

LIVRE BLANC

Présentation de la Sécurité Synchronisée™

SOPHOS

Sécurité Synchronisée

La Sécurité Synchronisée™ est au cœur de Sophos Fusion, le système de cyberdéfense IA-natif de pointe de Sophos. C'est le tissu conjonctif qui transforme les informations sur les menaces provenant de tous les points de contrôle connectés (Sophos et tiers) en une réponse aux menaces coordonnée.

Dans leur rapport « Tech FutureSight: Protect the Global Attack Surface With an Autonomous Cyber Defense System »[1], Gartner a identifié que « les organisations ont besoin d'une superposition intelligente qui connecte les différents éléments de leur arsenal de cybersécurité afin de répondre de manière proactive et réactive aux risques et aux menaces, à la vitesse machine ». La Sécurité Synchronisée est un élément clé de la mise en œuvre de cette fonctionnalité dans Sophos Fusion.

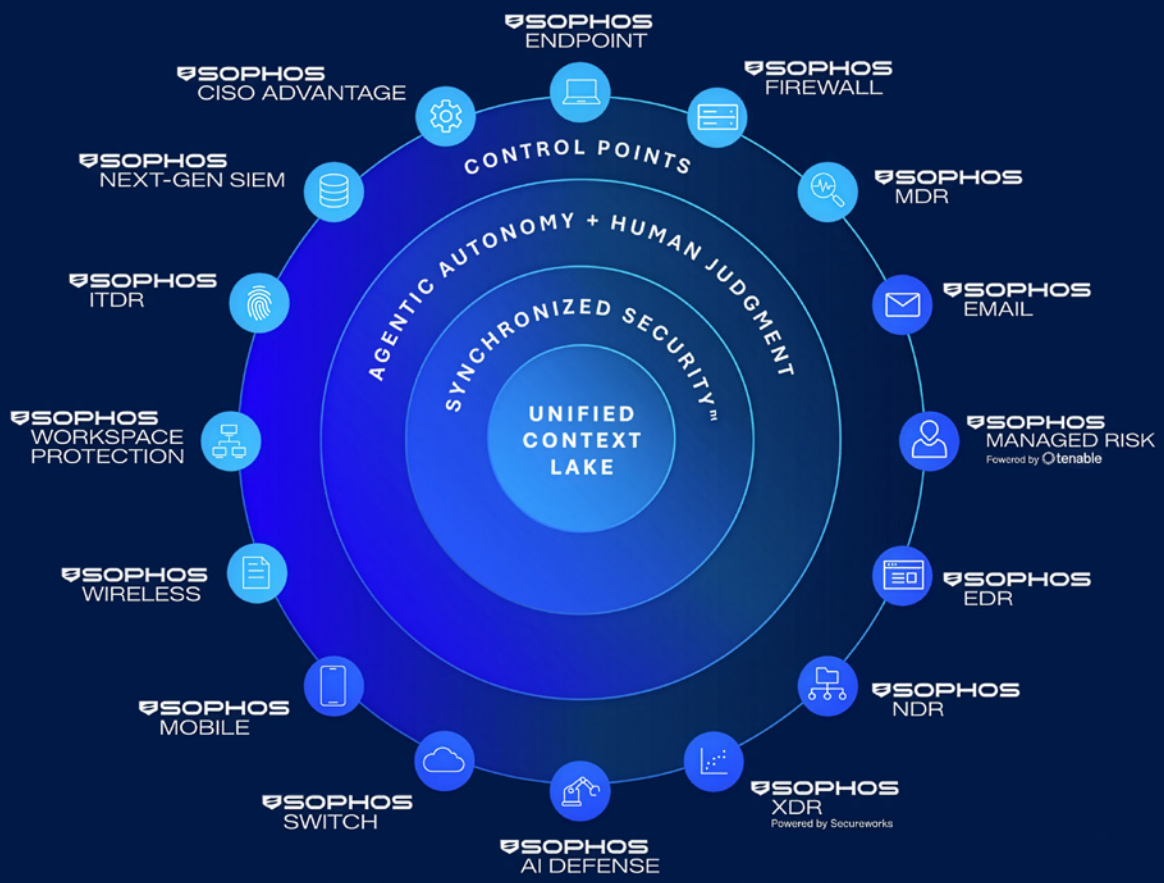
Le présent guide explique comment fonctionne la Sécurité Synchronisée, les avantages qu'elle procure et comment les organisations peuvent en tirer parti.

1 Tech FutureSight: Protect the Global Attack Surface With an Autonomous Cyber Defense System, Neil MacDonald, 12 décembre 2025. GARTNER est une marque déposée de Gartner, Inc. ou de ses sociétés affiliées.



