SOPHOS
Cybersecurity evolved.

Sécuriser le travail à distance

En tout lieu. Tous les appareils. Toutes les ressources.

Livre blanc Sophos Février 2021

Le travail à distance est appelé à perdurer : selon le Gartner, 74 % des organisations s'attendent à ce que certains employés continuent de travailler à distance une fois la pandémie terminée[1]. Dans le même temps, les ressources dont les personnes ont besoin pour travailler se trouvent également en différents endroits : sur des serveurs au bureau, dans des applications basées dans le Cloud, comme Office 365 ou Salesforce, et dans des environnements Cloud privés ou publics sur Amazon Web Services (AWS) ou Microsoft Azure.

Les équipes informatiques sont chargées de protéger chaque utilisateur et chaque ressource, où qu'ils se trouvent. En parallèle, les cybercriminels continuent d'améliorer leurs méthodes pour pénétrer dans les organisations qui se sont largement virtualisées.

Sécuriser le travail à distance, peu importe où se situent les personnes et les ressources, nécessite :

- Une connectivité sécurisée, pour que les utilisateurs puissent accéder aux ressources en tout lieu : à la maison, en déplacement ou au bureau
- La protection des appareils utilisés pour effectuer ces connexions : postes de travail, ordinateurs portables, téléphones mobiles et tablettes
- La protection des données et des charges de travail auxquelles les utilisateurs doivent accéder, qu'elles soient dans le Cloud ou sur votre réseau local
- Une gestion simple, pour que les équipes informatiques puissent gérer leurs organisations distribuées de n'importe où, sans alourdir leur charge de travail

Heureusement, Sophos couvre tous ces domaines. Nous proposons un portefeuille complet de produits de sécurité de nouvelle génération dotés de capacités de protection avancées. Tout est contrôlé depuis une plateforme de sécurité Web unique qui réduit les frais administratifs quotidiens tout en permettant aux équipes informatiques de gérer la sécurité de leur organisation depuis n'importe quel endroit.

Ce présent livre blanc vous explique comment Sophos répond à chacune de ces exigences. Il explore également les avantages en matière de productivité et de protection que les clients constatent lorsqu'ils utilisent un système de cybersécurité Sophos pour sécuriser leur organisation.

Se connecter en toute sécurité

Il n'y a aucun doute que la pandémie de Covid-19 a entraîné une augmentation massive du travail à distance. En mai 2020, 62 % des Américains salariés travaillaient à domicile. Cependant, le travail à distance était populaire avant même l'arrivée du Covid-19, et de nombreux employés de bureau télétravaillaient déjà quelques jours par semaine. Au Royaume-Uni, le télétravail a augmenté de 74 % au cours de la dernière décennie, tandis qu'en Australie, environ un tiers de la main-d'œuvre télétravaille régulièrement.

Le travail à distance est une solution gagnante pour les entreprises, mais aussi pour le personnel : les employés économisent du temps et des frais de déplacement, tout en bénéficiant d'une plus grande flexibilité et d'une meilleure productivité. Les entreprises, quant à elles, réduisent leurs coûts et gardent leurs salariés en poste plus longtemps. Mais pour les équipes informatiques, le travail à distance à long terme pose des problèmes de sécurité supplémentaires. Que les employés se connectent depuis leur salon, se rendent chez un client ou sirotent un café sur un hotspot Wi-Fi n'importe où dans le monde, votre réseau et vos données doivent être protégés en toutes circonstances.

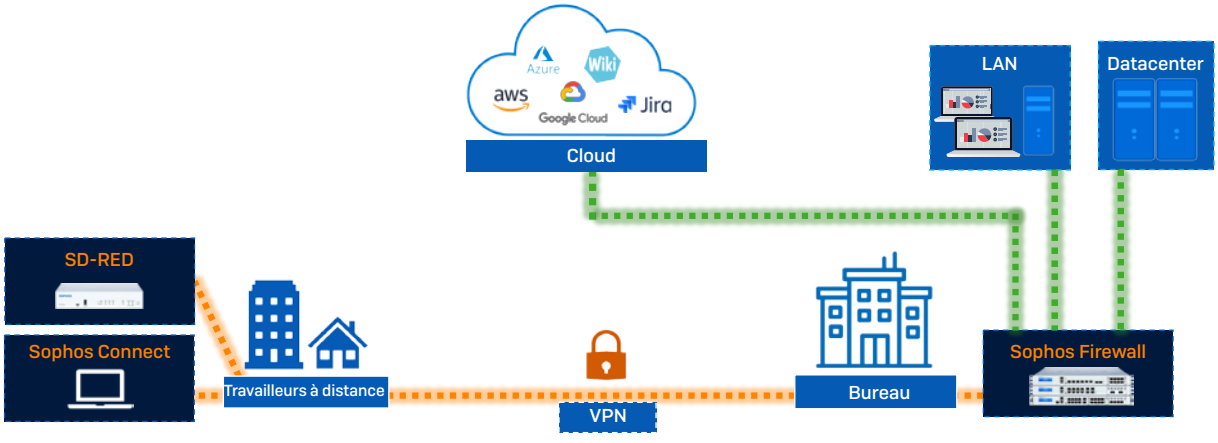
Avec Sophos, vos employés peuvent se connecter et travailler rapidement, efficacement et en toute sécurité, où qu'ils se trouvent. Nous proposons à la fois des options VPN traditionnelles et notre solution Zero Trust Network Access (ZTNA).

