SOPHOS
Cybersecurity evolved.

Guide de la cybersécurité dans le secteur de la santé

La cybersécurité pour le secteur de la santé qui bloque les attaquants sans entraver les soins aux patients

Un livre blanc Sophos. Avril 2021

Cybersécurité et soins aux patients

Lorsque l'on parle de soins aux patients, on pense en premier lieu aux médecins, aux infirmiers et à tous les autres soignants qui dispensent les services et actes médicaux. Mais alors que la santé dépend de plus en plus de la technologie (à travers l'IA, le Cloud et les appareils connectés) et que les attaquants ne cessent de développer leurs techniques, la cybersécurité joue un rôle direct et majeur dans la capacité à fournir ces soins.

« Une cybersécurité inefficace constitue un danger manifeste et réel pour la sécurité des patients… les cyberincidents peuvent perturber de manière significative les systèmes de santé et de soins, et contribuer directement aux préjudices causés aux patients. »

Institute of Global Health Innovation, Imperial College London, Royaume-Uni

La pandémie de Covid-19 a accéléré l'adoption de technologies de santé numériques telles que les solutions de surveillance à distance des patients, les consultations en ligne et les dispositifs à domicile, et a entraîné une augmentation du personnel mobile/distant. Si ces changements ont apporté des améliorations significatives en matière d'efficacité, qui se poursuivront à long terme, ils ont également accru les défis de la cybersécurité auxquels les équipes informatiques sont confrontées.

« (Les cyberattaquants) cherchent à exploiter la digitalisation du monde médical, qui va prendre de plus en plus d'ampleur à l'avenir. »

John Noble, Président du Comité d'assurance de l'information et de la cybersécurité, NHS Digital, Royaume-Uni

Les défis de la cybersécurité dans le secteur de la santé

En 2021, Sophos a mené une enquête auprès de 328 professionnels de l'informatique du secteur de la santé dans 30 pays. Cette enquête a révélé les difficultés croissantes rencontrées avec la cybersécurité. 63 % des personnes interrogées ont déclaré que le nombre de cyberattaques subies en 2020 a augmenté, ce qui peut s'expliquer en partie par un grand nombre d'attaques tirant parti de la pandémie. Il n'est donc pas étonnant que 70 % des répondants aient affirmé que leur charge de travail de cybersécurité a également augmenté en 2020.

Les cyberattaques gagnent non seulement en volume mais aussi en complexité. Pour 60 % des répondants, les attaques sont désormais trop avancées pour que l'équipe IT puisse y faire face seule.

63 %	60 %	70 %
Le nombre de cyberattaques a augmenté au cours de 2020	Les cyberattaques sont trop avancées pour que l'équipe IT puisse les gérer seule	La charge de travail de cybersécurité a augmenté au cours de 2020

La complexité est l'ennemi de la sécurité

Dans le secteur de la santé, les organisations ont généralement un ratio utilisateur/personnel informatique supérieur à la moyenne. Plus l'infrastructure de sécurité est complexe, plus il est difficile pour les équipes IT surchargées de la maintenir à jour et de tirer pleinement parti des capacités de protection disponibles.

Sophos : protéger le secteur de la santé

Sophos travaille avec des organismes de santé du monde entier pour relever leurs défis en matière de cybersécurité et leur permettre de fournir des soins ininterrompus aux patients. Face à la fréquence et à la sophistication croissantes des attaques, nous pouvons vous aider à protéger vos données et votre organisation tout en permettant à vos équipes IT de réduire leur charge de travail liée à la cybersécurité. Découvrez comment nous pouvons vous aider à relever les défis les plus courants rencontrés par les établissements de santé.

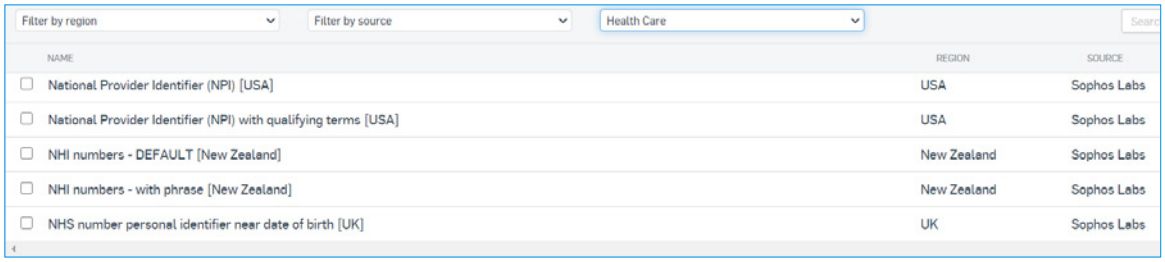
Sécurisez les données sensibles, où qu'elles se trouvent

Les établissements de santé détiennent une grande variété de données sensibles : des dossiers médicaux aux numéros de sécurité sociale en passant par les informations d'identification personnelle (IIP). Face à cette myriade de données — et autant d'endroits où elles sont stockées et utilisées — il peut être difficile de toutes les protéger.