Résumé rapide

- La Sécurité Synchronisée est un élément central du système de défense Sophos Fusion et est incluse automatiquement. Il n'est pas nécessaire d'acheter un module supplémentaire ni d'acquérir des licences pour des composants additionnels.
- Elle permet une réponse coordonnée aux menaces à travers les points de contrôle connectés. Pour l'activer, il faut que deux points de contrôle ou plus fonctionnent ensemble au sein de Sophos Fusion.
- La Sécurité Synchronisée fonctionne avec les points de contrôle à la fois Sophos et non Sophos. Les actions de réponse dans les environnements individuels des clients dépendent des contrôles connectés à Sophos Fusion, et du niveau d'action autonome que le client accorde à chaque point de contrôle.
- Sophos XDR est au cœur de la Sécurité Synchronisée. La solution corrèle les signaux provenant de l'ensemble de l'environnement du client en une seule chaîne d'attaque et permet des actions de réponse automatisées ou pilotées par des experts sur l'ensemble du système de défense.
- Les solutions Sophos peuvent également fonctionner ensemble sans Sophos XDR, ajoutant ainsi une profondeur supplémentaire à la Sécurité Synchronisée.
- La Sécurité Synchronisée s'appuie sur les fonctionnalités fondamentales éprouvées sur le terrain, que Sophos a lancées en 2015.



L'importance d'une réponse coordonnée

Les outils de sécurité sont traditionnellement conçus pour remplir efficacement une seule fonction. Un agent Endpoint sécurise l'appareil sur lequel il est exécuté (par exemple, un ordinateur de bureau, un ordinateur portable ou un serveur). Un pare-feu surveille ce qui traverse le réseau. Un service de protection des messageries contrôle ce qui atterrit dans les boîtes de réception. Chaque solution de protection excelle dans son domaine, mais reste aveugle à ce qui se passe en dehors.

Les attaquants l'ont compris il y a longtemps. Une intrusion moderne n'est pas un événement isolé en un seul lieu. Elle intègre dans sa conception les identités, la messagerie, les postes et le réseau, car c'est précisément dans l'espace qui les sépare que se situent les failles, et c'est là que les attaquants les exploitent.

Les conséquences sont bien connues de ceux qui ont déjà dirigé une équipe de cybersécurité. Les solutions individuelles restent limitées à leur propre domaine, identifiant des anomalies qui semblent en apparence isolées. Chacune de ces anomalies semble surmontable en soi. Personne n'a le temps ni le contexte nécessaire pour reconnaître que ces anomalies font partie d'une même attaque avant que les dégâts ne soient causés.

L'IA a accentué ces failles. Les attaques se déroulent désormais à la vitesse machine et à des volumes inédits. Cependant, la plupart des défenses fonctionnent toujours à vitesse humaine, avec un analyste jonglant entre les consoles pour corréler les alertes manuellement.

Ajouter un autre produit au parc ne comble pas cette faille. Les organisations devraient plutôt envisager de connecter les produits dans lesquels elles ont déjà investi. C'est précisément ce que fait la Sécurité Synchronisée dans Sophos Fusion.



La force de la Sécurité Synchronisée

La coordination transforme la rapidité, l'ampleur et la portée de la réponse aux menaces, changeant l'issue de l'attaque. Lorsque les postes, le réseau et d'autres contrôles agissent ensemble, le confinement s'opère en quelques secondes — et non après que quelqu'un s'en aperçoive et réagisse. Un poste compromis est isolé immédiatement avant qu'un adversaire ne puisse se déplacer latéralement, atteindre des données sensibles ou établir une persistance. De plus, comme la réponse est automatisée, elle fonctionne la nuit et le week-end alors que la présence humaine est souvent réduite.

La coordination comble également les failles sur lesquelles les attaquants comptent. Les points de contrôle tiers qui auparavant ne lançaient que des alertes commencent à contribuer activement à la défense. Les investissements de sécurité existants cessent de rester isolés et font partie intégrante de la réponse coordonnée.

L'impact opérationnel sur une équipe de sécurité est immédiat. Le confinement de routine se déroule sans intervention de l'analyste. Lorsqu'une investigation humaine est nécessaire, l'analyste dispose d'un contexte multicouche déjà assemblé, au lieu de le reconstituer à la main à travers plusieurs consoles.

Cette même coordination facilite la preuve de la protection. Le contexte multicouche est conservé, et une réponse coordonnée permet de disposer d'un historique cohérent des éléments identifiés et des mesures prises à cet égard. C'est le scénario de contrôle auquel s'attendent les auditeurs, les autorités de régulation et les assureurs. L'architecture qui améliore la protection améliore également la capacité du client à la démontrer.

La défense se renforce également à mesure qu'elle se développe. Chaque nouveau point de contrôle connecté à Sophos Fusion envoie un signal supplémentaire au Context Lake unifié et offre un nouveau point à partir duquel répondre, sans augmentation correspondante de l'effort opérationnel. Plus de couverture ne signifie pas plus de travail.

Pour les fournisseurs de services managés, la même coordination s'applique de manière cohérente à tous les environnements clients, y compris ceux qui combinent Sophos et des points de contrôle tiers. Le confinement automatisé réduit les tâches manuelles liées au triage et à la remédiation des incidents.

