

A man and a woman are looking at a computer screen. The man is in the foreground, looking intently at the screen. The woman is in the background, also looking at the screen. The screen displays lines of code, likely in a programming language like Python or JavaScript. The background is dark, and the lighting is focused on the screen and the people's faces.

LIVRE BLANC

Les systèmes de cyberdéfense à la loupe

Comment le nouveau modèle de cyberdéfense renforce la résilience à l'ère de l'IA agentique.

Résumé

Sur le papier, la couverture de cybersécurité de la plupart des organisations semble solide : elles se sont dotées de dizaines de produits de sécurité au fil des ans.

Pourtant, selon Gartner : « En moyenne, les organisations disposent de 45 outils de sécurité qui fonctionnent souvent en silos, créant de la complexité, des angles morts et des expositions non identifiées que les adversaires tenteront d'exploiter. »¹ Le problème n'est donc pas lié à une pénurie d'outils, mais au manque de connectivité entre eux.

Les attaquants exploitent déjà les failles entre les outils, se déplaçant entre la messagerie, la gestion des identités, les terminaux et le réseau en quelques minutes. L'IA augmente la vitesse, l'échelle et la portée des cybermenaces à un rythme sans précédent, permettant l'exécution à grande échelle d'attaques sophistiquées et multicouches.

Auditeurs, autorités de régulation et les assureurs cyber attendent désormais un ensemble complet de preuves, qui sont difficiles à produire avec des outils cyber fragmentés. La plupart des organisations peinent encore à répondre à ces trois questions fondamentales : sommes-nous protégés, où se situe notre plus grand risque et nos investissements sont-ils efficaces ?

Un nouveau modèle de cyberdéfense prend forme pour renforcer la sécurité à l'ère de l'IA. La plateforme de sécurité évolue vers le système de cyberdéfense. Voici ses traits caractéristiques :

- **Une vue unique en temps réel de l'environnement** alimentée par chaque point de contrôle de n'importe quel fournisseur.
- **Les réponses se coordonnent automatiquement** entre les points de contrôle : messagerie, identité, endpoint, réseau, et plus encore.
- **L'IA agentique répond à la vitesse et au volume des attaques modernes** tandis que les experts humains définissent les limites et assument la responsabilité des résultats.
- **Apprentissage continu** avec chaque nouvelle information, chaque menace stoppée sur l'ensemble de la base d'utilisateurs, renforçant les défenses partout, automatiquement.
- **La défense ne se pense plus à l'échelle de produits isolés, mais d'une architecture capable de les connecter**, à la fois sur le plan technologique et grâce à un réseau d'experts humains.

1. Gartner, « Tech FutureSight : Protect the Global Attack Surface With an Autonomous Cyber Defense System », Neil MacDonald, 12 décembre 2025.

Les menaces de l'ère de l'IA agentique sont déjà une réalité

Fin 2025, des chercheurs ont documenté la première campagne de cyberespionnage connue pilotée principalement par l'IA plutôt que par des opérateurs humains. L'IA a mené environ 80 à 90 % de l'opération par elle-même, à une vitesse et une échelle qu'aucune équipe humaine n'aurait pu égaler.

Source : Anthropic, novembre 2025

Un système de cyberdéfense, c'est...

Une architecture de sécurité unifiée où chaque point de contrôle partage une vue en temps réel, répond de manière coordonnée, apprend en continu et fonctionne à la vitesse machine, sous la responsabilité humaine.

Vos défis de cybersécurité à l'ère de l'IA

Des années de décisions d'achat raisonnées, prises au cas par cas en fonction des menaces, ont conduit à un environnement si complexe que cette complexité est devenue un risque en soi. Désormais confrontée à des attaquants opérants à la vitesse machine, cette pile de produits non coordonnés ne parvient pas à suivre le rythme. Comment en sommes-nous arrivés là ?

Les lacunes de l'approche par plateforme

Presque tous les grands fournisseurs de cybersécurité prétendent que leur plateforme peut faire tout ce dont vous avez besoin. Ils s'adressent aux acheteurs qui traitent chaque menace séparément, avec des solutions ponctuelles censées former une plateforme unifiée.