Les outils de protection préventifs et actifs de Sophos protègent l'intégralité du réseau de santé, jusqu'au plus petit appareil personnel.

Sécuriser l'appareil ou la charge de travail qui détient les données

La protection **Sophos Intercept X** en mode Endpoint ou Serveur déploie plusieurs couches de protection pour sécuriser les données sur vos systèmes Windows, Mac, Linux et virtuels. Renforcez votre protection avec des règles de protection contre la perte de données (DLP) spécifiques au domaine de la santé, utilisant des termes ou des types de données de ce secteur.



Sophos Device Encryption offre un moyen simple et rapide de s'assurer que les appareils Windows et macOS sont correctement chiffrés, protégeant ainsi vos données (et prouvant la conformité) en cas de perte ou de vol.

Sécuriser le réseau sur lequel transitent les données

Sophos Firewall utilise une technologie de détection des menaces basée sur l'IA pour empêcher les attaques d'atteindre vos données sensibles, vos systèmes médicaux critiques et les autres éléments de votre écosystème.

Stopper les fuites de données par email — intentionnelles ou accidentelles

Sophos Email chiffre les données personnelles d'identification, les dossiers des patients, les fichiers d'imagerie médicale et toute autre donnée sensible, empêchant la fuite de données accidentelle ou malveillante.

Contrôler l'accès à vos données

Sophos Zero Trust Network Access (ZTNA) vous donne un contrôle absolu sur les personnes pouvant accéder aux données sur votre réseau. Des contrôles très granulaires bloquent les mouvements latéraux tout en garantissant que seules les personnes autorisées peuvent accéder aux données sensibles.

Affrontez les ransomwares du secteur de la santé

Les ransomwares sont de plus en plus intelligents et destructeurs, et le secteur de la santé est une cible lucrative. Dans ce secteur, les coûts engendrés par un ransomware ne se limitent pas au paiement de la rançon. En effet, la perte des données des patients, le report ou l'annulation de procédures médicales peuvent avoir un coût énorme et dévastateur. Les outils Sophos de prévention et de chasse aux menaces proactives évoluent sans arrêt pour devancer les ransomwares, et défendre vos données et votre réseau contre ces attaques.

Empêcher les ransomwares de vous prendre en otage

Chez Sophos, nous sommes fiers d'être les leaders mondiaux de la protection contre les ransomwares.

Sophos Intercept X est la meilleure protection sur le marché contre les ransomwares pour les serveurs et les postes de travail. Elle met en œuvre plusieurs couches de sécurité pour reconnaitre et bloquer les ransomwares à chaque étape :

- CryptoGuard, qui restaure automatiquement les fichiers chiffrés par une personne non autorisée vers leur état d'origine sain
- Le Deep Learning alimenté par l'IA, qui bloque les ransomwares connus et inconnus
- La protection contre les exploits, qui bloque les techniques utilisées par les attaquants pour télécharger et installer les ransomwares
- La protection fondamentale des SophosLabs, basée sur les signatures virales

Sophos Managed Threat Response (MTR) offre notre plus haut niveau de protection contre les ransomwares avec ses fonctions proactives de chasse aux menaces, de détection et de réponse, le tout sous forme de service managé par une équipe d'experts 24 h/24, 7 j/7. Nous veillons sur vous, même lorsque vous dormez.

Sophos Rapid Response garantit une assistance d'urgence pendant les attaques de ransomware en cours, même si vous n'êtes pas client de Sophos. Notre équipe vous aidera à maîtriser rapidement l'attaque pour protéger vos réseaux, vos applications et vos données, et ainsi limiter les perturbations et les dommages.

Offrez aux utilisateurs un accès sécurisé où qu'ils se trouvent

Les soignants, où qu'ils travaillent (en première ligne dans les hôpitaux, au domicile des patients ou de chez eux), doivent pouvoir accéder à tout moment aux données sensibles des patients et aux systèmes de santé. Les outils Sophos permettent à vos utilisateurs de se connecter en toute sécurité de n'importe quel endroit, sans que cela impacte leur travail vital.

Permettre aux utilisateurs de se connecter en toute sécurité de n'importe où

Sophos Firewall fournit des connexions sécurisées pour Windows et macOS à l'aide du VPN gratuit Sophos Connect. Facile à déployer et à configurer, il offre à vos utilisateurs distants un accès sécurisé aux ressources sur le réseau ou le Cloud public depuis leurs systèmes Windows et macOS. Avec plus de 1,4 million de clients actifs, vous pouvez nous faire confiance.