Fonctionnement

La Sécurité Synchronisée commence par la télémétrie. Chaque point de contrôle connecté transmet en temps réel les informations qu'il recueille au Context Lake unifié. Les solutions de protection Endpoint, pare-feu, messagerie, cloud, réseau, gestion d'identité et les outils de productivité alimentent tous le même lac. Les points de contrôle tiers l'alimentent en parallèle de ceux de Sophos. Aucun élément n'est mis en file d'attente en vue d'être agrégé, et il n'existe pas de base de données secondaire à faire concorder ultérieurement.

Sophos XDR interprète l'image partagée et fait le travail qu'un analyste ferait autrement à la main. La solution relie les événements connexes et les résout en une seule chaîne d'attaque, plutôt qu'en une série d'alertes distinctes. La corrélation est la partie qui compte, car un point de contrôle ne voit jamais qu'un fragment.

Les actions de réponse sont ensuite renvoyées aux points de contrôle. Sophos XDR fournit les moyens : automatisation SOAR, playbooks, gestion des dossiers, et un large ensemble d'actions de réponse. La plupart fonctionnent automatiquement sans intervention humaine. Lorsqu'une expertise humaine est requise, un analyste interne peut déclencher la même action manuellement via Sophos XDR, tout comme un analyste Sophos MDR.

L'intégration bidirectionnelle avec des points de contrôle tiers signifie que Sophos Fusion peut extraire et transmettre des données via cette intégration. Par exemple :

- Il peut récupérer la télémétrie d'un pare-feu tiers non Sophos et transmettre une adresse IP à bloquer par le pare-feu.
- L'intégration ServiceNow ouvre, met à jour et ferme les dossiers.
- La fonction de réponse active aux menaces dans Sophos Firewall utilise des réponses déclenchées par API en fonction des flux de menaces tiers afin d'exclure du réseau tout appareil compromis ou non autorisé.

Fait unique, les points de contrôle Sophos agissent également les uns sur les autres directement, sans aucune intervention de Sophos XDR. La fonction Security Heartbeat intégrée transmet l'état d'intégrité d'un appareil depuis Sophos Endpoint vers les autres points de contrôle Sophos : un état « vert » indique que l'appareil est en bon état, un état « jaune » qu'il est potentiellement compromis et un état « rouge » qu'il est compromis.

Les autres points de contrôle Sophos sont conçus pour agir sur l'état d'intégrité de l'appareil. Une fois les points de contrôle connectés au même compte Sophos Fusion, les réponses de base n'ont pas besoin d'une configuration supplémentaire. Les capacités qui exploitent l'état d'intégrité, comme une règle de pare-feu qui limite l'accès à Internet ou une politique Sophos Workspace Protection, sont configurées par le client avant qu'elles ne prennent effet.

Collecter

Corréler

Répondre

Sophos Fusion collecte les données télémétriques, Sophos XDR établit le contexte, et les actions de réponse automatisées renvoient les mesures correctives vers les points de contrôle.

Une capacité, plusieurs dimensions de coordination

La Sécurité Synchronisée a été lancée en 2015, une première mondiale à l'époque, et s'est développée depuis plus de dix ans. La profondeur de coordination entre les points de contrôle varie d'un environnement client à l'autre en fonction de la combinaison exacte de points de contrôle qu'ils ont en place.

La coordination est la plus poussée entre les points de contrôle Sophos, car ils ont été conçus dès le départ pour fonctionner ensemble. Les points de contrôle tiers s'intègrent via les intégrations dans Sophos Fusion, et les actions de réponse varient en fonction des fonctionnalités proposées par l'autre éditeur.

La profondeur de coordination dépend également du niveau de contrôle qu'un client confie à Sophos Fusion pour chaque point de contrôle. Ce choix appartient au client, et le fait qu'il existe constitue un atout plutôt qu'une lacune. Si l'on demande à la plupart des organisations si un poste infecté doit être déconnecté du réseau sans approbation préalable, la réponse est oui. Si l'on demande si un système doit modifier de lui-même une règle de pare-feu afin de réduire son exposition, la réponse varie.

Les pare-feu illustrent parfaitement ce dilemme. Bloquer un poste compromis repose avant tout sur un changement de règle de pare-feu. De nombreuses organisations se méfient des modifications automatisées de la configuration du pare-feu, et les processus de contrôle des changements existent pour de bonnes raisons.

Les clients peuvent écrire leurs propres automatisations et playbooks et les exécuter à côté de ceux fournis par Sophos. Un client qui utilise Sophos Endpoint décide lui-même ce qu'un poste compromis signifie pour son pare-feu Fortinet, en examinant comment ce pare-feu se comporte et comment il est configuré. Une fois écrits, ces automatisations s'exécutent dans Sophos Fusion comme toute autre réponse coordonnée.



