueux où la protection et l'efficacité incomparables des solutions se renforcent mutuellement de manière continue.



Ce cercle vertueux fait gagner un temps considérable à votre équipe informatique et permet de réduire votre exposition aux menaces, le tout sans augmenter vos effectifs.

Bénéfices pour les clients

Pour mesurer les bénéficies concrets de la Sécurité Synchronisée de Sophos, nous avons réalisé une série d'entretiens avec 5 clients Sophos basés en Amérique du Nord, Europe et Asie. Chaque scénario de client était différent, avec des structures organisationnelles, des défis et des besoins professionnels spécifiques. Cependant, ils ont tous constaté la même chose :

Les clients ont déclaré qu'ils devraient ***doubler*** *leurs effectifs de sécurité pour maintenir le même niveau de protection s'ils ne disposaient pas de la Sécurité Synchronisée de Sophos.*

Ils nous ont également confié subir moins d'incidents de sécurité et être capable d'identifier et de répondre plus rapidement à ceux qui se présentent. Les résultats concrets pour les clients Sophos incluent :

- Réduction de 50 % des effectifs de la sécurité IT
- Réduction de plus de 90 % du temps consacré chaque jour à l'administration de la cybersécurité
- Réduction de plus de 90 % du temps nécessaire pour identifier les problèmes
- Réduction de 85 % du nombre d'incidents de sécurité
- Réduction significative des temps d'arrêt dans l'ensemble de l'entreprise

Client A : Prestataire de soins de santé, USA

- 4 500 employés
- 80 personnels IT, dont 3 dédiés à la cybersécurité
- Produits Sophos : Intercept X Advanced with EDR, XG Firewall, Intercept X for Server (Windows, Linux et machines virtuelles)

Le client A est un centre hospitalier régional, offrant des soins hospitaliers et ambulatoires, des consultations médicales, une maison de retraite et toute une gamme de services spécialisés.

Impact sur l'entreprise

- **Réduction de 50 % des besoins en ressources consacrées à la sécurité informatique**
  Le client emploie actuellement 3 responsables de la cybersécurité. Ils ont calculé que sans Sophos ils auraient besoin d'employer 3 analystes de sécurité supplémentaires à temps plein uniquement pour couvrir la réponse aux incidents.

  Avant Sophos, l'équipe devait analyser manuellement tous les événements sur le réseau et leur temps était essentiellement dédié à l'identification des incidents. Aujourd'hui, Sophos identifie pour eux les incidents de manière proactive et remédie automatiquement à la situation dans 95 % des cas. Ainsi, l'équipe peut se concentrer sur la résolution des 5 % d'incidents qui nécessitent une intervention manuelle.

- **Réduction de plus de 90 % des tâches quotidiennes d'administration de la sécurité**
  Le responsable de la sécurité IT passe 30 minutes par jour à examiner les logs et à analyser tout ce qui est problématique. Avant Sophos, il lui fallait une journée entière pour obtenir le même niveau d'information et de sécurité. Avec Sophos, toutes les données sont consolidées dans une seule plateforme d'administration et présentées dans un format cohérent, ce qui facilite l'identification des incidents et leur remédiation. Il n'est plus nécessaire de cartographier au quotidien les données de plusieurs sources pour tenter de différencier les données suspectes des données malveillantes ou bénignes.