VPN

Utilisez notre **client VPN Sophos Connect** gratuit et facile à déployer avec **Sophos Firewall** pour connecter les travailleurs distants au bureau principal et à vos ressources dans le Cloud. Sophos Connect compte plus de 1,4 million d'utilisateurs dans le monde. Vos utilisateurs distants obtiennent un accès sécurisé aux ressources situées sur le réseau de votre entreprise ou dans Cloud public depuis leurs appareils Windows et macOS.

Pour une connectivité à distance optimale, **Sophos SD-RED** (Remote Ethernet Device) est un dispositif plug-and-play simple qui fonctionne avec **Sophos Firewall** pour connecter les succursales, les sites distants et les personnes à votre réseau principal (qu'il soit physique ou dans le Cloud).

Il fournit un VPN dédié ou à double tunnel toujours actif, facile à déployer et à gérer grâce à des options flexibles. Il est également très petit et portable, ce qui le rend idéal pour les cadres dirigeants et les autres personnes qui ont besoin d'accéder à une connexion sécurisée à tout moment et en tout lieu.



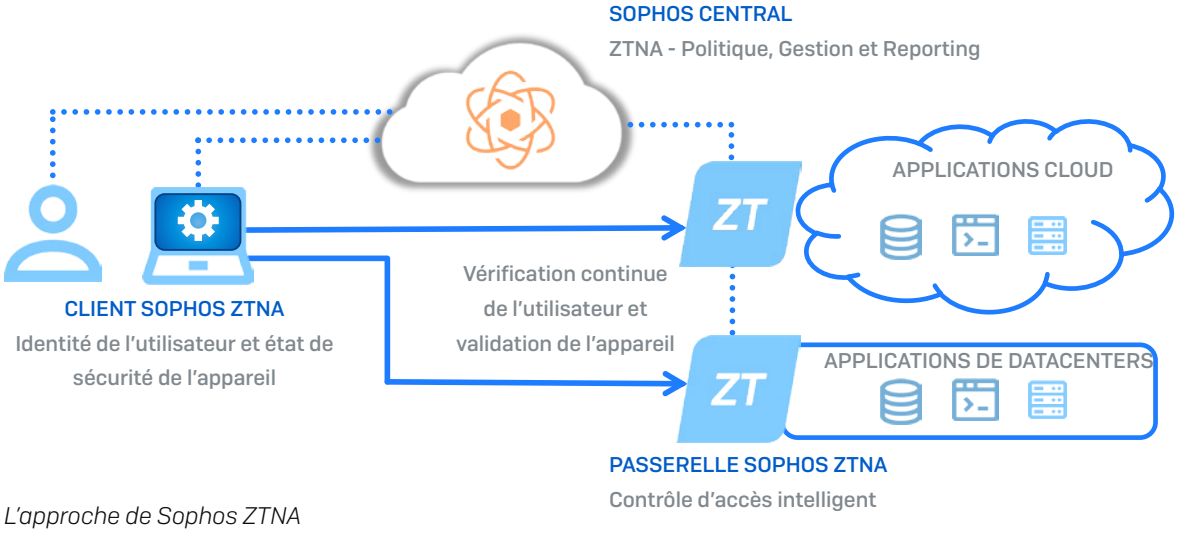
Connexion à distance sécurisée entre Sophos Firewall et le VPN Sophos Connect et SD-RED

ZTNA

Depuis des années, la technologie VPN permet aux travailleurs de se connecter à distance. Elle a d'ailleurs joué un rôle majeur au début de la pandémie, en aidant les organisations à mettre en place un télétravail sécurisé en quelques jours seulement. Cependant, de plus en plus d'organisations souhaitent aujourd'hui une offre de sécurisation avancée pour laquelle le VPN n'a pas été conçu.

Sophos Zero Trust Network Access (ZTNA) est une excellente alternative au VPN d'accès à distance. Il permet aux utilisateurs de se connecter aux ressources de l'entreprise depuis n'importe quel endroit, de manière simple et transparente. Il renforce également votre sécurité en vérifiant constamment l'utilisateur, généralement avec une authentification multifacteur et un fournisseur d'identité, et en validant l'état de sécurité et de conformité de l'appareil.