La philosophie de plateforme consistant à construire un système unifié partait d'une bonne intuition, mais ce qu'ils vendent s'apparente souvent à un patchwork d'outils construits à la hâte ou acquis, destinés à répondre aux effets de mode ou à faire grimper le cours d'une action. Les promesses ne sont pas tenues :

- **On promet aux clients une «interface unique»**, mais lorsqu'ils sont testés en situation réelle, les intervenants doivent toujours passer d'une console à l'autre.
- **On promet des données partagées**, mais les produits de la plateforme ne peuvent pas analyser ces données ensemble pour détecter une attaque touchant les identités, le cloud et les postes.
- **On promet aux clients une intégration**, mais chaque produit conserve son propre modèle de données et les actions de réponse restent cloisonnées entre les domaines.

Tout le travail lié à la gestion de plateforme — configuration, personnalisation, création d'un flux de travail utilisant toutes les parties ensemble — est laissé au client.

Selon Gartner®,
«Le simple ajout d'outils supplémentaires à la pile ne fournira pas la structure de cyberdéfense intelligente dont les organisations ont besoin pour atténuer les attaques orchestrées par l'IA comme celle qu'Anthropic a récemment identifiée.»

Neil MacDonald
Gartner | VP, Distinguished Analyst and Gartner Fellow Emeritus

Gartner, 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.

Les attaques inter-domaines déjouent les défenses fragmentées

Les analyses et les modèles de données fragmentés dans les produits de plateforme sont du pain béni pour les attaquants. Le scénario d'attaque suivant nous montre pourquoi :

- **Étape 1 :** Un email convaincant atterrit dans une boîte de réception.
- **Étape 2 :** Le destinataire saisit son mot de passe sur une fausse page de connexion.
- **Étape 3 :** L'attaquant se connecte depuis un emplacement inconnu.
- **Étape 4 :** L'attaquant ajoute discrètement une règle de boîte de réception pour surveiller le trafic.
- **Étape 5 :** L'attaquant utilise son accès pour atteindre un partage de fichiers et exfiltrer des données.

Cinq étapes, chacune aboutissant sur un domaine différent.

- **La sécurité des messageries** voit l'email.
- **La solution de gestion des identités** voit la connexion inhabituelle.
- **La protection Endpoint** détecte une petite anomalie.
- **Le pare-feu** enregistre la connexion sortante.

Chaque produit se concentre sur sa partie du signal et fait techniquement son travail. Pourtant **aucun d'entre eux n'a accès à une vue d'ensemble**, car aucun ne transmet ce qu'il sait aux autres pendant que l'attaque est encore en cours. Pris ensemble, ces parties de signal ressemblent davantage à du bruit qu'à un scénario d'attaque cohérent. Lorsque la chaîne devient évidente, il est déjà trop tard.

Ce type de mouvements latéraux est courant dans les attaques modernes, et il est aussi fréquemment ignoré. Le [rapport Sophos L'état des ransomwares 2026](#) a montré que 55 % des cybercriminels ont réussi à chiffrer des données même lorsque le pare-feu avait détecté l'attaque.

Attaques à la vitesse machine, réponse à la vitesse humaine

Prenez maintenant cette attaque inter-domaines et compressez la chronologie de l'attaque de quelques jours à quelques minutes. C'est ce que l'IA a rendu possible. Désormais, une défense qui attend qu'une personne remarque une alerte dans un produit et la recoupe avec un autre produit est une défense dépassée. Le problème ne vient pas de la lenteur des équipes de défense, mais de la lenteur des réponses, outil par outil. Les flux de travail hautement manuels ne peuvent pas suivre le rythme d'une attaque automatisée. Le temps qu'un opérateur formule une réponse, l'attaquant est déjà passé à l'étape suivante.



L'expertise est rare. Le bruit ne l'est pas.

Faute de personnel disponible, renforcer les équipes pour faire face au problème n'est pas une option. La pénurie de compétences en cybersécurité est bien réelle et ne montre aucun signe d'amélioration. Dans l'étude 2025 d'ISC2 sur la main-d'œuvre, 95 % des équipes de sécurité ont signalé au moins une lacune en matière de compétences, et 59 % l'ont qualifiée de critique ou significative, contre 44 % l'année précédente.