La réalité des ransomwares dans le secteur de la santé

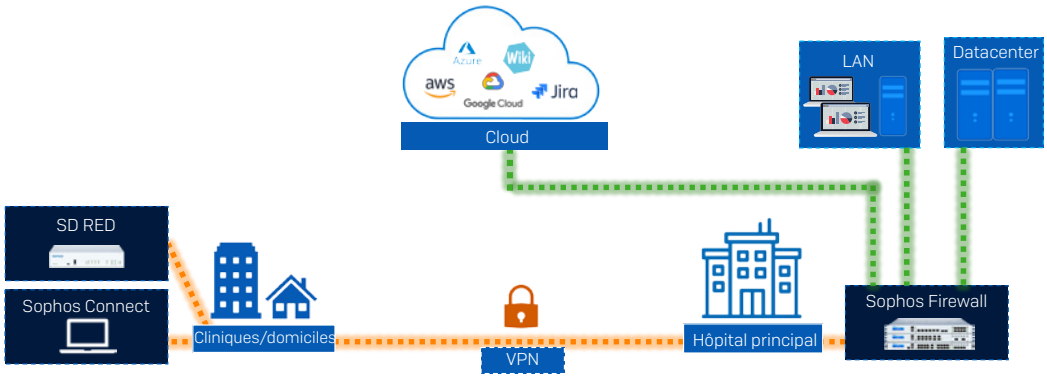
34 % ont été touchés par un ransomware l'an dernier

65 % des attaques ont chiffré les données

34 % ont payé la rançon

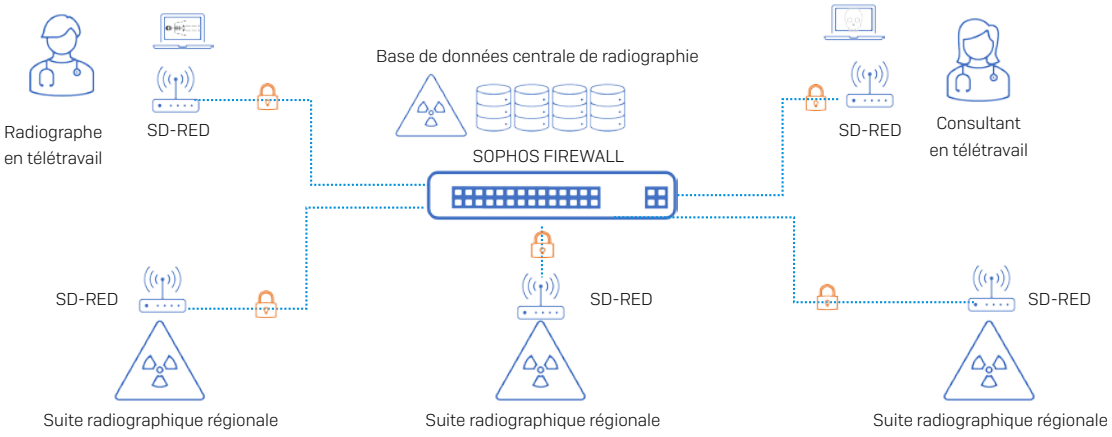
Coût moyen de rétablissement : 1,27 M$

L'état des ransomwares 2021, Sophos



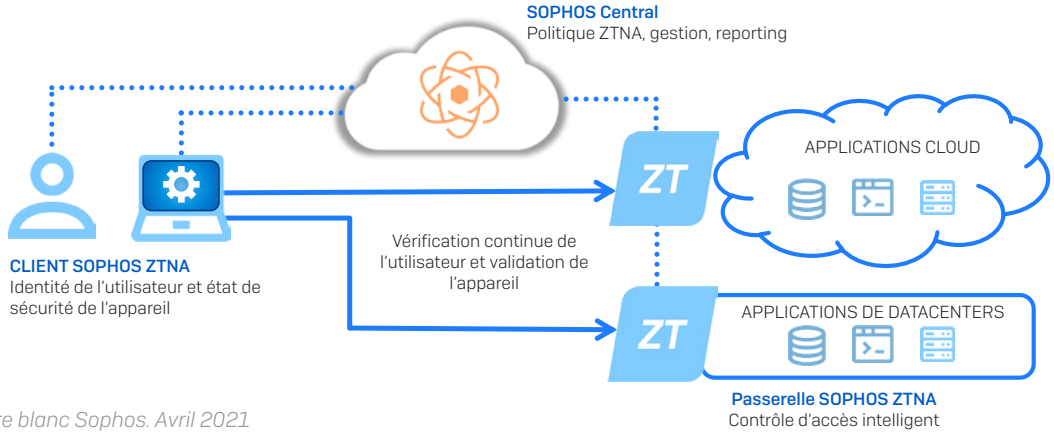
Sophos Firewall offre un accès distant sécurisé à l'aide du client Sophos Connect et des appareils SD-RED.