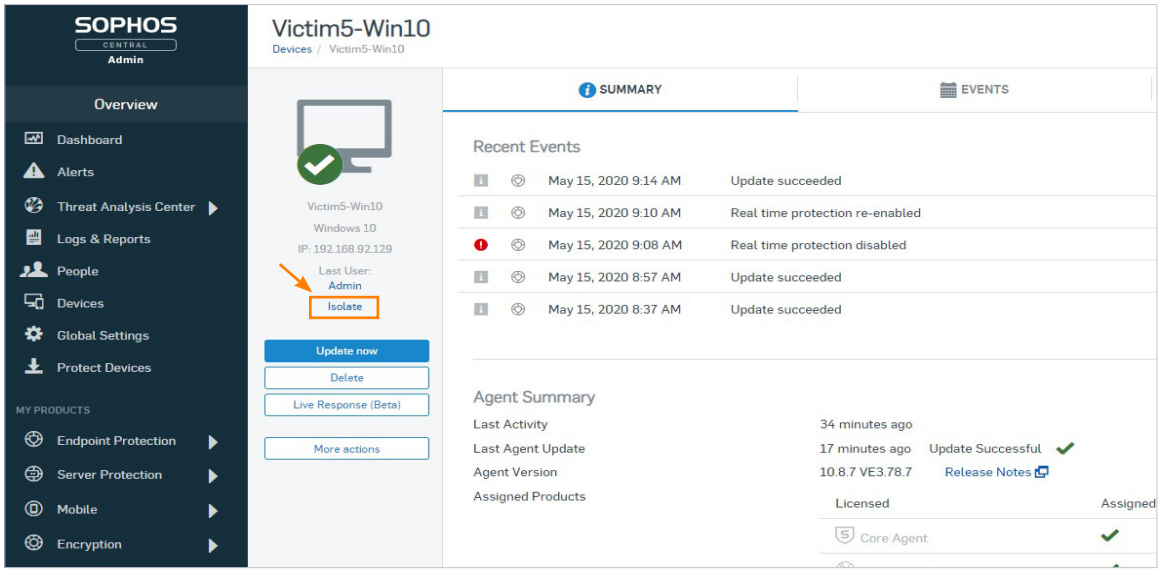
- **Réduction de 85 % des incidents de sécurité**
  En tant qu'hôpital, ils détiennent de grandes quantités de données personnelles identifiables (PII) sensibles, ainsi que des informations de paiement, ce qui en fait une cible de choix pour les cybercriminels. Avant Sophos, ils déploraient en moyenne 3 incidents de sécurité par jour qui nécessitaient une investigation plus approfondie. Avec Sophos, ce chiffre a été réduit à une moyenne de 1 incident tous les 3 jours.

- **Réduction de plus de 90 % du temps consacré à l'investigation d'un incident**
  Avant Sophos, une investigation approfondie d'un incident prenait environ 3 heures et nécessitait un accès local à l'ordinateur affecté. Aujourd'hui, tout est fait à distance via la plateforme Sophos Central et ne prend pas plus de 15 minutes.

  Auparavant, l'équipe devait désactiver la carte réseau, puis travailler physiquement sur l'appareil pour enquêter et résoudre le problème avant de tout reconnecter manuellement. Elle devait également s'adapter aux flux de travail des utilisateurs, par exemple attendre qu'un médecin ne soit plus en consultation pour pouvoir accéder au système. La possibilité d'isoler l'appareil via la console Sophos Central permet à l'équipe d'analyser l'incident à distance sans affecter la disponibilité des utilisateurs et du système.

  Réduire le temps de l'investigation et pouvoir tout gérer à distance a également permis de réduire de manière significative les perturbations pour les autres utilisateurs de l'hôpital.

- **Protection ininterrompue pendant les investigations**
  Auparavant, pour les besoins de l'investigation manuelle, les appareils étaient retirés du réseau et la protection ne pouvait pas être mise à jour lorsqu'ils étaient hors ligne. Avec Sophos, lorsque l'équipe informatique isole un appareil pour analyser l'incident, il reste en ligne et continue de recevoir les mises à jour de sécurité.



Client B : Prestataire de services d'éducation, Inde

- 700 employés
- Siège social à Bangalore, + des responsables locaux sur place dans toute l'Inde et la région de l'Asie du Sud-Est
- Produits Sophos : Intercept X Advanced with EDR, Intercept X Advanced for Server, XG Firewall

Le client B fournit des services éducatifs à des universités dans toute l'Inde et la région de l'Asie du Sud-Est. Il protège des dizaines de milliers d'étudiants grâce à une équipe informatique centralisée basée au siège social à Bangalore, ainsi qu'à une équipe de responsables informatiques basés sur sites.