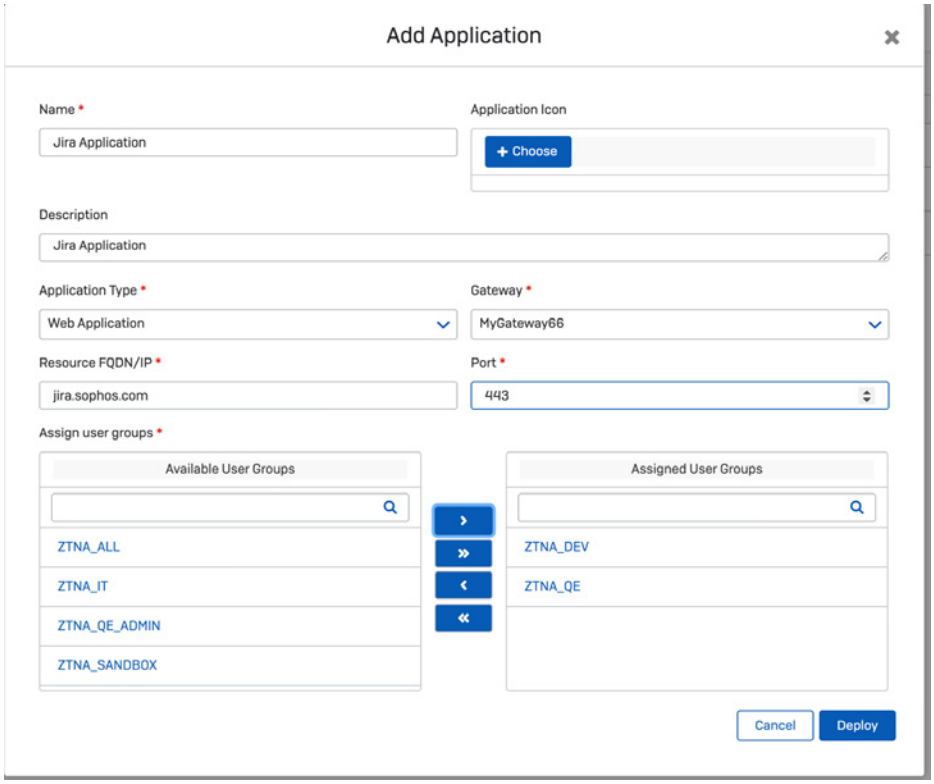
Sophos ZTNA s'assure que l'appareil est enregistré, à jour, et correctement protégé, et que le chiffrement est activé. Il utilise ensuite ces informations pour prendre des décisions en fonction de politiques de sécurité personnalisables afin de déterminer les privilèges et l'accès des utilisateurs aux applications réseau critiques.



L'approche de Sophos ZTNA

Avec Sophos ZTNA, vous pouvez :

- Renforcer vos cyberdéfenses. Sophos ZTNA vous offre des contrôles granulaires : tout utilisateur, tout appareil, toute application peut être contrôlé individuellement en fonction de la politique de sécurité de l'entreprise et du niveau de risque toléré. Il se défait du concept de 'confiance implicite' en une personne sur la base de sa seule présence sur le réseau. Au lieu de cela, il renforce la protection et réduit le risque de mouvement latéral sur le réseau en évaluant constamment l'identité et l'état de sécurité de l'appareil avant d'autoriser un accès.
- Augmenter votre efficacité. Sophos ZTNA étant géré depuis la plateforme Sophos Central, il est facile d'enregistrer de nouveaux utilisateurs ou de prendre en charge un environnement de travail changeant. De plus, il est davantage transparent pour les utilisateurs finaux et leur offre une expérience de connexion sans friction par rapport au VPN.



Ajoutez aisément des applications avec Sophos ZTNA

Quelle que soit la méthode que vous choisissez, les produits de sécurité primés de Sophos vous aideront à sécuriser vos employés en tout lieu et sur tout appareil.

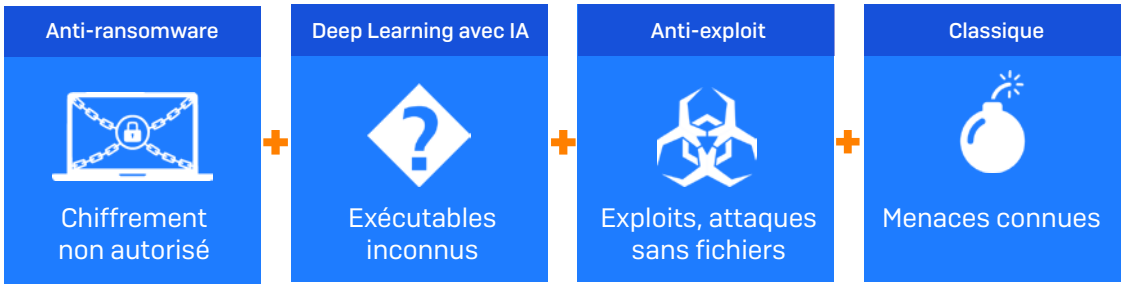
Protection des appareils

51 % des organisations ont été touchées par un ransomware l'an passé et les cybercriminels ont réussi à chiffrer les données dans 73 % de ces attaques[2].

Associez ces statistiques alarmantes à la nécessité de sécuriser toutes sortes d'équipements (ordinateurs de bureau, ordinateurs portables, appareils d'entreprise et personnels) avec une multitude de systèmes d'exploitation (Windows, macOS, Linux, Android, Chromebook et iOS), et vous vous préparez à faire face à un réel casse-tête de cybersécurité.

Sophos Intercept X vous offre la meilleure protection sur le marché pour sécuriser tous ces appareils et toutes ces plateformes. Vous bénéficiez de plusieurs couches de technologie qui bloquent les attaquants à de nombreux points de la chaîne de frappe, notamment :

- Protection anti-ransomware. Elle bloque le chiffrement non autorisé des fichiers, des disques durs et des enregistrements de démarrage, et les restaure vers leur état d'origine sain.
- Deep Learning avec IA. Il utilise des millions d'attributs de fichiers pour analyser les menaces et prévenir les malwares connus et inédits, et bloque ces derniers avant qu'ils ne puissent s'exécuter.
- Technologie anti-exploit. Elle bloque les exploits, les techniques d'adversaires actifs et les attaques sans fichier et basées sur des scripts.
- Protection basée sur les signatures virales. Cette protection de base bloque les menaces connues.