La Sécurité Synchronisée en action

La coordination est plus facile à comprendre à l'aide d'exemples. Les cas d'usage ci-dessous montrent la même capacité fonctionnant à des profondeurs différentes, plutôt qu'une liste de fonctionnalités distinctes.

Coordination entre les produits Sophos

Lorsque Sophos Endpoint trouve une menace sur un poste ou un serveur, il définit l'état d'intégrité de Security Heartbeat de cet appareil sur « rouge ». Le nouvel état est automatiquement partagé via le Security Heartbeat avec les autres points de contrôle Sophos connectés. Plusieurs réponses suivent automatiquement :

- Sophos Endpoint tente de remédier à la menace, ce qui peut impliquer notamment de bloquer et d'annuler le chiffrement effectué par un ransomware, ou de mettre en place un niveau de contrôle plus élevé afin de contenir un attaquant actif.
- Sophos Firewall limite l'accès à Internet de l'appareil, coupant toute connexion à un serveur command-and-control et l'empêchant d'atteindre les appareils sains.
- Sophos Wireless, Sophos Switch et Sophos Workspace Protection limitent l'accès de l'appareil aux ressources sur le réseau, limitant davantage l'impact de la compromission.
- Les postes sains sont informés de l'état d'intégrité « rouge » et rejetteront les demandes de connexion réseau de l'appareil affecté.

Ce même mécanisme détecte les problèmes qui ne se manifestent jamais sous la forme d'une infection. Un poste ou un serveur envoyant de grands volumes de spam ou d'emails de phishing est défini sur un état d'intégrité « rouge ». Sophos Endpoint recherche alors les utilisateurs ou applications malveillants jusqu'alors non identifiés, et Sophos Email bloque les emails frauduleux avant qu'ils n'atteignent de boîtes de réception.

Un poste ou un serveur peut rester à l'état d'intégrité « rouge » pendant quelques secondes, voire plusieurs jours, selon les mesures de remédiation nécessaires. Une fois nettoyé, l'état d'intégrité de l'appareil repasse en « vert » et l'accès est rétabli automatiquement sur l'ensemble du système.

La valeur de la Sécurité Synchronisée apparaît plus clairement dans les moments où personne n'est là pour garder un œil sur le système. Un serveur compromis tard un vendredi soir est coupé en quelques secondes, au lieu de donner à un adversaire tout le week-end pour se déplacer sur le réseau.

SCÉNARIO

Sophos Endpoint détecte une menace et définit l'état d'intégrité du Security Heartbeat sur « rouge ». Le nouvel état est partagé automatiquement avec chaque point de contrôle Sophos connecté. Lorsque la menace sur le poste est supprimée, le même cycle est suivi pour rétablir l'accès.

SIGNAL

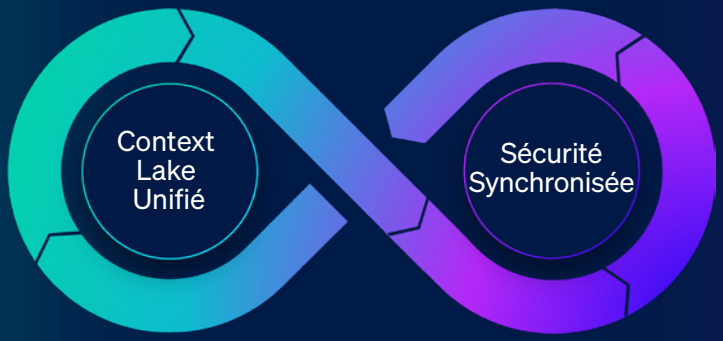
RÉPONSE COORDONNÉE

SOPHOS ENDPOINT

Détecte une menace

SOPHOS FUSION

AI-Native Cybersecurity Defense System



SOPHOS FIREWALL

Supprime la connectivité réseau et restreint l'accès au réseau.

SOPHOS WIRELESS

SOPHOS SWITCH

SOPHOS WORKSPACE PROTECTION

Restreint l'accès de l'appareil aux ressources du réseau.

SOPHOS ENDPOINT

Les postes sains rejettent la communication réseau.

Sophos Endpoint avec un pare-feu tiers

La coordination ne se limite pas aux points de contrôle Sophos. Un client utilisant Sophos Endpoint avec un pare-feu Fortinet peut faire en sorte qu'un appareil compromis déclenche une réponse au niveau du pare-feu Fortinet. Le client définit la nature de cette réponse et son étendue, ce qui permet de maintenir l'automatisation dans les limites de son propre processus de gestion des changements. Les capacités d'automatisation et de playbook (SOAR) de Sophos XDR permettent d'y parvenir, grâce à l'intégration de Fortinet dans Sophos Fusion.