Impact sur l'entreprise

- **Réduction de 50 % des ressources nécessaires pour la gestion quotidienne de la sécurité**
  Auparavant, ils employaient 4 ingénieurs pour gérer la sécurité au quotidien. Depuis qu'ils ont adopté Sophos, seuls 2 ingénieurs sont nécessaires pour assurer la sécurité dans toute l'organisation.
- **Réduction de 94 % du temps nécessaire pour identifier les zones à haut risque nécessitant une investigation**
  Avant Sophos, il fallait au client 3 à 4 heures pour identifier les incidents critiques qu'il devait analyser de manière plus approfondie. Aujourd'hui, il ne lui faut plus que 10 à 15 minutes pour identifier les priorités en matière de sécurité sur l'ensemble du parc IT depuis Sophos Central.
- **Réduction de 98 % du temps nécessaire pour identifier la source d'un trafic indésirable sur le réseau**
  Auparavant, il fallait 2 jours (et parfois plus) pour identifier quel appareil sur le réseau était à l'origine d'un problème de performance ou de sécurité. Aujourd'hui, il ne faut plus que 15 minutes pour identifier le problème et lancer des actions pour y remédier.
- **Réduction de 95 % du temps consacré à la gestion des mises à jour des firmwares**
  Auparavant, les mises à jour des logiciels prenaient entre 3 et 4 heures, ce qui créait de réels problèmes de disponibilité et de risques. Aujourd'hui, avec Sophos, les mises à jour ne prennent pas plus de 10 minutes. Avec 20 à 25 mises à jour par an, ils gagnent ainsi 75 heures par an (l'équivalent de 2 semaines de travail complètes).

Client C : Prestataire de services en recherche clinique, USA

- 150 employés répartis sur quatre sites
- 2 informaticiens, couvrant tous les domaines, y compris la cybersécurité
- Produits Sophos : Intercept X Advanced with EDR, XG Firewall, Central Device Encryption

Le client C est un organisme du secteur privé qui fournit les données d'essais cliniques nécessaires pour obtenir les autorisations de mise sur le marché de nouveaux médicaments. En raison de la nature de ses activités, il détient de grandes quantités de données personnelles sensibles.

Impact sur l'entreprise

- **Réduction de 50 % des besoins en ressources informatiques**
  Ce client dispose d'une petite équipe de 2 personnes seulement pour gérer tous les aspects des technologies de l'information. Actuellement, ils passent 1 heure par jour à examiner les logs et à analyser tout ce qui est problématique. S'ils devaient se séparer de Sophos, ils estiment qu'ils devraient engager 1 ou 2 ingénieurs en sécurité supplémentaires pour gérer les logs.

- **Réduction de 33 % du temps nécessaire pour traiter un incident potentiel**
  Auparavant, lorsqu'un appareil connaissait un incident de sécurité, la solution était de réimager la machine, ce qui prenait entre 90 minutes et 2 heures. Aujourd'hui, ils peuvent mener des investigations approfondies, allant de l'isolement du système et de la traque des menaces jusqu'à l'analyse et la remédiation complètes de la sécurité, le tout en 1 heure environ, sans avoir à réinitialiser la machine. Un avantage supplémentaire de l'approche Sophos est que l'utilisateur peut commencer à être productif dès que l'investigation est terminée, alors qu'avec la restauration de l'image, il perdrait du temps à réinitialiser la configuration et à réinstaller les logiciels sur sa machine.
- **Réduction de 88 % du risque de menace car ils peuvent identifier les problèmes beaucoup plus rapidement**
  Grâce à la Sécurité Synchronisée de Sophos, l'équipe IT peut identifier les nouveaux incidents qui doivent être examinés dans les minutes qui suivent l'arrivée d'un événement suspect. Avant Sophos, il fallait une journée entière pour parcourir les logs afin de trouver les incidents qui devaient être analysés. Ce gain de temps réduit considérablement l'exposition aux menaces.
- **Amélioration du comportement des utilisateurs**
  Avec Sophos, les utilisateurs savent désormais que l'équipe informatique peut rapidement résoudre les problèmes et les incidents sans les interrompre ni entrainer de surcroît de travail. Ainsi, l'équipe informatique rapporte que les utilisateurs sont désormais beaucoup plus disposés à signaler des problèmes ou des préoccupations (par exemple, ils ont cliqué sur un lien potentiellement malveillant dans un email).

