SOPHOS
Cybersecurity evolved.

Écosystème de cybersécurité adaptatif Sophos ACE (Adaptive Cybersecurity Ecosystem)

Sophos Adaptive Cybersecurity Ecosystem (ACE), ou écosystème de cybersécurité adaptatif, est un système étendu conçu pour optimiser la prévention, la détection et la réponse aux menaces. Il protège les systèmes interconnectés d'aujourd'hui et défend contre les cyberattaques toujours plus évolutives combinant désormais automatisation et piratage en direct.

Sophos ACE exploite l'automatisation et des opérateurs humains, ainsi que l'apport collectif des produits Sophos, des partenaires, des clients et des développeurs, pour créer une protection qui s'améliore en permanence — un cycle vertueux qui apprend et progresse en continu. Et surtout, vous pouvez démarrer par une base simple et évoluer petit à petit: commencez par la technologie Sophos Endpoint ou Firewall et étendez ensuite votre protection.

Un livre blanc Sophos. Mai 2021

Un paysage en mutation

Le paysage dans lequel se développe la cybersécurité est en constante évolution, et des changements importants sont intervenus ces dernières années, tant dans les environnements des entreprises que dans la nature des attaques.

Mutation des entreprises : l'interconnectivité

Dans leur recherche constante de moyens d'améliorer leur productivité et leur efficacité, les entreprises ont créé une chaîne d'approvisionnement très interconnectée, tout comme l'infrastructure et les technologies nécessaires à son fonctionnement. La migration des données et des applications vers le Cloud a apporté de nombreux avantages, comme la possibilité de travailler depuis n'importe où, la réduction des coûts d'exploitation et l'amélioration des performances et de l'évolutivité, tout en catalysant la croissance de la chaîne d'approvisionnement mondiale et numérique.

En parallèle, la crise du Covid-19 a rapidement accéléré l'adoption du travail à domicile/distance, et ce faisant, a fait voler en éclats les derniers vestiges de périmètre organisationnel. Les personnes, applications, appareils et données peuvent maintenant se trouver n'importe où.

Si ces systèmes interconnectés et dispersés nous sont utiles, ils créent également de nouveaux défis pour la sécurité. En effet, de nombreuses entreprises ont du mal à cartographier l'étendue de leur réseau, et donc de sécuriser tous les systèmes qui y sont connectés.

Des adversaires intelligents et capables de s'adapter ciblent sans relâche ces systèmes, attirés par l'ampleur des opportunités qu'ils offrent. L'attaque de SolarWinds en décembre 2020 en est un exemple récent, mais pas le seul, ayant touché des victimes de tous horizons : grands fournisseurs de technologie, petites entreprises, entités du secteur public du plus haut niveau, etc.

Mutation des attaques : de l'automatisation à l'opérationnel

Lorsque vous travaillez dans le domaine de la cybersécurité, il est facile de perdre de vue un fait important, mais largement sous-estimé : dans la bataille qui se joue autour de nos systèmes et données critiques, la victoire est du côté des personnes qui se défendent.

Les gros titres des journaux qui rapportent de nouvelles violations de sécurité ont une utilité importante : ils nous rappellent qu'il faut prendre des mesures préventives et rester vigilant. Mais ces histoires sont l'exception à la règle. Les entreprises qui se défendent avec succès contre des milliers de tentatives de violation quotidiennes ne font jamais la Une des journaux.

Non seulement l'efficacité de la cybersécurité s'est considérablement améliorée, mais les outils et services de sécurité managés les plus récents sont plus accessibles et efficaces que jamais. Des technologies anti-ransomware, anti-exploit, anti-phishing et de détection des comportements sont désormais à la disposition de tous.

MUTATION DES ENTREPRISES

Chaîne d'approvisionnement interconnectée

Migration dans le cloud des applications et des données

Environnements de travail distants

MUTATION DES ATTAQUES

Les cyber défenseurs gagnent

Automatisation et opération des attaquants

Coûts des violations plus élevés

Ces capacités, qui sont facilitées, améliorées et accélérées par l'intelligence artificielle et le Machine Learning, s'attaquent aux tactiques, techniques et procédures adverses connues et documentées dans le cadre de MITRE ATT&CK, ainsi qu'aux attaques nouvelles et inédites. En comblant les failles, en bloquant les chemins et en arrêtant les techniques, le coût de certaines attaques a fondamentalement augmenté pour les attaquants, les obligeant à s'adapter. Les améliorations en matière de sécurité sont si importantes que le vieil adage « un attaquant n'a besoin de réussir qu'une seule fois. » n'est plus une réalité. Pour gagner de l'argent, les attaquants doivent désormais réussir plusieurs fois au cours d'une même attaque.