De plus, Sophos Intercept X sécurise n'importe quel appareil sur n'importe quelle plateforme ; vos employés peuvent donc travailler en toute sécurité sur l'appareil de leur choix :

- Ordinateurs de bureau et portables sous Windows et macOS
- Serveurs Windows et Linux
- Environnements de bureau virtuels hébergés par des fournisseurs de Cloud
- Appareils mobiles fonctionnant sous Android, iOS ou Chromebook

EDR (Endpoint Detection and Response)

Les cyberattaques les plus dévastatrices sont celles qui sont pilotées manuellement et qui exploitent des outils et des processus légitimes tels que PowerShell. Le piratage en temps réel permet aux attaquants de contourner les produits et protocoles de sécurité en modifiant leurs tactiques, techniques et procédures (TTP) au fur et à mesure de leur progression. Une fois à l'intérieur de votre réseau, les attaquants peuvent se déplacer latéralement pour exfiltrer des données, déployer des ransomwares et installer des logiciels malveillants et des portes dérobées en vue d'attaques futures.

Pour bloquer ces attaques manuelles, il faut une réponse pilotée manuellement par des experts Threat Hunting. **Intercept X with EDR** (Endpoint Detection and Response) vous donne les outils dont vous avez besoin pour traquer les menaces depuis la même console utilisée pour gérer votre protection endpoint Intercept X.

Il s'agit de la première solution EDR conçue à la fois pour les analystes de sécurité et les administrateurs informatiques. Tandis que d'autres outils EDR nécessitent souvent une équipe dédiée ou un SOC interne (Security Operations Center), Sophos EDR est simple à utiliser sans sacrifier sa capacité à effectuer des analyses puissantes.

Avec Intercept X with EDR, vous pouvez analyser les signaux suspects et les menaces, et améliorer votre hygiène informatique grâce à de puissantes requêtes SQL personnalisables et prêtes à l'emploi. Exemples de cas d'usages fréquents :

- Chrome est lent. Identifiez quelles extensions de Chrome non autorisées ont été installées.
- Vérification de l'activité sur le réseau. Recherchez les tentatives de connexion ayant échoué et les communications actives à partir de PowerShell.
- Requêtes logicielles. Vérifiez que les fichiers sensibles ont été supprimés des appareils ou que vous n'avez pas dépassé l'utilisation de la licence logicielle.
- Analyse du phishing. Identifiez les utilisateurs qui ont cliqué sur un lien suspect et s'ils ont téléchargé des fichiers.

De plus, vous pouvez accéder à distance aux appareils à l'aide d'un outil de ligne de commande. Cela vous permet de redémarrer des appareils, arrêter des processus actifs, exécuter des scripts ou des programmes, modifier des fichiers de configuration, exécuter des outils d'investigation et installer/désinstaller des logiciels.

Services MDR (Managed Detection and Response)

Si vous n'avez pas le temps, la capacité ou l'expertise pour mener vos propres recherches de menaces et investigations, le service **Sophos Managed Threat Response (MTR)** est là pour vous aider.

Sophos MTR est une équipe d'experts en réponse aux menaces et Threat Hunting qui fournissent des capacités de surveillance, de détection et de réponse 24 h/24 et 7 j/7, sous la forme d'un service entièrement managé. Ils traquent de manière proactive les menaces et incidents potentiels, les confirment et les bloquent avant qu'ils ne causent des dommages.

L'équipe MTR corrèle également les flux de données provenant de vos solutions de protection Sophos pour identifier les indicateurs d'une compromission. Contrairement à d'autres services MDR, Sophos ne se contente pas de vous notifier lorsqu'un problème surgit ; nous déterminons et prenons les actions les plus appropriées pour neutraliser la menace.

Appareils mobiles

Lorsque les employés utilisent leurs propres appareils pour travailler, les équipes informatiques ont alors la tâche de protéger les données de l'entreprise sans compromettre la vie privée des utilisateurs. **Sophos Mobile**, notre solution UEM (Unified Endpoint Management), sécurise les appareils iOS, Android, Chrome OS, Windows 10 et macOS. Elle vous permet de protéger n'importe quelle combinaison d'appareils personnels et professionnels avec un minimum d'efforts et est idéale pour les scénarios BYOD (Bring Your Own Device).

Sophos Mobile vous permet de :

- Bloquer les menaces spécifiques aux mobiles. Bénéficiez d'une défense de pointe contre les malwares mobiles, le phishing, les attaques de type « man-in-the-middle » et bien d'autres encore, le tout optimisé par Intercept X.
- Sécuriser les données de l'entreprise. Choisissez entre la gestion complète des appareils ou la gestion des conteneurs uniquement, en fonction de vos besoins.
- Réduire les tâches admin. Le portail libre-service permet aux utilisateurs d'enregistrer leurs appareils macOS, Windows 10 ou mobiles personnels, de réinitialiser leurs mots de passe et d'obtenir de l'aide, sans intervention du service informatique.