Or, parallèlement, la charge de travail ne cesse d'augmenter. Une petite équipe peut vite se retrouver face à un nombre trop important de produits, d'alertes et de tableaux de bord pour assurer une surveillance réaliste. La majorité de ces alertes ne sont que du bruit, mais quelqu'un doit parvenir à déceler tout signal qui s'y cacherait.

L'IA était censée alléger cette pression, mais dans certains environnements, elle a produit l'effet inverse.

Ajouter l'IA comme un énième produit crée les mêmes problèmes : plus de bruit et d'alertes, car elle n'a pas été conçue pour interagir nativement avec le reste des produits de la plateforme. Ainsi, l'équipe de cybersécurité ne doit pas seulement passer au crible les faux positifs, elle doit aussi faire face aux hallucinations de l'IA.



Le seuil de pauvreté Cyber est réel

Le seuil de pauvreté Cyber désigne la limite en dessous de laquelle une organisation ne peut pas être sécurisée efficacement. Il n'est pas défini par la taille, le budget d'une organisation, ou par la présence ou non d'un RSSI. En fait, de nombreuses organisations bien financées se situent en dessous de ce seuil.

Le seuil de pauvreté Cyber est un seuil de capacité stratégique.

Votre organisation se contente-t-elle de posséder une technologie de sécurité, ou est-elle capable de l'exploiter en tant que système ? Les grandes équipes peuvent dépenser des sommes considérables dans des outils que personne ne sait utiliser, tandis qu'une entreprise manufacturière de 200 personnes, bien organisée, peut mettre en place un système de défense plus performant que celui d'organisations bien plus importantes. De nombreuses organisations se situent sans le savoir en dessous du seuil de pauvreté parce qu'elles supposent que la capacité à gérer la sécurité en tant que système était déjà en place en interne.

Pour ces organisations, la plus grande faille ne provient pas d'un outil absent. Elle provient de l'absence d'une stratégie claire et de l'orchestration nécessaire pour faire fonctionner les contrôles existants ensemble contre les menaces accélérées par l'IA. Ces organisations continuent d'investir, mais peinent toujours à répondre à trois questions fondamentales :

- Sommes-nous protégés ?
- Où se situent nos plus grands risques ?
- Nos investissements fonctionnent-ils réellement ?



Les autorités de régulation exigent davantage de preuves de la résilience.

Les autorités de régulation et les assureurs cyber ne se soucient pas de savoir si vous possédez les bons produits. Ce qu'ils souhaitent, ce que vous leur démontriez les choses suivantes :

- Un contrôle coordonné entre les domaines.
- Des preuves conservées et auditables.
- Des divulgations cohérentes et opportunes.
- Une résilience testée en conditions réelles.

Ces nouvelles réglementations représentent de lourdes charges pour les organisations qui possèdent encore un parc de sécurité réparti sur des dizaines de produits, chacun comportant son propre modèle de données et sa propre période de conservation des données. Dans ces conditions, fournir les preuves demandées par un auditeur ou un assureur peut devenir un travail à temps plein : exporter des journaux depuis des systèmes distincts, les assembler manuellement et espérer que le résultat raconte toujours une histoire cohérente. Un contrôle qui ne peut être démontré est, à des fins de conformité, un contrôle qui ne compte pas.

Le fil conducteur

Aucun de ces problèmes n'est résolu en ajoutant un produit ou un bouton supplémentaire à une console. Toutes ces difficultés partagent une cause première unique : des défenses qui fonctionnent en vase clos ne feront jamais le poids face à des menaces qui agissent de manière coordonnée. Combler cet écart nécessite une approche différente, et non un énième produit.



Systèmes de cyberdéfense : une approche moderne de la sécurité

Si le problème est la fragmentation, la réponse n'est pas la consolidation en soi. Acheter un produit qui essaie de tout faire et échoue n'est pas mieux que d'avoir plusieurs bons produits qui ne se coordonnent pas bien.

Au lieu de cela, les organisations devraient rechercher un système de cyberdéfense : un ensemble de produits et services de sécurité conçus pour fonctionner comme un système unifié. Chaque point de contrôle doit contribuer à une compréhension partagée de l'environnement et apporter une réponse en tant que partie d'un tout coordonné. Le système doit être parfaitement connecté, synchronisé, automatisé, intelligent et adaptatif. Cinq principes décrivent à quoi cela ressemble en pratique.