Ils sont de fait passés de malwares automatisés à une approche plus globale qui combine automatisation et piratage manuel. Le principal objectif des adversaires est de ne pas être détectés, et la meilleure façon d'y parvenir est d'agir comme un employé, en employant des outils locaux, des appareils locaux et des modèles de trafic classiques.

Ces attaques sophistiquées, qui nécessitent un investissement humain important, sont d'autant plus coûteuses pour les victimes. En effet, les attaquants sont en mesure d'exploiter leur connaissance approfondie de l'environnement de la victime pour causer un maximum de dommages, et générer un profit substantiel.

La mutation de la cybersécurité vers les opérations de sécurité

La mutation des entreprises et des attaques nécessite une évolution de la sécurité informatique. Les entreprises font face à des adversaires intelligents qui modifient sans cesse leur objectif à mesure qu'ils l'atteignent, obligeant les équipes de cybersécurité à développer des contre-mesures qui améliorent leurs chances de gagner.

Pour cela, il faut tout d'abord passer de la **gestion de la sécurité à des opérations de sécurité**. L'époque des politiques de sécurité de type « Set-and-Forget » (définir et oublier) est révolue. À mesure que les attaquants s'impliquent manuellement, les équipes de cybersécurité doivent se mettre au même niveau pour chasser et détecter les comportements et les événements suspects avant que ces derniers ne se transforment en violation.

Les équipes de sécurité doivent chercher les activités suspectes le plus tôt possible dans la chaîne d'attaque afin de donner aux défenseurs la possibilité de répondre avant que des dommages ne soient causés. Même les attaquants les plus furtifs vont laisser des indices derrière eux, et les équipes de sécurité doivent trouver et suivre ces pistes pour bloquer l'attaque dès ses prémices. Il ne s'agit plus seulement de trouver un signal suspect dans le bruit de fond, mais d'identifier les signaux faibles critiques avant qu'ils ne deviennent des signaux forts. Plus le signal est fort, plus vous êtes proche d'une violation. Avec des outils appropriés, les failles informatiques peuvent être détectées de manière proactive et corrigées avant qu'un adversaire ne soit en mesure de les découvrir et de les utiliser dans une attaque.

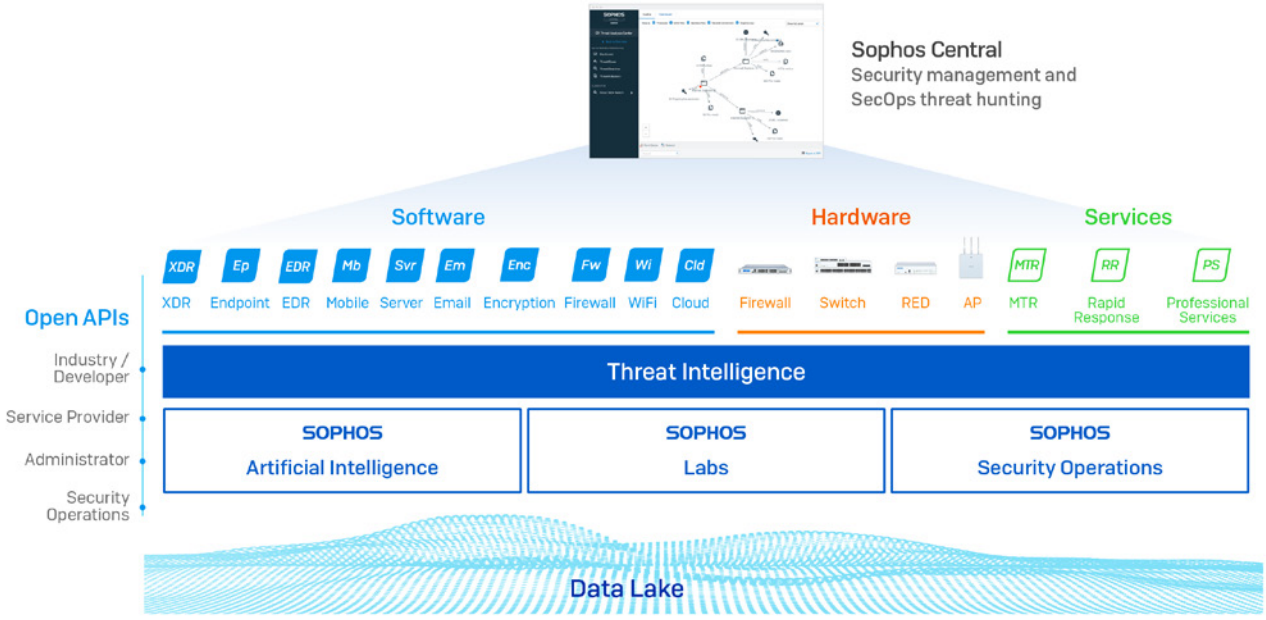
Les entreprises étant désormais tellement interconnectées, la sécurité doit suivre le mouvement. Les équipes de cybersécurité doivent passer de produits de sécurité individuels non intégrés à un **système de sécurité adaptatif** qui offre le maximum de prévention automatique, tout en permettant aux opérateurs de rechercher et de détecter des signaux plus faibles (tels que des comportements et des événements suspects) et de les empêcher de se transformer en violation.