Pour une connectivité sécurisée ultime, **SD-RED** (Remote Ethernet Device) est un petit boitier plug-and-play qui fonctionne avec **Sophos Firewall** pour connecter les sites et les individus distants à votre réseau principal. Il est idéal pour les petites cliniques et les cabinets médicaux ainsi que les personnes avec des données très sensibles.



Exemple d'utilisation de Sophos Firewall et SD-RED en radiographie.

Pour un accès sécurisé Next-Gen, **Sophos Zero Trust Network Access** place l'identité au centre de la défense, en validant en permanence l'utilisateur, l'appareil et la conformité aux politiques. Il offre aux utilisateurs une expérience sans friction et transparente, et permet aux équipes informatiques de rendre les nouveaux utilisateurs rapidement opérationnels.



Renforcez votre équipe informatique

En 2020, dans le cadre d'une enquête, nous avions interrogé 5 000 responsables IT de différents secteurs, dont celui de la santé. 81 % des répondants ont déclaré que leur difficulté à trouver et à garder des professionnels de la sécurité compétents constituait un défi majeur pour garantir la sécurité informatique de leur organisation.

Quelle que soit votre problématique : besoin d'une expertise ou d'une capacité supplémentaire pour compléter vos ressources, les spécialistes de la sécurité Sophos peuvent devenir une extension de votre équipe et assurer la sécurité de vos systèmes de santé et des données de vos patients, 24 h/24 et 7 j/7.

Des experts en cybersécurité dédiés pour renforcer votre équipe IT

Sophos Managed Threat Response (MTR) est une équipe d'experts en chasse et réponse aux menaces, qui agit comme une extension de votre propre équipe. Elle apporte aux équipes IT limitées ou surchargées du secteur de la santé la capacité et l'expertise supplémentaires dont elles ont besoin pour faire face à toutes les menaces.

L'équipe Sophos MTR surveille votre environnement 24 h/24 et 7 j/7, en chassant de manière proactive et en validant les menaces et incidents potentiels. Si elle repère quelque chose de suspect, elle peut faire appel aux experts en malwares des SophosLabs pour investiguer et vérifier les indicateurs suspects.

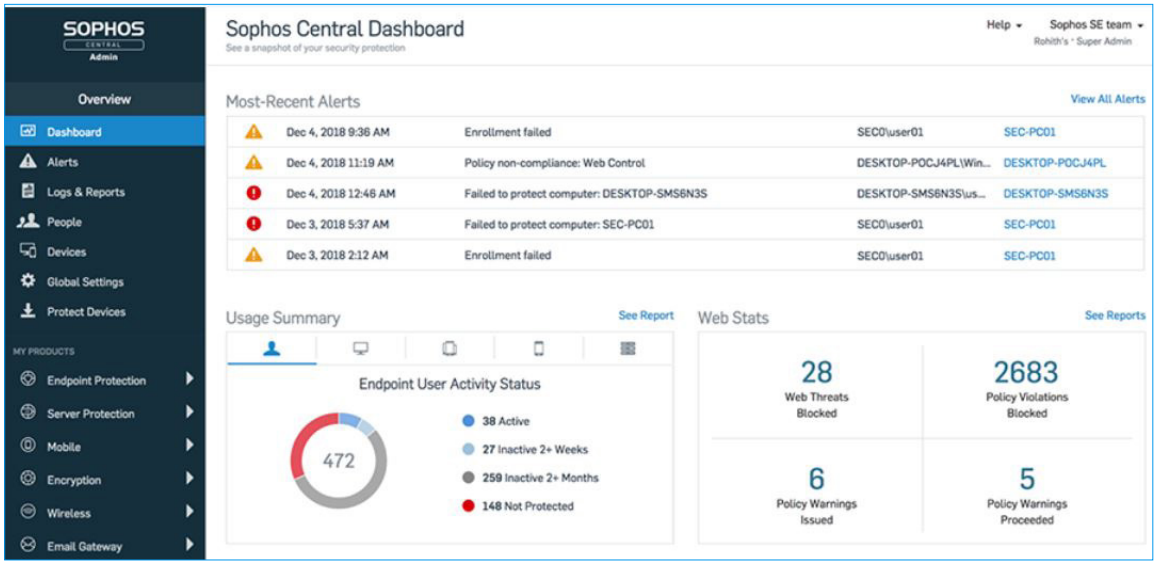
En outre, si vous le souhaitez, les équipes Sophos MTR peuvent aussi agir à votre place. Contrairement à d'autres services de détection et de réponse managés, notre équipe ne se contente pas de vous informer des problèmes, elle peut également neutraliser la menace pour vous. C'est vous qui décidez du niveau d'action que nous sommes autorisés à prendre et de la manière dont nous travaillons avec votre équipe.