1 Des points de contrôle synchronisés et autonomes

Un système de cyberdéfense commence par des points de contrôle. Il s'agit des technologies et services où la télémétrie de sécurité est observée et où les règles de sécurité sont appliquées. Les points de contrôle peuvent à la fois voir et agir sur ce qui leur arrive. Endpoint, pare-feu, messagerie, identité, outils de productivité, et plus encore sont tous des points de contrôle.

2 Une vue partagée, en temps réel

Un système de défense diffère d'une plateforme par le fait qu'il possède une compréhension partagée unique de ce qui se passe dans l'environnement. Chaque point de contrôle transmet ce qu'il voit dans une couche de données commune en temps réel, sans copie ni rapprochement différés. Cela donne à l'ensemble du système une vue unique et partagée des événements en temps réel. Aucun angle mort, aucune lacune dans la réponse.

3 Une réponse coordonnée à travers chaque couche

Une réponse coordonnée commence par une détection dans une couche qui peut automatiquement déclencher une action dans les autres sans qu'un analyste ait à relayer le signal d'une console à l'autre.

Ainsi, une connexion suspecte peut entraîner une surveillance accrue au niveau des couches endpoint et messagerie. Un fichier malveillant sur un appareil peut amener le pare-feu ou le réseau à bloquer la connexion qu'il tente d'établir. Le système apporte une réponse unifiée, car il perçoit déjà une attaque comme un tout. Et lorsqu'une attaque se propage rapidement, ce type de coordination est essentiel.



4 Une IA agentique avec responsabilité humaine

La rapidité est le facteur décisif. Des attaques qui se jouent en quelques minutes ne peuvent pas être stoppées par des défenses dépendantes d'une intervention humaine. C'est pourquoi l'IA doit être au centre du système, et non en périphérie.

Dans un système de cyberdéfense, l'IA est l'architecture : elle est intégrée, pas ajoutée. L'IA corrèle les signaux à travers chaque couche, repère la forme d'une attaque dès son apparition et pilote la détection, l'investigation et la réponse à la vitesse machine. Ce système AI-Native se distingue des technologies d'IA greffées après coup à un seul produit, qui ne peuvent voir que les données spécifiques à ce produit.

L'IA intégrée à un système de cyberdéfense peut raisonner sur tout ce que le système voit. Cependant, une réponse à la vitesse machine sans responsabilité humaine est un handicap, et non un avantage. Les systèmes de cyberdéfense ne suppriment pas l'intervention humaine dans la sécurité. Au contraire, ils les orientent là où l'expertise humaine est la plus importante : définir les limites, gérer les décisions inédites ou à haut risque, examiner les incidents et assumer l'entière responsabilité des résultats.

L'IA garantit la rapidité et la scalabilité. Le triage de routine et les actions rapides à haut niveau de confiance.

Les experts humains définissent la limite de confiance : ce que l'IA peut décider seule et quand des opérateurs humains doivent intervenir. Ils interviennent lorsque le contexte est inconnu ou que les enjeux sont élevés.

À mesure que le système gagne en confiance, cette limite peut s'étendre. Cela dit, la responsabilité incombe toujours aux experts humains.

L'IA garantit la rapidité et la scalabilité.

Les experts humains définissent la limite de confiance.

5 Une intelligence cumulative

Les systèmes de défense apprennent. Une menace rencontrée n'importe où devient une connaissance partout. L'endpoint voit ce que le pare-feu a vu. La passerelle de messagerie indique à la couche d'identité ce qu'elle a intercepté. Chaque outil apprend aux côtés des autres et s'appuie sur ce qui a été fait auparavant. Tout cela se produit sans aucune configuration manuelle. L'intelligence du système de défense s'enrichit à mesure que le nombre d'utilisateurs augmente et que davantage de modèles sont observés, lui permettant d'évoluer aussi vite que les attaques pilotées par l'IA.

Des plateformes aux systèmes de cyberdéfense

Pris ensemble, ces cinq principes définissent une catégorie à part entière. Les systèmes de cyberdéfense sont l'évolution de la plateforme, optimisés pour l'ère de l'IA. Une plateforme n'est généralement qu'un ensemble de produits derrière une console partagée, liés par une connexion et un contrat de licence plutôt que par conception.