Les environnements des entreprises et les attaques évoluent en permanence. L'avenir de la sécurité informatique est un système qui permet une boucle de rétroaction unique qui **apprend et s'améliore en continu**. Les nouvelles informations et nouveaux événements détectés par l'équipe opérationnelle peuvent être automatisés, améliorant la prévention et réduisant le nombre de nouvelles attaques entrant dans le système. De même, à mesure que les logiciels d'automatisation s'améliorent, les opérateurs peuvent trouver plus rapidement les comportements et les événements suspects, réduisant davantage les incidents. Ce cycle vertueux améliore en permanence la sécurité globale des entreprises et de leurs activités connectées.

Écosystème de cybersécurité adaptatif Sophos (ACE)

La bonne nouvelle est que ce système existe déjà. L'écosystème de cybersécurité adaptatif Sophos ACE (Adaptive Cybersecurity Ecosystem) répond à cette nouvelle réalité. Il exploite la puissance de l'automatisation et l'expertise des analystes pour évoluer de la gestion de la sécurité aux opérations de sécurité. L'automatisation permet d'analyser et de répondre plus rapidement aux comportements et aux événements suspects, tandis que les analystes humains sont plus à même de corréler de multiples signaux suspects et d'en interpréter la signification.

Sophos ACE a été conçu pour protéger l'interconnexion de nos entreprises et du monde en ligne. Il protège les systèmes et les données où qu'ils se trouvent, et apprend et s'améliore en permanence pour se prémunir contre les évolutions technologiques et les attaques futures.



Sophos ACE s'appuie sur l'**intelligence sur les menaces** collective provenant des SophosLabs, de Sophos Security Operations (des analystes qui réalisent une chasse aux menaces avancée dans des milliers d'environnements clients via notre service Managed Threat Response) et du groupe Sophos Artificial Intelligence. Ces capacités d'intelligence en temps réel améliorent en permanence les technologies de pointe de nos offres **logicielles** et **matérielles** de premier plan.

Un **data lake** unique et intégré rassemble les données provenant de tous nos produits et de nos sources d'intelligence sur les menaces. Des analyses en temps réel du data lake permettent aux défenseurs de prévenir les violations en trouvant de manière proactive les signaux suspects dans le bruit de fond. En parallèle, des **API ouvertes** permettent aux clients, partenaires et développeurs de créer des outils et des solutions qui interagissent avec le système. Tout est géré depuis la **plateforme d'administration Sophos Central**. Toute votre sécurité est au même endroit pour une efficacité inégalée.

Ces 5 éléments : intelligence sur les menaces, technologies Next-Gen, data lake, API et gestion centralisée fonctionnent ensemble pour créer un écosystème de cybersécurité adaptatif qui apprend et s'améliore en continu. Et si la puissance de l'écosystème complet est considérable, vous pouvez l'utiliser à l'échelle, petite ou grande, qui vous convient. De nombreux clients commencent par notre protection Endpoint ou Firewall, puis étendent leur protection à leur propre rythme.