Passez moins de temps à la gestion de la cybersécurité

Lorsque les ressources IT sont limitées, il devient difficile de passer au crible le déluge d'alertes de sécurité pour décider de celles à traiter en priorité. Sophos vous aide dans cette tâche, en vous offrant un tableau de bord centralisé de votre sécurité et une automatisation qui résout les problèmes avant que vous n'ayez à vous en préoccuper, ce qui vous permet de consacrer votre temps à des projets plus stratégiques.

Simplifier la gestion de la cybersécurité

Sophos Central est notre plateforme web unifiée où vous pouvez gérer tous vos produits de sécurité Sophos. Plus besoin de passer d'une console à l'autre pour sécuriser votre organisation. Avec Sophos Central, vous pouvez déployer et gérer votre protection en toute facilité, et mener des investigations grâce à différents produits capables de mettre en corrélation les données de multiples services, le tout en un seul endroit.



Gérez l'ensemble de votre cybersécurité depuis la plateforme Sophos Central

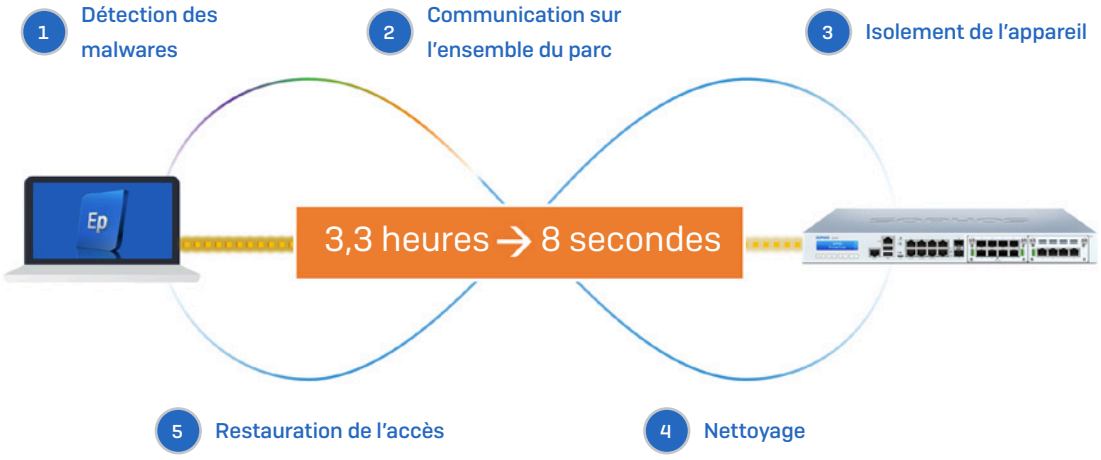
Automatiser votre protection

Sophos Central permet aux produits Sophos de partager activement des informations et de travailler en synergie et en temps réel pour répondre automatiquement aux incidents. Cette intégration et cette automatisation renforcent votre protection tout en réduisant la charge de travail de vos équipes IT.

Exemple 1 : Réponse automatisée aux incidents

- Si Sophos Intercept X identifie une menace sur un poste de travail, il notifie Sophos Firewall instantanément.
- Sophos Firewall isole automatiquement le système infecté du réseau, y compris des autres appareils sur le même LAN.
- Intercept X nettoie la menace et notifie Sophos Firewall une fois la tâche accomplie.
- Sophos Firewall rétablit immédiatement l'accès au réseau.

L'ensemble de ce processus, qui prend environ 3 h 30 manuellement, se déroule en moins de 8 secondes.