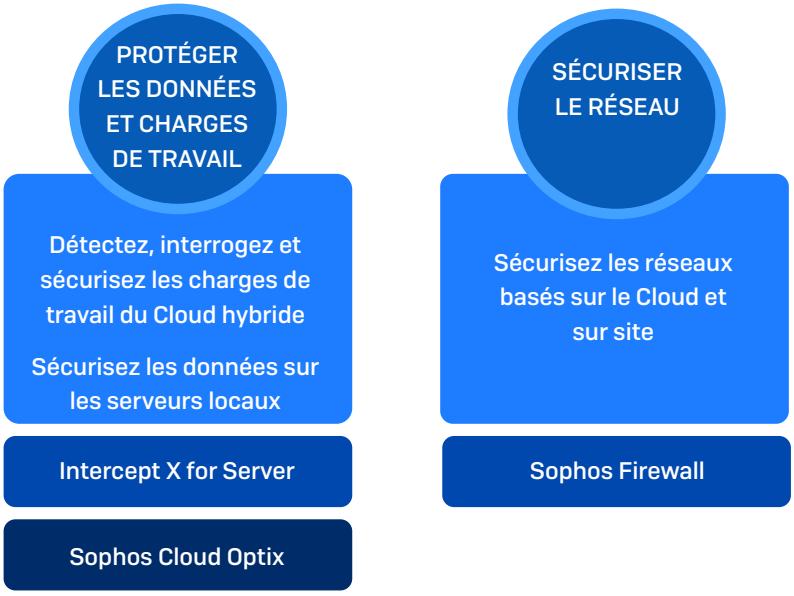
Protection des ressources

En fonction des besoins de votre entreprise, il se peut que vous exécutiez des serveurs sur site, utilisiez des applications dans le Cloud ou hébergiez des ressources dans des environnements de Cloud privés ou publics sur AWS, Azure ou GCP. Et il est fort probable que vous fassiez tout cela à la fois.

Le Cloud prend une place de plus en plus centrale dans les opérations quotidiennes de la plupart des organisations. C'est pourquoi les cybercriminels sont attentifs aux opportunités offertes par le Cloud, à tel point que 70 % des entreprises utilisant le Cloud public ont subi un incident de sécurité au cours des 12 derniers mois[3].

Lorsqu'il s'agit de sécuriser vos ressources, où qu'elles se trouvent, vous devez faire deux choses :

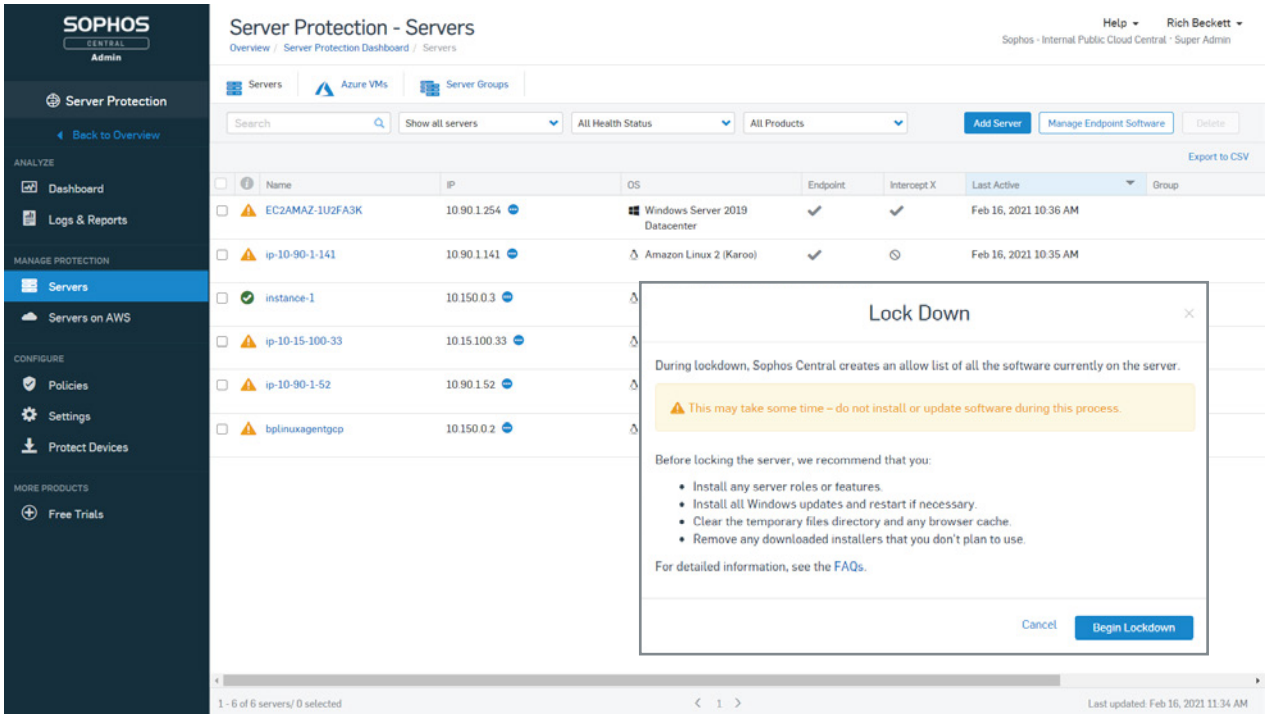
1. Protéger les données et les charges de travail elles-mêmes
2. Sécuriser le réseau sur lequel elles se trouvent pour empêcher les intrus d'entrer



Protection de vos données et de vos charges de travail

Vos données et vos charges de travail sont vos ressources les plus importantes. **Sophos Intercept X for Server** protège les environnements de serveur Cloud, locaux ou hybrides. Il protège les machines et bureaux virtuels Windows et Linux contre les menaces les plus récentes.