Un système de cyberdéfense fonctionne autrement. Ses données sont partagées, l'IA est intégrée, la réponse est coordonnée et les experts humains restent aux commandes. Il s'agit d'une architecture conçue pour fonctionner comme un seul produit plutôt que comme une collection de produits disposés pour en avoir l'apparence.

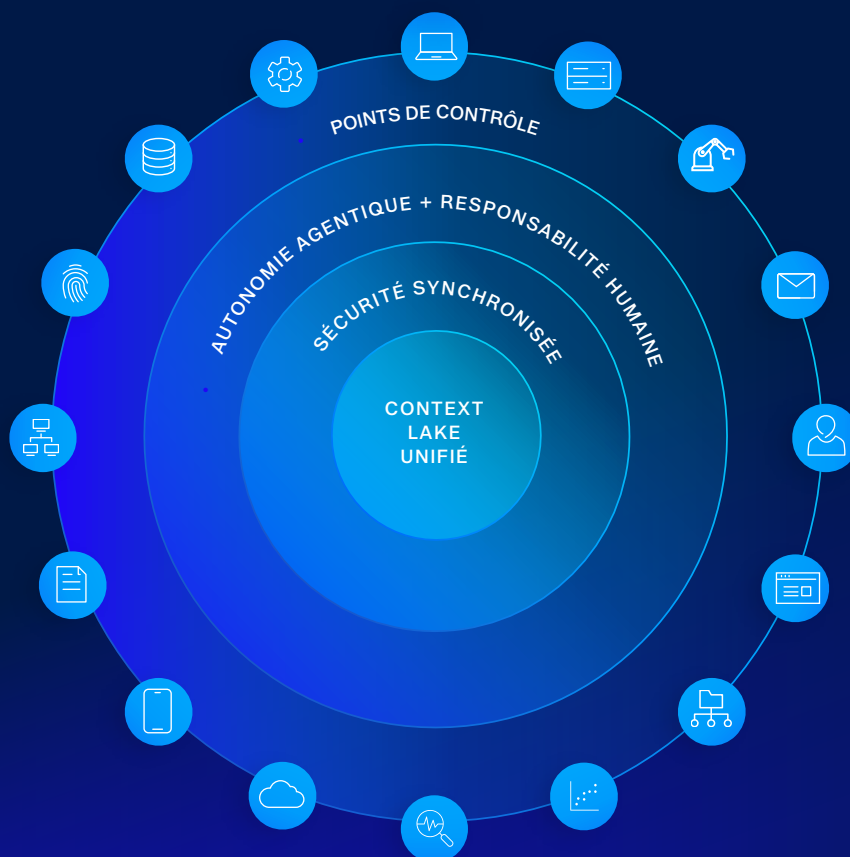


Sophos Fusion : le système de cyberdéfense Sophos

Sophos Fusion est le système de cyberdéfense le plus complet du secteur, développé pour un monde où les menaces évoluent à la vitesse de l'IA. Grâce à l'architecture Sophos AI-Native Cybersecurity Defense System et à plus de 500 intégrations Sophos et tierces, il voit tout, connecte tout et permet à vos défenses de répondre comme un seul et même système.

Sophos Fusion met en pratique les principes du système de cyberdéfense : une architecture unique et ouverte où chaque point de contrôle fonctionne comme un tout, optimisé par une IA agentique, avec expertise humaine pour protéger les organisations contre les menaces basées sur l'IA dont la vitesse de déplacement dépasse les capacités de réactions des équipes de défense.

Plus un client active de solutions du portefeuille Sophos, plus Sophos Fusion apporte de la valeur.



Des points de contrôle synchronisés et autonomes

Chaque point de contrôle que vous possédez déjà fournit des renseignements sur les menaces en temps réel et initie des actions de réponse. L'architecture est entièrement ouverte : elle s'intègre nativement aux produits Sophos et à plus de 500 technologies tierces. Ainsi, les investissements que vous avez déjà réalisés font partie d'une défense coordonnée plutôt que de fonctionner en vase clos.