L'année dernière, de nombreux centres d'opérations de sécurité (SOC) se sont virtualisés. Sophos ACE peut être géré par des experts en sécurité depuis n'importe quel endroit, permettant aux entreprises de trouver les meilleurs talents spécialisés cybersécurité dans le monde. Par ailleurs, nos experts peuvent gérer la détection et la réponse aux menaces en tant que service pour vous.

L'évolution de la Sécurité Synchronisée

La Sécurité Synchronisée, c'est-à-dire la capacité des produits Sophos à partager des informations en temps réel via un Security Heartbeat™ et à automatiser la réponse aux incidents, est la pierre angulaire de notre protection depuis de nombreuses années. Lors de son lancement en 2015, la Sécurité Synchronisée était un concept unique sur le marché, et nous continuons d'offrir l'intégration la plus complète avec des données multi-produits plus riches.

« Sophos reste leader du marché grâce à ses capacités XDR entre ses produits Endpoint et Firewall. »

Gartner
Gartner Magic Quadrant for Enterprise Network Firewalls,
Analystes : Rajpreet Kaur | Adam Hils | Jeremy D'Hoinne | 9 novembre 2020

L'écosystème de cybersécurité adaptatif de Sophos s'appuie sur l'automatisation et l'intégration de la Sécurité Synchronisée pour étendre davantage le système de cybersécurité Sophos.

Plus de visibilité

Personne ne sait d'où viendra la prochaine attaque, et il est tout simplement impossible pour les opérateurs humains de tout surveiller. Vous avez besoin d'un système qui surveille tout pour vous permettre de réagir rapidement aux menaces émergentes. C'est pourquoi nous avons étendu l'écosystème pour inclure un éventail encore plus large de technologies, notamment la nouvelle solution Sophos XDR (Extended Detection and Response) et nos API. Les produits Sophos voient et enregistrent tous les événements suspects, les comportements et les détections dans votre environnement, vous donnant les informations dont vous avez besoin à portée de main.

Plus de données

Le data lake combine et corrèle les données provenant de tous ces capteurs pour fournir des informations plus approfondies sur les produits. Les opérateurs peuvent l'interroger directement avec Sophos Intercept X with XDR. Vous pouvez identifier les comportements et les événements suspects dans l'ensemble de votre environnement — et empêcher les problèmes de se transformer en violation.

Plus d'intelligence

Avec la croissance rapide de notre service Managed Threat Response (MTR), nous sommes en mesure d'ajouter des données en temps réel provenant de nos chasseurs de menaces pour compléter les données de détection. En parallèle, nous continuons à faire progresser nos modèles d'IA et les données de détection des menaces des SophosLabs.

Plus d'intégration

Les SophosLabs, Sophos AI et Sophos Security Operations travaillent ensemble, intégrant leur expertise au profit de tous les clients dans un cycle virtuel. Par exemple, PowerShell est un outil légitime avec de nombreux usages de confiance qui est aussi largement détourné par les attaquants. Les opérateurs MTR entraînent nos modèles d'IA à distinguer les « bonnes » et les « mauvaises » utilisations de PowerShell sur la base de leurs expériences réelles. L'ensemble du système est ensuite mis à jour grâce à cet apprentissage de l'IA, afin d'améliorer la protection des clients.

L'écosystème de cybersécurité adaptatif Sophos (ACE) en action

Sophos ACE est un système qui existe déjà et qui renforce et étend la protection dans des scénarios réels. En mars 2021, un groupe de cyberattaquants appelé Hafnium a exploité la vulnérabilité ProxyLogon dans Microsoft Exchange. Il s'agissait d'une vulnérabilité de type Zero Day et les attaquants ont profité des failles inhérentes à la conception d'Exchange pour éviter de déclencher des détections immédiates.

Dès que la vulnérabilité a été connue, le service Sophos Managed Threat Response (MTR) a instantanément mis à jour la surveillance des capteurs pour inclure les comportements associés à ProxyLogon. Les données étant versées dans le data lake, l'équipe Sophos MTR a eu un accès instantané à toutes les données dont elle avait besoin pour identifier et remédier aux activités malveillantes liées à cette vulnérabilité.