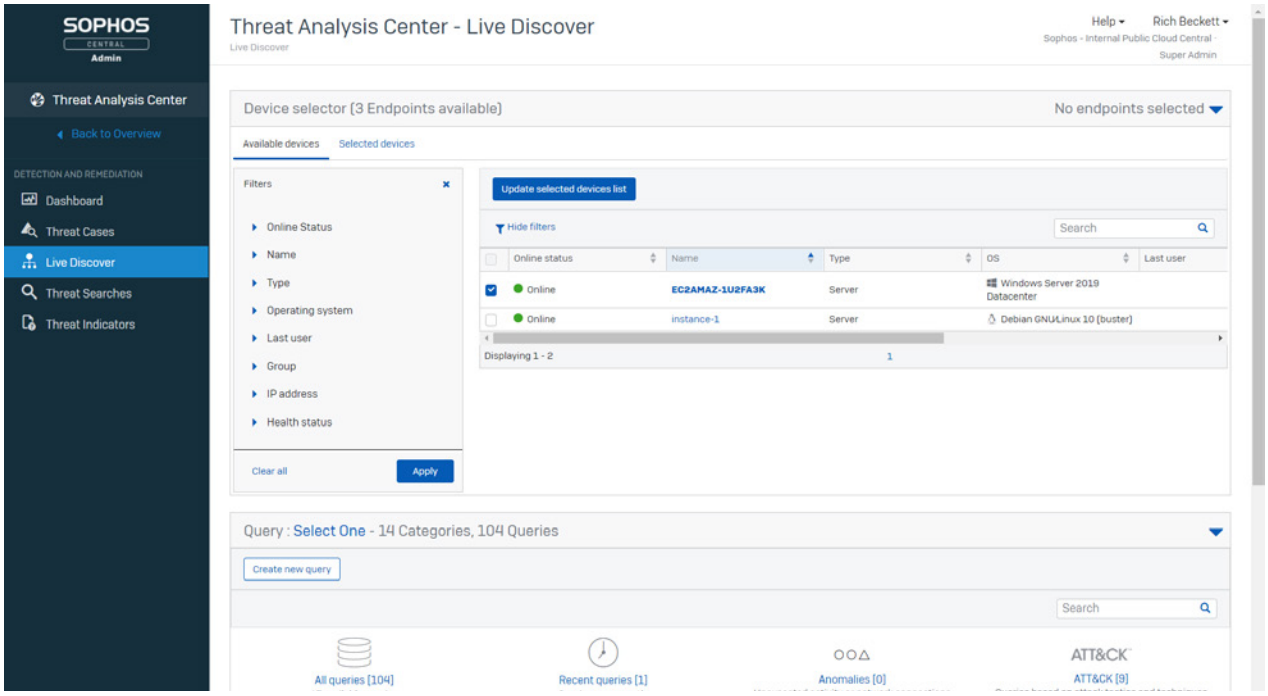
- Bloquez les attaques avancées. Notamment les ransomwares, les attaques basées sur un exploit et les malwares inédits.
- Verrouillez vos charges de travail de serveurs. Contrôlez ce qui peut ou ne peut pas s'exécuter et recevez des notifications lorsqu'une tentative de modification non autorisée est détectée.
- Gérez tout de manière centralisée. Déployez et maintenez tout à partir d'une seule console, y compris les scénarios mixtes comprenant des charges de travail dans le Cloud et des serveurs sur site.



Intercept X for Server

Vous pouvez également étendre vos investigations EDR à vos serveurs, qu'ils soient sur site ou dans le Cloud, avec **Intercept X for Server with EDR**. Cela vous permet de :

- Réaliser des opérations informatiques critiques et traquer les menaces. Identifiez les problèmes de performance, visualisez ce qui est installé et où il est installé, et traquez les activités suspectes.
- Détecter automatiquement les charges de travail dans le Cloud. Gardez un œil sur les services Cloud critiques, dont les compartiments S3, les bases de données et les fonctions sans serveur.
- Détecter les déploiements non sécurisés. Faites confiance à l'IA pour surveiller en permanence vos environnements de Cloud et vous notifier les irrégularités.