Technologie et télémétrie Microsoft

Quasiment toutes les entreprises utilisent la technologie Microsoft, et l'identité est le principal vecteur d'attaque des ransomwares. Un jeton de session volé ou un compte compromis donne à un adversaire un moyen légitime d'accéder au système, et aucune mesure de confinement sur le poste ne sera efficace si le compte lui-même reste compromis. La réponse doit s'étendre à l'environnement Microsoft pour finaliser la remédiation.

Le verrouillage du compte est l'exemple le plus clair : Sophos Fusion peut verrouiller un compte Microsoft compromis pour empêcher l'adversaire d'accéder au compte, puis le déverrouiller dès que le compte peut à nouveau être utilisé en toute sécurité. Le compte est considéré comme un point de contrôle comme un autre : il s'agit d'un élément que le système peut détecter et sur lequel il peut agir, et non d'un élément qu'un administrateur traite séparément a posteriori.

L'intégration est bidirectionnelle. La télémétrie provenant d'une gamme de sources Microsoft alimente le même Context Lake unifié que les points de contrôle Sophos, Microsoft Entra ID et Microsoft Graph Security parmi eux. Ainsi, un signal Microsoft peut générer une réponse à un point de contrôle Sophos tout aussi facilement que l'inverse. Une connexion suspecte signalée par Microsoft peut isoler un poste protégé par Sophos, sans qu'aucune des deux parties ne soit configurée pour surveiller l'autre.

Le périmètre réseau, filaire et sans fil

Les switchs et les points d'accès sont rarement considérés comme faisant partie d'un système de cyberdéfense. Ce sont des infrastructures, acquises pour acheminer le trafic et permettre aux utilisateurs de rester connectés, et la plupart des organisations les traitent en conséquence. Pourtant, ils se situent au point où chaque appareil rencontre le réseau, ce qui en fait l'un des premiers endroits où un appareil compromis ou non autorisé peut être bloqué.

Dans Sophos Fusion, les Sophos Switchs et les points d'accès Sophos Wireless fonctionnent comme des points de contrôle : ils contribuent en partageant ce qu'ils observent au niveau des appareils connectés, et ils peuvent agir en fonction des informations recueillies par l'ensemble du système. Les administrateurs peuvent identifier les nouveaux appareils ou les appareils non autorisés, les clients connectés à un SSID inattendu ou un appareil branché sur le mauvais port du switch.

La réponse active aux menaces, une fonctionnalité de la Sécurité Synchronisée dans Sophos Firewall, transforme ce contexte en action. Grâce à la télémétrie du Context Lake unifié, un appareil peut être bloqué au niveau de la couche d'accès filaire ou sans fil avant que l'attaque ne se déplace plus loin dans le réseau. Les clients choisissent d'activer ou non la réponse active aux menaces, ils décident eux-mêmes s'ils souhaitent autoriser le blocage automatisé au niveau de la couche d'accès.

Les appareils réseau tiers suivent le même schéma que celui illustré ci-dessus avec l'exemple du pare-feu tiers.



Sophos AI Defense découvre l'utilisation de Shadow AI

La coordination ne se limite pas aux malwares et aux intrusions. Sophos AI Defense est un point de contrôle dans Sophos Fusion qui régit l'utilisation de l'IA au sein d'une entreprise. Il interprète la télémétrie de l'activité de l'IA à partir d'une variété de produits Sophos dans le Context Lake unifié, aux côtés de tous les autres signaux, visibles par Sophos EDR, Sophos XDR et Sophos MDR. Sophos AI Defense est conçu pour mettre en évidence les détails précis de l'utilisation de l'IA, et une fois ces informations intégrées dans le Context Lake unifié, elles sont traitées par la même fonctionnalité de Sécurité Synchronisée que toutes les autres données.

L'exemple du Shadow AI montre pourquoi cela est nécessaire. Un employé commence à utiliser un outil d'IA que personne ne connaît, en y collant du code source et des dossiers clients. Le navigateur voit les données collées, le poste voit l'application et le pare-feu voit le trafic vers un service d'IA provenant d'un appareil qui n'est peut-être pas du tout gouverné. Aucun point de contrôle ne permet d'avoir une vue d'ensemble, si bien que l'outil passe inaperçu.

Sophos AI Defense rassemble ces signaux et les évalue dans leur contexte, donnant à un analyste de sécurité les preuves dont il a besoin pour comprendre ce qui s'est passé. Il combine des données télémétriques issues de l'identité, des autorisations, du comportement, de l'exposition des données et de l'emplacement, tant au niveau de l'utilisateur que du modèle d'IA, ce qui permet de distinguer une utilisation acceptable d'une activité non gouvernée qui comporte des privilèges excessifs ou allant à l'encontre de la politique de sécurité.