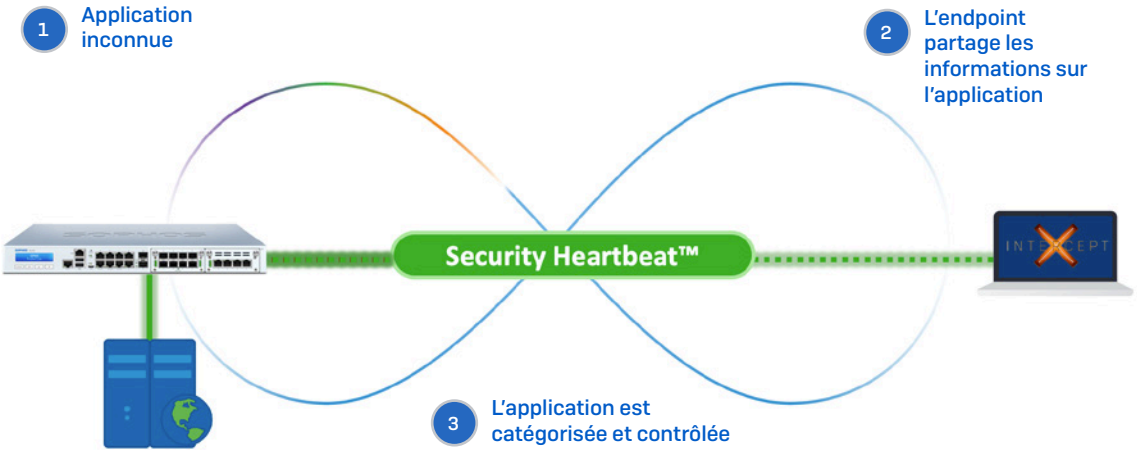


Automatisation de la réponse aux incidents

Exemple 2 : Identifier toutes les applications indésirables sur le réseau

En moyenne, 43 % du trafic réseau n'est pas identifié. Dans certains cas, ce sont des applications personnalisées qui n'ont pas de signature standard. Dans d'autres cas, c'est l'application elle-même qui dissimule son identité au pare-feu, car elle est mal intentionnée.

- Si Sophos Firewall repère une application qui ne correspond pas à une signature connue, au lieu de l'assigner à une catégorie de trafic générique telle que « HTTPS », il contacte Sophos Intercept X.
- Intercept X renvoie le nom de l'application, le correctif et la catégorie à Sophos Firewall pour classification. L'application est alors automatiquement assignée au groupe approprié.
- Si ce groupe applique des mesures de contrôle (tel que le blocage), ces mêmes règles sont appliquées à l'application. Si nécessaire, par exemple dans le cas d'applications personnalisées, l'administrateur peut définir manuellement une catégorie et une politique à appliquer.



Identification de toutes les applications et processus sur le réseau

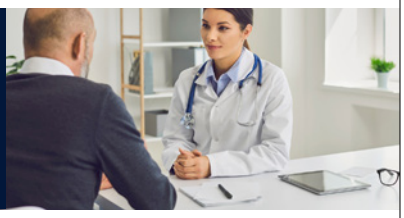
Réduire le coût total de possession dans les environnements réels

Les avantages d'un système de cybersécurité Sophos sont s'additionnent. Combiner les technologies Next-Gen, la réponse automatisée aux incidents, le partage en temps réel des informations et bénéficier d'une plateforme de gestion unifiée offre des avantages considérables, tant sur la protection que sur le coût total de possession (TCO).

Les clients qui utilisent Sophos Intercept X Endpoint et Sophos Firewall déclarent que, sans Sophos, ils devraient ***doubler leur effectif de sécurité pour maintenir le même niveau de protection****. Ils rapportent une réduction des incidents de sécurité allant jusqu'à 85 %.*

CUSTOMER CASE STUDY **HEALTHCARE PROVIDER, U.S.**

A regional healthcare provider whose services include inpatient and outpatient care, medical practices, nursing homes, and a range of specialist services.



Business impact of a Sophos cybersecurity ecosystem

50% reduction in IT security resource requirements
The customer has three employees dedicated to cybersecurity. They calculate they would, if they didn't use Sophos, need to employ three additional full-time security analysts solely to cover incident response.

90%-plus reduction in day-to-day cybersecurity workload
Prior to Sophos, reviewing logs and investigating areas of concern would take an entire day. Now they achieve the same level of confidence in just 30 minutes.

85% reduction in security incidents
Previously, they experienced three incidents each day on average. This has now dropped to an average of one every three days.

90%-plus reduction in time to investigate an incident
Before using Sophos, it took the team roughly three hours to thoroughly investigate an incident. This has now dropped to less than 15 minutes, with everything done remotely via the Sophos Central platform and without disrupting other users and impacting system availability.

CUSTOMER-AT-A-GLANCE

Number of users
4,500 employees

Sophos solutions
- Sophos XG Firewall
- Sophos Intercept X Advanced with EDR
- Sophos Intercept X for Server Protection (Windows, Linux, and virtual machines)

CUSTOMER CASE STUDY **CLINICAL TRIALS PROVIDER, U.S.**

A private sector organization that provides the clinical trial data needed to secure regulatory approval for new medications.

Business impact of a Sophos cybersecurity ecosystem

50% reduction in IT resource requirements
Currently, the customer spends one hour a day reviewing logs and investigating issues. They advise that they would need to hire one or two more security engineers just to manage the logs if they moved away from Sophos.

33% reduction in time to deal with a potential issue
Previously, to address a security issue with a device, they would reimage the machine, which took between 90 minutes and two hours. With Sophos, they can conduct a full investigation and remediate in approximately one hour – with no reimaging.