Cette solution inclut également l'intégration de la sécurité Microsoft la plus approfondie sur le marché, sur tous les contrats Microsoft plutôt que seulement les plus coûteux, afin que même les organisations disposant de licences Microsoft d'entrée de gamme puissent renforcer leurs défenses avec cette télémétrie.

Une vue partagée, en temps réel

Toute la télémétrie issue de chaque point de contrôle circule en temps réel dans le Context Lake unifié, une couche de données partagée unique. Il n'y a aucun délai d'agrégation ni aucun magasin de données distinct au niveau de chaque point de contrôle. Considérez cela comme un système nerveux partagé : chaque point de contrôle détecte ce que tous les autres points de contrôle détectent, au moment même où cela se produit. Cette compréhension partagée est ce qui rend la coordination possible.

Une réponse coordonnée à travers chaque couche : Sécurité Synchronisée

La Sécurité Synchronisée est le tissu conjonctif qui transforme la compréhension partagée en action coordonnée au sein de Sophos Fusion. Elle permet aux points de contrôle Sophos et non Sophos de répondre automatiquement aux menaces de façon coordonnée.

Une détection au niveau d'un poste peut ainsi déclencher une réponse au niveau du pare-feu. Une identité compromise peut verrouiller l'accès à l'ensemble de l'environnement. Un email suspect peut déclencher une vigilance renforcée sur toutes les autres couches. Plus vous déployez de solutions Sophos, plus vous débloquez d'avantages liés à la Sécurité Synchronisée.

L'approche est similaire à celle d'un système d'extinction d'incendie d'un bâtiment moderne : un capteur dans une pièce ne se contente pas de déclencher une alarme ; il ferme les portes coupe-feu, redirige le flux d'air et active les sprinkleurs aux étages voisins. Sophos Fusion fonctionne de la même manière, comme un tout coordonné. Il peut le faire car les données sont déjà unifiées. Aucune configuration ou action supplémentaire n'est requise.

Une IA agentique avec responsabilité humaine

Sophos Fusion détecte, investigate et apporte une réponse à la vitesse machine, mais jamais sans supervision humaine. Chaque action s'inscrit toujours dans des limites définies et continuellement ajustées par des experts humains. C'est pour cela que l'on parle d'IA agentique : une IA capable de raisonner face à de nouvelles situations, et pas seulement de suivre des playbooks fixes.

L'image du pilote automatique en aviation permet de bien comprendre l'idée. Le système peut piloter l'avion, mais le pilote définit les paramètres, surveille les instruments et prend le relais lorsque la situation est inhabituelle ou à haut risque.

Dans Sophos Fusion, cette capacité agentique est fournie par Fusion AI, l'IA agentique native de Sophos. Sophos intègre plus de 50 modèles d'IA dans ses défenses, tous continuellement affinés grâce aux renseignements sur les menaces en temps réel. Par exemple, Sophos Email utilise plus de 20 modèles, y compris des modèles propriétaires de traitement du langage naturel (NLP) qui analysent le texte, le ton, le contexte et la structure des emails, pour identifier les attaques de phishing et BEC (Business Email Compromise).

Sophos MDR, un service 24/7 où les experts Sophos surveillent et apportent une réponse en votre nom, exploite le plus grand SOC agentique sur le marché en utilisant le système de cyberdéfense de Sophos. Il s'agit du plus vaste dispositif de détection et de réponse managées du secteur, protégeant plus de 40 000 organisations. Il résout 52 % des incidents de bout en bout grâce à l'IA, avec une moyenne de 89 secondes entre le déclenchement de l'alerte et celui de la réponse automatisée, tandis que les experts humains restent responsables des décisions qui comportent un risque organisationnel.

Une intelligence cumulative

Le système de cyberdéfense de Sophos apprend de chaque attaque, et pas seulement des attaques visant votre organisation. Chaque menace rencontrée dans l'une des plus de 625 000 organisations protégées par Sophos est réinjectée dans Sophos Fusion, ainsi que chaque cas particulier résolu par un analyste et chaque nouvel environnement mis en ligne. Sophos X-Ops améliore cela grâce à sa propre expertise approfondie et aux renseignements sur les menaces en temps réel qui sont ensuite automatiquement diffusés à chaque produit Sophos et à chaque client, améliorant ainsi leurs défenses.