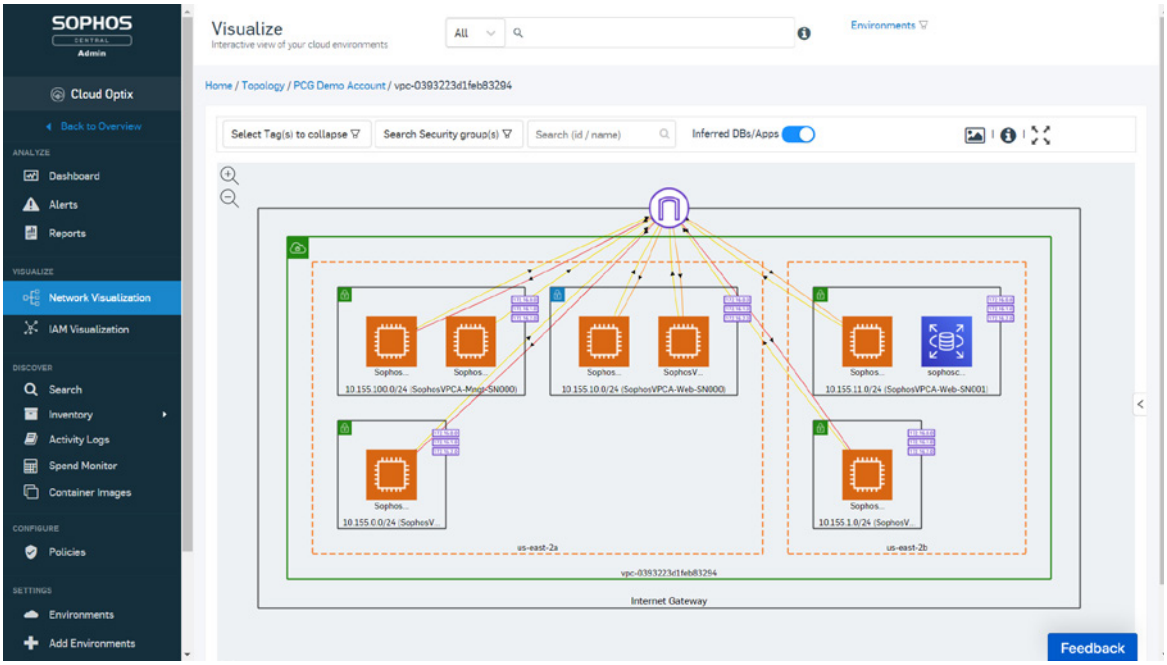


Étendez vos investigations EDR à votre serveur

Protéger les données et les charges de travail implique deux éléments clés : le premier est la protection. Le second est la visibilité. Vous avez besoin de garder une visibilité claire et permanente sur ce qui est exécuté et de pouvoir configurer les services des fournisseurs de Cloud afin de prévenir toute violation de sécurité.

Sophos Cloud Optix, notre solution de gestion de la posture de sécurité du Cloud (CSPM), vous offre la visibilité dont vous avez besoin pour sécuriser votre organisation, notamment :

- Visibilité multi-Cloud. Inventaire détaillé des ressources sur le Cloud, y compris les serveurs, les conteneurs, le stockage, le réseau et l'IAM pour AWS, Azure et GCP.
- Priorisation en fonction du niveau de risque. Analysez en continu les configurations pour identifier les risques de sécurité et les accès IAM surprivilégiés.
- Gestion de la conformité. Contrôlez en permanence la conformité grâce aux modèles prêts à l'emploi, aux politiques de sécurité personnalisables et aux outils de collaboration.
- Sécurité intégrée. Identifiez les pare-feu Sophos Firewall et la protection des charges de travail sur AWS
- Optimisation des coûts du Cloud. Gérez les dépenses AWS et Azure sur un seul écran.



Sophos Cloud Optix

Les alertes de sécurité pour vos environnements Cloud sont utiles, comme les services Amazon GuardDuty, mais vous pouvez être vite submergés par leur volume. Les notifications qui nécessitent une réelle attention peuvent être noyées dans la masse.

Chez Sophos, nous utilisons Sophos Cloud Optix pour protéger les environnements Amazon Web Services utilisés pour héberger Sophos Central, notre plateforme de cybersécurité. L'un des principaux avantages que notre propre équipe de sécurité a tiré de Cloud Optix est la possibilité de se concentrer sur ce qui est important.

« Avec Sophos Cloud Optix, nous réduisons considérablement la surproduction d'alertes. L'intelligence artificielle intégrée à Sophos Cloud Optix corrèle les données et nous montre ce qui est vraiment significatif et exploitable. »

Ross McKerchar, VP et CISO, Sophos

Protection du réseau

Pour protéger vos ressources, vous devez également sécuriser les réseaux sur lesquels elles sont exécutées. **Sophos Firewall** offre une protection et une visibilité inégalées pour les environnements sur site, AWS et Azure.

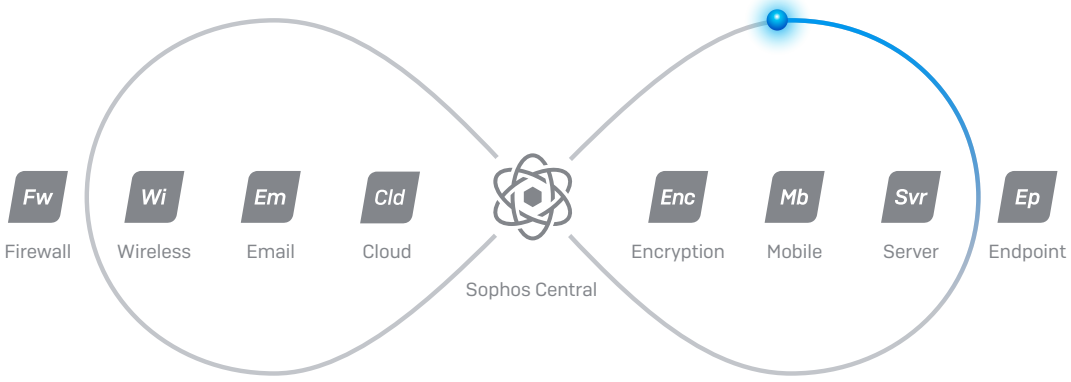
- Protection intégrée et multicouche pour bloquer les menaces les plus avancées
- Solution puissante tout-en-un avec WAF, IPS, ATP, filtrage des URL, routage basé sur le chemin d'accès et blocage au niveau national, reporting complet, ainsi qu'une visibilité totale sur l'activité des utilisateurs et du réseau
- Visibilité des applications Cloud, découverte du Shadow IT et réponse automatisée aux menaces
- Capacité de renforcer la protection de vos charges de travail Cloud contre le piratage, tel que les injections SQL et le cross-site scripting, tout en offrant un accès sécurisé aux utilisateurs grâce à l'authentification reverse proxy
- Souplesse d'exécution en tant que solution autonome et haute disponibilité