88% reduction in threat risk due to faster issue identification
Prior to using Sophos, it took a full day just to investigate the logs to find the issues. With Sophos, the IT team can identify new issues for investigation within minutes of a suspicious event arriving.

Improved user behavior
As users are aware that the IT team can now address issues quickly and without impacting work, they are far more willing to report issues or concerns.

CUSTOMER-AT-A-GLANCE

Number of users
150 employees across four locations

IT team
Two IT staff, covering all areas including cybersecurity

Sophos solutions
- Sophos XG Firewall
- Sophos Intercept X Advanced with EDR
- Sophos Device Encryption

Un sentiment de sécurité renforcé pour les soignants

Dans un environnement médical sous haute pression, les risques liés aux erreurs humaines seront toujours difficiles à éliminer et à contrôler. Sophos fournit un filet de sécurité vital pour que les soignants puissent travailler rapidement et plus sereinement.

Empêcher les menaces d'atteindre vos utilisateurs

Nous pouvons vous aider à alléger la pression sur vos utilisateurs — et par extension sur votre équipe informatique — en empêchant les menaces de les atteindre en tout premier lieu :

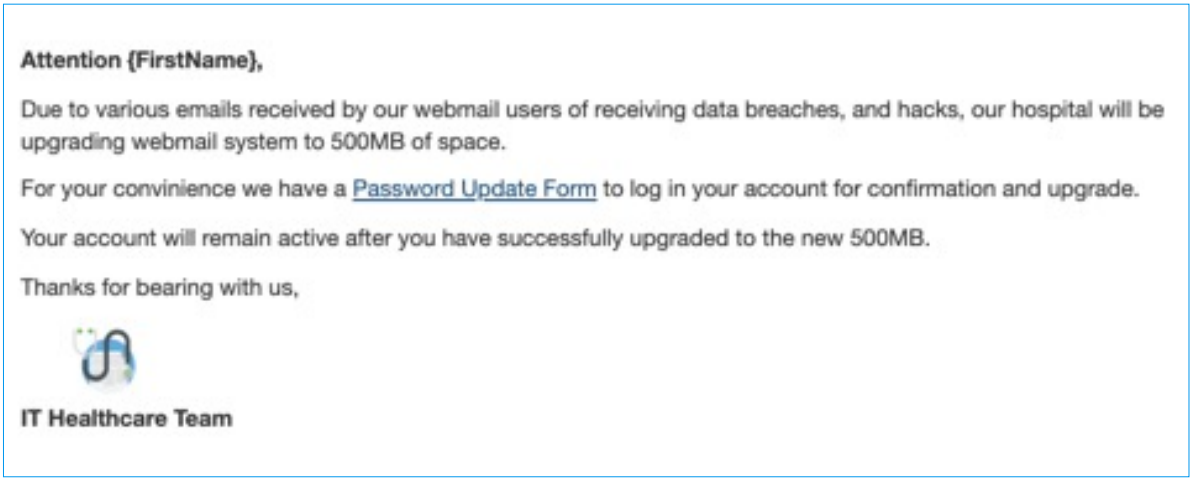
Intercept X with EDR combine des capacités anti-ransomware, la prévention des exploits et la détection basée sur l'IA pour bloquer les menaces en tout point de la chaîne d'attaque. Vos utilisateurs seront plus sereins en sachant qu'ils bénéficient de la meilleure protection Endpoint sur le marché.

Sophos Email protège de manière prédictive, grâce à l'IA, les messageries de vos utilisateurs. Il identifie les emails malveillants et les supprime automatiquement, avant même que les destinataires aient la possibilité de cliquer sur un lien suspect.

L'écosystème de cybersécurité Sophos permet aux produits Sophos de fonctionner ensemble pour répondre automatiquement aux menaces, en les bloquant et en les nettoyant en quelques secondes seulement.

Former vos utilisateurs à la détection des menaces

Sophos Phish Threat aide les utilisateurs à reconnaitre les emails malveillants grâce à une formation en ligne et à des simulations d'emails de phishing. Vous pouvez cibler la formation sur le personnel qui en a le plus besoin, soit par la nature de leur fonction, soit en raison de leurs performances lors des tests de simulation.



Attention {FirstName},

Due to various emails received by our webmail users of receiving data breaches, and hacks, our hospital will be upgrading webmail system to 500MB of space.

For your convinience we have a Password Update Form to log in your account for confirmation and upgrade.

Your account will remain active after you have successfully upgraded to the new 500MB.