Son fonctionnement est similaire à celui du système immunitaire chez l'homme. Chaque menace rencontrée par le corps devient une partie de sa mémoire permanente, cataloguée, comprise et prête à être mobilisée si elle réapparaît. Sophos Fusion fonctionne de la même manière. Un nouveau client est protégé dès le premier jour contre des menaces qu'il n'a jamais vues auparavant, car le système les a déjà rencontrées.

C'est pourquoi le chiffre de plus de 625 000 est important. Il reflète l'étendue de l'expérience qui permet à la protection et aux renseignements de se combiner. Plus le système voit de choses, mieux il parvient à défendre tous ceux qui s'y trouvent.

Sophos Fusion : l'expérience concrète de cette architecture du système de cyberdéfense

Sophos AI-Native Cybersecurity Defense System est l'architecture. Sophos Fusion est l'endroit où vous en faites l'expérience. Un seul endroit pour gérer vos points de contrôle Sophos, voir la situation complète depuis chaque point de contrôle connecté et prendre des mesures.

Cela signifie qu'il n'y a rien de plus à acheter ou à activer, et qu'il n'est pas nécessaire de modifier votre façon de travailler. Chaque point de contrôle Sophos fait déjà partie de Sophos Fusion; dès que vous en déployez un, vous êtes intégré à l'architecture. Et plus vous connectez de points de contrôle Sophos ou tiers, plus le système révèle son potentiel, alimentant une vue partagée plus riche et créant davantage de valeur sur tout ce que vous utilisez déjà.

L'attaque vue depuis Sophos Fusion

Revenons à l'attaque multi-étapes mentionnée précédemment. Un email piégé, des identifiants volés, une connexion inhabituelle, une règle de transfert de boîte de réception et des mouvements latéraux vers des données sensibles. Dans Sophos Fusion, la télémétrie provenant de Sophos Email et de l'environnement Microsoft du client converge vers le Context Lake unifié. Sophos XDR corrèle ensuite ces signaux à leur arrivée, reconnaissant la séquence comme une attaque connectée plutôt que comme cinq alertes sans lien.

À partir de là, la Sécurité Synchronisée coordonne la réponse entre la messagerie, l'identité, le poste et le réseau. L'IA agentique agit à la vitesse machine, tandis que les analystes Sophos MDR agissent directement et prennent les décisions à haut risque. L'attaque qui pourrait passer inaperçue auprès de produits isolés est interceptée par un système qui a une vision d'ensemble.

Ce que Sophos Fusion signifie pour votre organisation

Sophos Fusion assure la cyber-résilience à l'ère de l'IA agentique, dans quatre domaines essentiels pour l'entreprise.

- **Protection contre les menaces accélérées par l'IA qui se déplacent plus rapidement que les équipes de défense ne peuvent répondre.** Les attaques multi-étapes sont détectées et contenues rapidement, même si l'IA accélère leur vitesse et leur ampleur, car chaque point de contrôle partage le contexte et réagit de concert plutôt que d'agir isolément.
- **Un impact accru généré par vos équipes et vos investissements.** L'IA agentique absorbe le travail fastidieux et routinier de triage et de réponse, permettant à votre équipe et à vos points de contrôle existants d'en faire plus sans ajout de personnel ni de complexité supplémentaire. Chaque outil connecté, Sophos ou non, contribue au résultat final.
- **Une posture renforcée en matière de conformité et de cyberassurance.** Une couverture 24/7, un contexte conservé entre les couches et une réponse coordonnée vous fournissent les preuves attendues par les auditeurs, les autorités de régulation et les assureurs, à partir d'un enregistrement unique consultable plutôt que de journaux exportés manuellement. L'architecture qui renforce la protection vous permet également de mieux en démontrer l'efficacité.
- **Une stratégie de cybersécurité alignée sur votre activité** En connectant et en coordonnant vos défenses, Sophos Fusion vous permet de dépasser la gestion de tableaux de bord tactiques pour gagner en assurance opérationnelle, en bénéficiant d'une visibilité claire sur l'emplacement de vos lacunes et de vos risques les plus importants, ainsi que sur l'efficacité de vos investissements. C'est le moyen pour les organisations de toute taille, avec ou sans RSSI, de mettre enfin en œuvre la stratégie qu'elles cherchaient depuis longtemps à bâtir.