L'application des mesures intervient ensuite aux points de contrôle :

- Sophos Workspace Protection contrôle le navigateur, y compris le copier-coller, les téléversements, les téléchargements et les captures d'écran.
- Sophos Endpoint restreint l'accès aux applications et aux sites Web d'IA sur l'ensemble des groupes d'utilisateurs et des types d'appareils.
- Sophos Firewall contrôle le trafic des services d'IA au niveau de la couche réseau, y compris les appareils non gouvernés et l'activité non liée au navigateur.
- Les produits Sophos peuvent inspecter les prompts, les téléversements et les interactions de l'IA en temps réel, en conservant le code source, les données des clients et les données financières à l'intérieur de l'entreprise.
- Un administrateur peut bloquer un outil d'IA spécifique dans le parc IT depuis Sophos Fusion.

Les politiques de sécurité ne sont pas une fin en soi. Une intrusion ou un comportement d'agent non autorisé apparaît dans les mêmes flux de travail de Sophos EDR, Sophos XDR et Sophos MDR que toute autre détection, traitée avec l'automatisation et les playbooks déjà utilisés pour les menaces liées aux identités, aux postes et au réseau. La portée de la coordination dépend des points de contrôle connectés à Sophos Fusion.

82 %

des organisations ont découvert des outils ou des flux de travail d'IA inconnus dans leur environnement.[2]

2 Cloud Security Alliance, The Shadow AI Agent Problem in Enterprise Environments, 2025

Une coordination qui va au-delà de la réponse aux menaces

Entre les points de contrôle Sophos, la coordination va plus loin que le partage d'un verdict sur une menace. Un point de contrôle peut poser une question directe à un autre et agir en fonction de la réponse. Un poste ou un serveur protégé par Sophos Endpoint dispose déjà de la plupart des informations que Sophos Firewall ne peut pas vous fournir concernant le trafic réseau. Trois échanges montrent ce que cela permet : identifier l'application derrière le trafic sur un port, identifier l'utilisateur derrière une session et décider si un appareil est apte à recevoir un accès.

Contrôle synchronisé des applications

Prenons une connexion non classifiée sur un port inhabituel. Un pare-feu qui l'inspecte de manière isolée ne voit qu'un flux de paquets, et guère plus. Sophos Firewall peut demander à Sophos Endpoint quelle application envoie et reçoit des données sur ce port et obtenir une réponse indiquant quelle application est en cause. Les clients peuvent alors autoriser ou bloquer l'application en fonction de cette information. Au fil du temps, cela permet également d'avoir une image précise de ce qui s'exécute sur le réseau, qui est généralement plus varié que ce à quoi on pourrait s'attendre.

Des identités, pas des adresses IP

L'identité de l'utilisateur fonctionne de la même manière. Sophos Endpoint transmet les informations utilisateur authentifiées à Sophos Firewall, ce qui permet de définir des règles en fonction des personnes et de leur identité, plutôt qu'en fonction des adresses utilisateur ou IP, qui sont susceptibles de changer. Cela évite aux administrateurs de mapper manuellement ces informations, qui ont tendance à rapidement devenir obsolètes.

Seuls les appareils sains se connectent

Les décisions d'accès en bénéficient également. Un VPN traditionnel n'a aucun moyen de savoir si un appareil est sain ou non, et autorise l'accès au terminal sur la seule base de ses identifiants. Cependant, Sophos Workspace Protection vérifie l'état d'intégrité de l'appareil avec Sophos Endpoint avant d'accorder quoi que ce soit. Ainsi, un poste compromis n'atteint jamais les applications ou les données du réseau.

De tels échanges ne sont pas fixes. Chacun d'entre eux existe car Sophos l'a conçu, et Sophos n'a cessé d'étendre les capacités au fil du temps. Ce qui est partagé entre les points de contrôle Sophos aujourd'hui est considérablement plus riche que ce qui était partagé entre eux il y a dix ans.

Rien de tout cela ne commence par une réponse aux menaces, mais elle en reste rarement séparée. Une application dont personne ne peut expliquer l'origine, ou un utilisateur connecté là où il n'a rien à faire, relève d'un détail opérationnel jusqu'au moment où ce n'est plus le cas. Une visibilité qui facilite la gestion d'un réseau permet de détecter plus facilement une menace émergente.

Une réponse coordonnée dans un environnement hybride

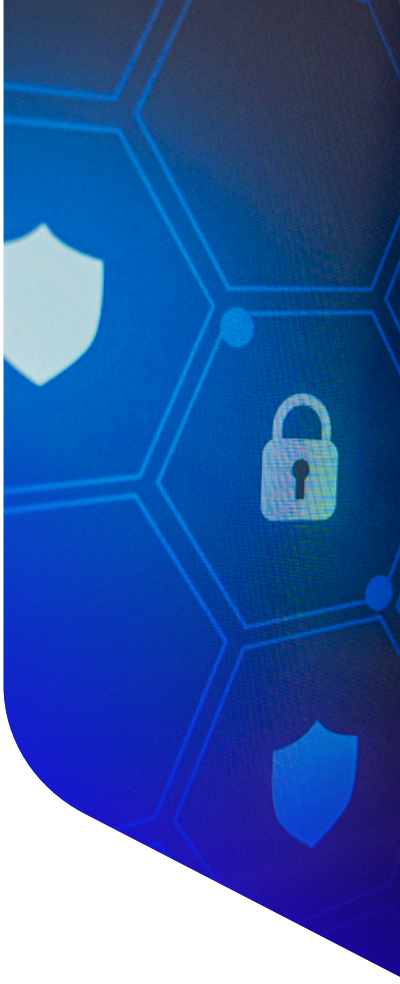
Cet exemple concret issu de Sophos MDR montre la Sécurité Synchronisée en action. L'organisation impactée était un client Sophos MDR exécutant Sophos Endpoint et Sophos Email, aux côtés de Microsoft Entra ID, Microsoft Graph Security et d'un pare-feu Fortinet. Ils étaient également doté d'un Sophos Firewall sur un réseau séparé. Chacun de ces points de contrôle alimentait le même Context Lake unifié.