Et pour faciliter le déploiement dans le Cloud, tout est disponible dans une seule image de machine virtuelle préconfigurée.

Simplification de la gestion

Avec Sophos, vous pouvez gérer l'ensemble de votre sécurité depuis une seule plateforme Web : Sophos Central. Plus besoin de jongler entre différentes consoles pour protéger votre organisation. Tout est au même endroit. Sophos Central vous permet également de lancer des investigations multi-produits avec facilité, en corrélant les données de plusieurs services.

Et comme la plateforme Sophos Central est hébergée dans le Cloud, elle est idéale pour les équipes informatiques dispersées. Avec plus de 400 000 utilisateurs dans le monde, soyez rassurés en sachant que vous utilisez la plateforme de cybersécurité la plus fiable sur le marché.



Sophos Central permet également aux produits Sophos de partager en temps réel des informations sur les menaces et l'état de la sécurité et de travailler ensemble pour répondre automatiquement aux menaces. C'est ce que nous appelons la Sécurité Synchronisée. Les avantages incluent :

- Réponse automatisée aux incidents. Si un produit Sophos détecte quelque chose de suspect, comme un appareil non conforme ou une infection par un malware, il partage cette information avec le reste du système de cybersécurité. Les autres produits répondent alors automatiquement à l'incident, en quelques secondes seulement. Par exemple :
  - Sophos Firewall isole instantanément les appareils infectés, empêchant la menace de se propager et bloquant les mouvements latéraux.
  - Intercept X analyse automatiquement les postes de travail où une boîte de réception compromise a été détectée, limitant ainsi l'impact des menaces diffusées par email.
  - Sophos Wireless restreint l'accès au réseau des appareils non conformes, empêchant tout appareil malveillant et non sécurisé d'accéder à votre réseau sans fil.
- Aperçu unique. Les équipes informatiques bénéficient d'une visibilité et d'un contrôle accrus de leur réseau, avec notamment la possibilité de :
  - Identifier les appareils infectés à l'aide de leur nom plutôt que leur adresse IP, accélérant ainsi les investigations de sécurité.
  - Identifier toutes les applications sur le réseau. En moyenne, 43 % du trafic réseau est considéré comme « non catégorisé », ce qui signifie que l'équipe informatique ne sait pas s'il est bénin ou malveillant. Avec la Sécurité Synchronisée, Sophos Firewall et Intercept X travaillent ensemble pour identifier et catégoriser automatiquement TOUTES les applications sur le réseau.

Protection inégalée. Efficacité inégalée.

L'utilisation d'un système de cybersécurité Sophos vous permet de bénéficier d'une protection de nouvelle génération, d'une plateforme d'administration unique, du partage de l'intelligence sur les menaces entre les produits et de la réponse automatisée aux incidents. Ensemble, ces fonctionnalités permettent aux équipes informatiques de réaliser des gains d'efficacité et de productivité considérables.

En fait, les clients qui utilisent Sophos Intercept X et Sophos Firewall, administrés dans Sophos Central, affirment qu'ils sont en mesure de **doubler l'efficacité de l'équipe informatique** tout en bénéficiant d'**une baisse de 85 % des incidents de sécurité**.

« Disposer d'outils qui détectent et corrigent automatiquement la plupart des événements de sécurité permet à notre petite équipe informatique de gérer la sécurité de l'entreprise et d'éviter qu'elle ne soit compromise. »

Chief Technology Officer, fournisseur de services logiciels

Sécurisation en tout lieu, de tous les appareils et toutes les ressources

Le recours au travail flexible et à distance, ainsi que l'utilisation croissante du Cloud, sont devenus incontournables. Ils facilitent la vie, mais ils posent également de nouveaux défis aux équipes informatiques, tout en offrant de nouvelles opportunités aux cybercriminels. Pour sécuriser ce nouvel environnement, il faut des connexions sécurisées, des ressources sécurisées et des appareils sécurisés, où qu'ils se trouvent, sans ajouter de coûts informatiques supplémentaires.

Sophos peut vous aider à relever ces nouveaux défis grâce à des solutions puissantes et fiables. Contactez votre représentant Sophos pour discuter de vos besoins, ou démarrez un essai gratuit sans obligation pour tester l'un de nos produits.

1 https://www.gartner.com/en/newsroom/press-releases/2020-04-03-gartner-cfo-surey-reveals-74-percent-of-organizations-to-shift-some-employees-to-remote-work-permanently2

2. L'état des ransomwares 2020, Livre blanc Sophos

3. L'état de la sécurité du Cloud 2020, Livre blanc Sophos

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

210215 WPFR (MP)

SOPHOS