Tous les clients Sophos font déjà partie de Sophos Fusion, le système de défense Sophos. Il s'agit d'une mise à niveau automatique et transparente, protégeant les clients contre les menaces inhérentes à l'ère de l'IA.

Démarrer avec Sophos Fusion

Chaque solution Sophos fait partie de Sophos Fusion, faisant de chacune d'elles un point d'entrée plutôt qu'un outil autonome. La prise en main est aussi simple que le déploiement d'un produit ou d'un service Sophos — Sophos MDR, Sophos XDR, Sophos Endpoint, Sophos Firewall et Sophos Email sont des points de départ courants. Plus vous ajoutez de solutions, plus vous débloquez le potentiel de l'architecture.

Il n'est pas nécessaire de changer les autres points de contrôle tiers sur lesquels vous vous appuyez aujourd'hui. Intégrez-les dans Sophos Fusion pour fournir en continu des renseignements sur les menaces en temps réel et exécuter des actions de réponse. Commencez là où votre risque est le plus élevé, puis étendez progressivement votre couverture à votre rythme.

Prêt à commencer ? Contactez un expert Sophos pour identifier le point de départ adapté à votre environnement, ou apprenez-en plus sur sophos.fr/fusion.

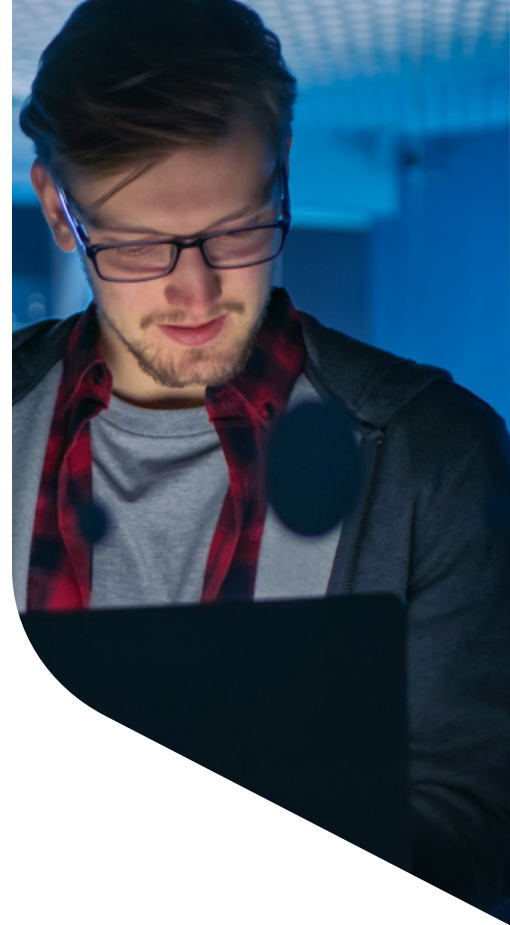
Conclusion

Pendant des années, la réponse par défaut à chaque nouvelle menace a consisté à ajouter un produit de plus, une habitude qui a créé une fragmentation dont les attaquants tirent désormais parti. L'IA n'a fait qu'aggraver le problème en creusant l'écart entre la rapidité avec laquelle une attaque se propage et la capacité des équipes à répondre console après console. Ajouter plus de produits ne comblera pas cet écart. Seul un système de cyberdéfense le pourra.

Avec un système de cyberdéfense, la défense ne se joue plus au niveau des produits pris séparément, mais au niveau de l'architecture qui les connecte :

- Une seule vue partagée
- Une réponse coordonnée à travers chaque couche
- Une IA intégrée pour agir à la vitesse machine
- Des experts humains conservant le discernement et la responsabilité, à leur juste place

Sécuriser à l'ère de l'IA signifie faire en sorte que tout ce que vous possédez déjà fonctionne ensemble comme un tout. Sophos Fusion, l'architecture Sophos AI-Native Cybersecurity Defense System, permet d'appliquer ce modèle sans avoir à remplacer vos investissements actuels.



Prêt à discuter de vos besoins en matière de cybersécurité à l'ère de l'IA ?

Discutez avec un **expert Sophos dès aujourd'hui**.

Sophos France

Tél. : 01 34 34 80 00

Email : info@sophos.fr