Client D : Prestataire de service public, Serbie

- 300 employés
- 10 personnels IT, dont 4 dédiés à la cybersécurité
- Produits Sophos : Intercept X Advanced, Intercept X Advanced for Server, XG Firewall, Sophos Email, Sophos Mobile

Le client D est un organisme du secteur public qui couvre la capitale serbe, Belgrade. Ce client Sophos de longue date a évolué vers nos produits Next-Gen administrés dans Sophos Central.

Impact sur l'entreprise

- **Réduction de 50 % du temps consacré à la gestion quotidienne de la sécurité**
  Ils consacrent désormais 30 minutes par jour à l'administration de la sécurité, analysant les alertes, les logs, les utilisateurs, les appareils, le trafic et les applications dans la console d'administration Sophos Central, pour s'assurer que tout est en ordre. Auparavant, il leur fallait au quotidien au moins 2 fois plus de temps pour identifier les incidents de sécurité à traiter en priorité et prendre les mesures nécessaires.
- **Réduction de plus de 90 % du temps consacré à la gestion quotidienne de la sécurité par rapport aux autres éditeurs**
  Le client estime, sur la base de son expérience, que la gestion quotidienne de la sécurité prendrait une journée entière avec d'autres éditeurs, contre seulement 30 minutes avec Sophos.
- **Zéro incident de sécurité majeur**
  Le client utilise Sophos depuis de nombreuses années et n'a pas connu d'incident de sécurité majeur depuis 8 à 10 ans. Cela ne veut pas dire qu'il n'est pas la cible d'attaques, mais plutôt que ses produits Sophos y remédient rapidement et discrètement en arrière-plan, sans que l'utilisateur ne s'en aperçoive.

Client E : Organisme de réglementation, Slovénie

- 150 employés, dont 1/3 travaille à distance et 2/3 sont basés au siège social
- 2 informaticiens, couvrant tous les domaines, y compris la cybersécurité, + le soutien de fournisseurs externes pour les grands projets
- Produits Sophos : Sophos Endpoint Protection, Intercept X Advanced for Server, XG Firewall, Sophos Mobile, Sophos Device Encryption

Le client E est un organisme du secteur public chargé de veiller à ce que les produits répondent aux normes requises. Ce client Sophos de longue date a évolué vers nos produits Next-Gen administrés dans Sophos Central.

Impact sur l'entreprise

- **Réduction de 50 % du temps consacré à la gestion quotidienne de la sécurité**
  Ils consacrent chaque jour 15 à 30 minutes à l'administration de la sécurité : contrôle du pare-feu, analyse des alertes, nettoyage de la quarantaine des emails, etc. Auparavant, ils y auraient passé au moins 2 fois plus de temps. Ce gain d'efficacité est dû au fait qu'ils peuvent gérer tous leurs produits de sécurité dans une seule console et qu'ils n'ont pas besoin de passer d'une application à l'autre ou d'un serveur à l'autre.
- **Zéro incident de sécurité majeur**
  Le client n'a pas souvenir d'un incident de sécurité majeur depuis qu'il utilise Sophos.

Conclusion

Comme le montrent les témoignages de nos clients, la stratégie de Sophos en matière de cybersécurité permet de réaliser de réelles économies en termes de protection et d'efficacité. Cela fait gagner un temps considérable à votre équipe informatique et permet de réduire votre exposition aux menaces, le tout sans augmenter vos effectifs.

Bien que les environnements, les ressources et les défis de nos clients varient d'une société à l'autre, ils font tous état d'une réduction de 50 % de la charge de travail en matière de sécurité informatique grâce à l'utilisation de la Sécurité Synchronisée de Sophos. Les clients profitent au quotidien du gain de temps de plus de 90 % dans l'administration de la cybersécurité, ainsi que d'une réduction de 85 % du nombre d'incidents de sécurité.

Pour en savoir plus sur les solutions de cybersécurité de Sophos et pour commencer un essai gratuit sans obligation, allez sur **www.sophos.fr**, ou discutez avec un représentant Sophos.

Équipe commerciale France
Tél. : 01 34 34 80 00
Email : partners@sophos.fr

20-06-12 WPFR (NP)

SOPHOS