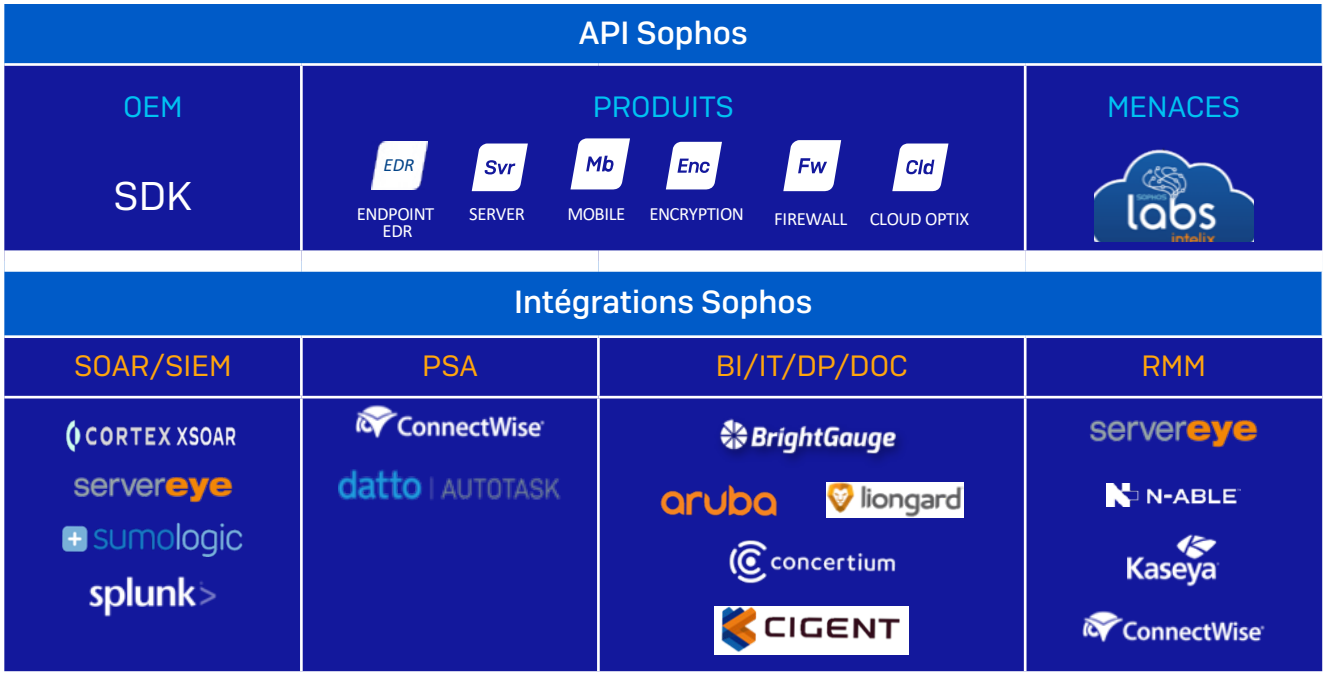
De plus, l'équipe MTR a combiné ses compétences en matière de chasse aux menaces avec la technologie Sophos EDR pour découvrir de nouveaux éléments ou indicateurs de compromission (IOC) liés à l'attaque. Ces indicateurs ont été partagés directement avec les SophosLabs qui les ont utilisés pour publier des IOC supplémentaires liés à la vulnérabilité d'Exchange, offrant ainsi une protection supplémentaire à tous les clients Sophos.

Une plateforme ouverte avec des intégrations puissantes et des API ouvertes

Dans notre monde interconnecté, il est essentiel que la cybersécurité puisse s'intégrer à l'environnement élargi des entreprises. La cybersécurité présente de multiples facettes et l'écosystème de cybersécurité adaptatif de Sophos prend en charge un large éventail de besoins en matière de sécurité, notamment :

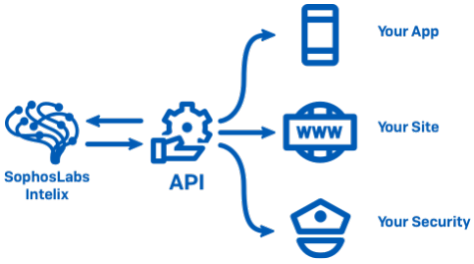
- MSSP — en soutenant la fourniture de cyberdéfenses avancées à leurs clients.
- Partenaires Channel — en rationalisant leurs processus commerciaux.
- Fournisseurs d'accès à Internet (FAI) — en leur permettant de garantir la sécurité des services Internet qu'ils fournissent.
- PME — en facilitant la création d'outils personnalisés pour contrôler et activer la sécurité.