- L'attaquant a commencé par lancer un leurre généré par IA, en utilisant une page de phishing hébergée sur un site légitime. L'utilisateur a cliqué, puis saisi son mot de passe.
- Le kit a volé le jeton de session actif plutôt que l'identifiant. Ce faisant, l'attaquant a réussi à contourner l'authentification multifacteur, rendant ainsi la réinitialisation du mot de passe inefficace.
- L'attaquant s'est connecté à partir d'une infrastructure connue pour être utilisée par des attaquants et a créé une règle de boîte de réception « silencieuse » masquant tous les emails provenant d'un fournisseur spécifique, ce qui constitue la mise en place d'une fraude par virement bancaire.
- Quatre points de contrôle ont détecté une activité suspecte : Sophos Endpoint, deux solutions Microsoft et le pare-feu Fortinet. Aucun signal n'était assez fort pour déclencher une réponse.
- Une détection Sophos spécialement conçue a été déclenchée et les signaux individuels ont été regroupés en une seule chaîne d'attaque.
- La connexion a été bloquée, les sessions ont été révoquées et le poste a été isolé. Les adresses IP malveillantes ont été bloquées par Sophos Firewall, grâce aux données de télémétrie fournies par le pare-feu Fortinet.

Un humain a ensuite pris le relais. Un analyste a confirmé que la règle de la boîte de réception désignait un fournisseur spécifique, ce qui l'identifiait comme une préparation à la fraude par virement bancaire.



Comment activer la Sécurité Synchronisée



La Sécurité Synchronisée n'est pas un produit, une référence produit (SKU) ni un module complémentaire, et il n'est pas nécessaire d'obtenir une licence supplémentaire. Les clients l'obtiennent automatiquement lorsque deux points de contrôle ou plus fonctionnent ensemble dans Sophos Fusion, que les points de contrôle soient Sophos ou non.

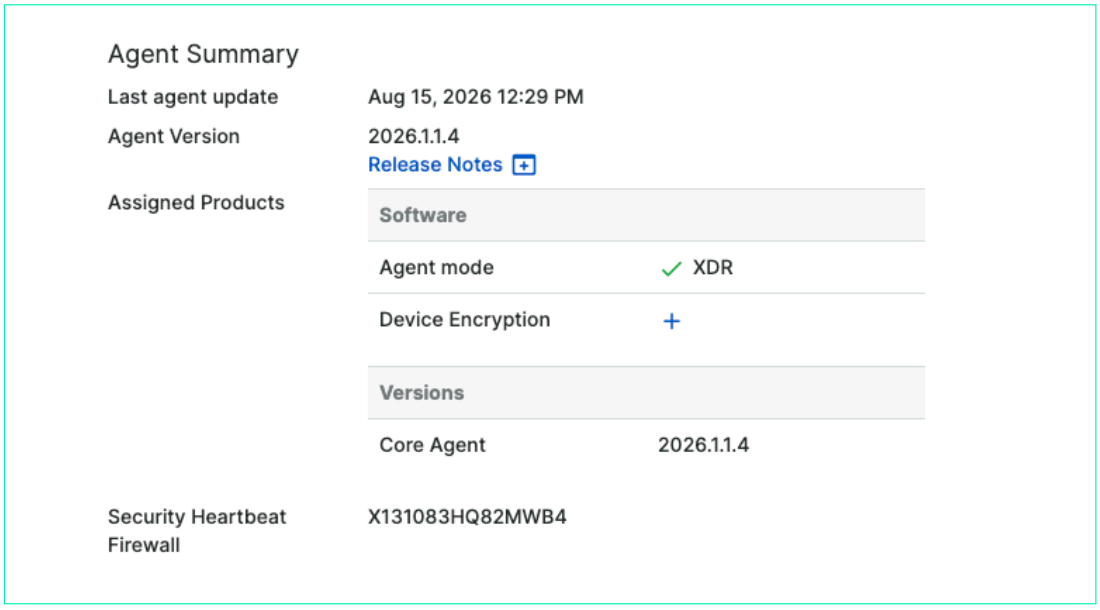
Un point de départ courant consiste à gérer Sophos Endpoint et Sophos Firewall depuis le même compte Sophos Fusion. La coordination entre ces solutions s'active dès qu'elles sont toutes deux connectés au compte, sans qu'aucune configuration supplémentaire ne soit nécessaire. Les cas d'usage qui s'appuient sur l'état d'intégrité, comme l'utilisation de l'état d'intégrité dans le cadre des règles de pare-feu ou des politiques Sophos Workspace Protection, sont mis en place par le client.