Une multitude d'API et d'intégrations sont déjà en place (et d'autres sont à venir) avec Sophos ACE, qui gère déjà plus de 5 millions de requêtes API par jour.



Exemple d'API : SophosLabs Intelix™

Intelix est une suite d'API RESTful simples et à réponse rapide qui permet aux applications d'identifier, de classer et de prévenir les menaces, renforçant ainsi leur sécurité. Les clients, partenaires et développeurs de l'écosystème Sophos peuvent utiliser ces API pour effectuer des recherches de menaces dans le Cloud, des analyses statiques ou dynamiques des fichiers. Vous trouverez de plus amples informations sur les API SophosLabs Intelix sur : https://www.sophos.com/fr-fr/labs/intelix.aspx.



Sophos ACE : pour un impact réel sur l'entreprise

Les bénéfices de l'écosystème de cybersécurité adaptatif Sophos ACE s'additionnent. La combinaison de technologies Next-Gen (intelligence sur les menaces des SophosLabs, Sophos AI et Sophos Security Operations), d'un système intégré, adaptatif et en apprentissage permanent, et d'une gestion centralisée via la plateforme Sophos Central a un impact considérable sur la protection et l'efficacité.

Technologies Next-Gen	**+**	**Intelligence sur les menaces**	**+**	**Système adaptatif intégré**	**+**	**Gestion centralisée**

Les clients utilisant conjointement Sophos Firewall et Sophos Intercept X nous disent déjà qu'ils auraient dû doubler leurs effectifs de sécurité pour maintenir le même niveau de protection s'ils n'avaient pas un système de cybersécurité Sophos. Ils nous ont également dit qu'ils ont subi moins d'incidents de sécurité et ont pu identifier et répondre plus rapidement aux problèmes qui étaient apparus. Sophos ACE s'appuie sur ces éléments pour transformer davantage le coût total de possession de la cybersécurité ainsi que la protection.

Prise en main

L'écosystème de cybersécurité Sophos est très flexible, et pour démarrer il suffit de déployer un des produits ou services de protection Sophos. Les entreprises bénéficient immédiatement de l'expertise combinée en matière d'intelligence sur les menaces de Sophos AI, SophosLabs et Sophos Security Operations. Vous pouvez ensuite étendre votre écosystème selon les besoins de votre entreprise. Les solutions de départ les plus populaires incluent :

Sophos Intercept X pour vos postes ou vos serveurs (avec la possibilité d'ajouter les fonctions EDR ou XDR)

Sophos Firewall – matériel, logiciel ou virtuel

Service Sophos Managed Threat Response (MTR)

Pour en savoir plus, contactez votre représentant Sophos, consultez notre site Web ou démarrez un essai gratuit.

Gartner Magic Quadrant for Enterprise Network Firewalls,
Analystes : Rajpreet Kaur | Adam Hils | Jeremy D'Hoinne | 9 novembre 2020

Gartner ne fait la promotion d'aucun fournisseur, produit ou service cité dans ses publications de recherche, et ne conseille aucunement aux utilisateurs de technologies de ne sélectionner que les fournisseurs ayant obtenu les meilleures notes ou toute autre distinction. Les publications de recherche de Gartner reflètent les opinions de l'organisme de recherche Gartner et ne devraient pas être interprétées comme un énoncé de faits. Gartner décline toute responsabilité, expresse ou implicite, liée à cette étude, y compris toute responsabilité quant à la valeur marchande ou à l'adéquation à un besoin particulier.

Apprenez-en plus sur les ransomwares et sur la façon dont Sophos peut vous aider à protéger votre entreprise.

Sophos fournit des solutions de cybersécurité de pointe aux entreprises de toutes tailles, les protégeant en temps réel contre les menaces avancées telles que les malwares, les ransomwares et le phishing. Grâce à des fonctionnalités Next-Gen éprouvées, les données de votre entreprise sont sécurisées efficacement par des produits alimentés par l'intelligence artificielle et le Machine Learning.

2021-04-26 (SB-NP)

SOPHOS