La coordination avec les points de contrôle tiers commence par l'intégration de ces derniers dans Sophos Fusion, qui prend en charge les intégrations natives de Sophos
ainsi que plus de 500 intégrations tierces. Cependant, le niveau de réponses automatisées disponibles varie d'un point de contrôle à l'autre. La réponse active aux menaces dans les points de contrôle Sophos en est un exemple : elle doit être activée par le client, car elle n'est pas activée par défaut.

Sophos fournit des automatisations et des playbooks qui s'exécutent automatiquement via la Sécurité Synchronisée, couvrant un large éventail de cas d'usage. Les clients peuvent créer leurs propres automatisations lorsque celles proposées par défaut ne sont pas adaptées à leur environnement, comme décrit ci-dessus.

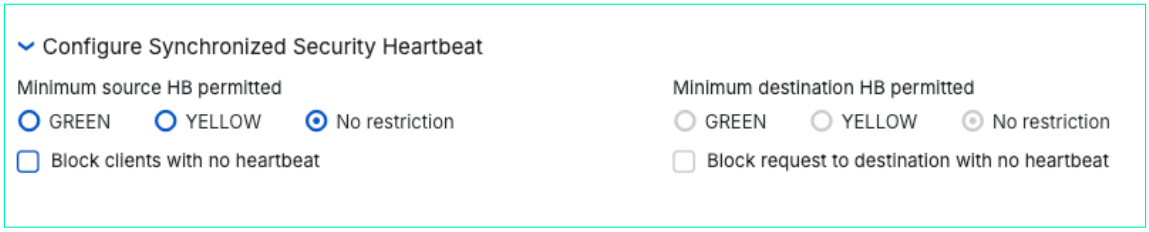
Coordination de Sophos Endpoint avec Sophos Firewall

Pour confirmer la coordination de Sophos Endpoint avec un pare-feu, ouvrez le « Résumé de l'ordinateur » dans Sophos Fusion. Il indique le numéro de série du Sophos Firewall recevant le Security Heartbeat de ce terminal.



Politiques Sophos Firewall avec la Sécurité Synchronisée

Une règle de pare-feu peut, le cas échéant, exiger que l'état d'intégrité d'un appareil soit « vert » avant que celui-ci ne soit autorisé à accéder à Internet. Les appareils non protégés (c'est-à-dire ceux qui n'utilisent pas Sophos Endpoint) ne pourraient alors plus se connecter, tout comme tout appareil dont l'état d'intégrité serait douteux.



Réunir tous les éléments

Le problème n'a jamais été le manque d'outils de sécurité. Il réside plutôt dans le fait que les outils dont dispose déjà une organisation ont tendance à fonctionner de manière isolée, et que les attaquants ont mis au point des méthodes pour exploiter les failles qui existent entre eux. La Sécurité Synchronisée permet à vos outils de sécurité de fonctionner comme une défense unifiée et coordonnée.

Si vous exécutez deux points de contrôle ou plus dans Sophos Fusion, la Sécurité Synchronisée travaille déjà en votre nom. Connectez plus de points de contrôle, et sa portée s'étend davantage. Les outils non Sophos dans lesquels vous avez déjà investi sont intégrés dans la réponse, plutôt que relégués à un simple rôle de reporting.

Le degré d'automatisation reste votre décision. Une coordination qui ignore vos processus de contrôle des modifications n'aurait aucun intérêt. C'est donc vous qui déterminez le niveau d'automatisation, point de contrôle par point de contrôle.

C'est l'intérêt pratique du système de cyberdéfense Sophos. Ce n'est pas une liste plus longue de produits, mais ceux que vous utilisez déjà qui fonctionnent de concert à la vitesse machine, plus rapidement qu'une attaque accélérée par l'IA ne peut passer d'un produit à l'autre.

Pour en savoir plus, consultez www.sophos.fr/synchronizedsecurity

Sophos France
Tél. : 01 34 34 80 00
Email : info@sophos.fr

© Copyright 2026. Sophos Ltd. Tous droits réservés.
Immatriculée en Angleterre et au Pays de Galles N° 2096520, The Pentagon, Abingdon Science Park, Abingdon, OX14 3YP, Royaume-Uni.
Sophos est la marque déposée de Sophos Ltd. Tous les autres noms de produits et d'entreprises mentionnés dans ce document sont des marques ou des marques déposées de leurs propriétaires respectifs.