Thanks for bearing with us,

IT Healthcare Team

Exemple de simulation d'un email de phishing dans Sophos Phish Threat

Implémentez une sécurité qui ne ralentit pas les soins de santé

Dans le secteur médical, plus que dans la plupart des autres secteurs, il est essentiel que les choses marchent vite et bien. C'est pourquoi de nombreux utilisateurs du secteur déploient des applications non approuvées pour faciliter leur travail. Ce phénomène expose votre réseau et vos données à des risques accrus. Sophos vous aide à lutter contre le Shadow IT sans gêner vos opérations quotidiennes.

Une protection avancée qui maintient la continuité des opérations

Intercept X with EDR sécurise vos systèmes d'extrémité et vos serveurs, et empêche les menaces de perturber vos utilisateurs. Les fonctionnalités EDR vous permettent d'interroger à distance les systèmes de vos utilisateurs et, si nécessaire, de les corriger.

Sophos Firewall protège votre réseau contre les menaces et permet de facilement donner la priorité au trafic réseau de confiance, garantissant ainsi la poursuite des processus critiques sans interruption. De plus, il vous offre une visibilité et un contrôle sur le Shadow IT, en permettant d'identifier et de bloquer les activités susceptibles de mettre votre organisation en danger.

Les produits Sophos sont excellents en soi, mais tout leur potentiel se révèle lorsqu'ils fonctionnent en synergie. Comme nous l'avons vu, Sophos Intercept X et Sophos Firewall travaillent ensemble pour répondre automatiquement aux menaces et améliorer votre visibilité.

Sécuriser les technologies héritées

L'un des défis rapportés par de nombreuses organisations du secteur est la nécessité de sécuriser les équipements hérités. Ces appareils utilisent souvent des systèmes d'exploitation obsolètes qui ne peuvent pas être mis à jour pour des raisons réglementaires, mais qui doivent être connectés au réseau. Si un appareil ne peut pas être patché ou mis à jour, et ne dispose pas d'une solution antivirus ou anti-malware prise en charge, vous devez envisager une solution physique.

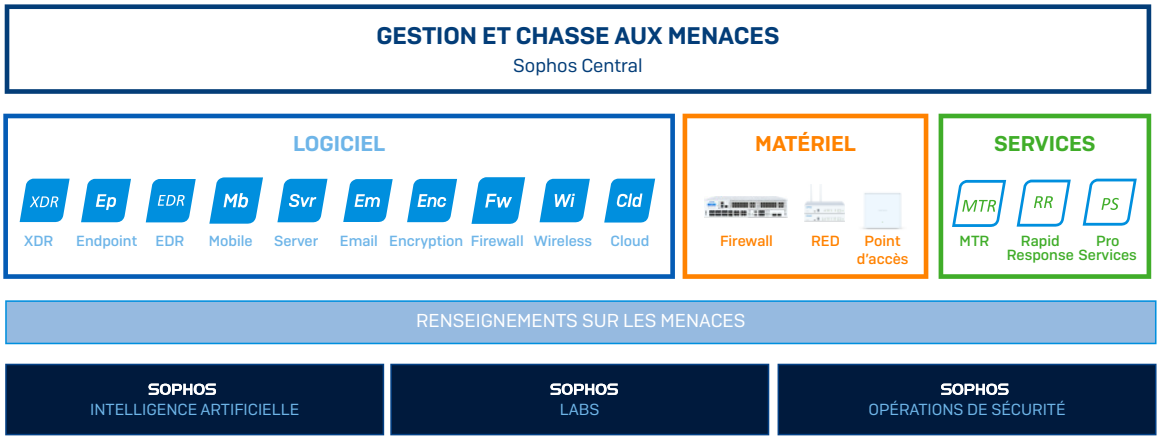
Sophos Firewall et **SD-RED** (Remote Ethernet Device) peuvent vous aider dans ce cas. En plaçant un boitier SD-RED « devant » l'appareil exposé, il peut diriger tout le trafic vers un pare-feu Sophos Firewall pour l'analyser. Si votre réseau est très plat, vous devrez probablement apporter quelques petites modifications aux schémas d'adresses IP, voire à la topologie des switchs. Nos spécialistes techniques pourront discuter de votre situation particulière et vous conseiller sur la manière de procéder.

Sécurisation des équipements hérités

Conclusion

Protéger les environnements informatiques du secteur de la santé et les données sensibles qu'ils détiennent nécessite une sécurité multi-couches. En implémentant une sécurité intelligente à chaque point vulnérable, des réseaux aux données, vous pouvez protéger vos systèmes, votre personnel et vos patients contre les risques internes et externes.

Toutes les solutions Sophos font partie de notre écosystème de cybersécurité adaptatif. Elles fonctionnent parfaitement seules — et de nombreuses organisations commencent avec un seul produit — mais elles sont encore plus efficaces ensemble. À mesure que vous développez votre protection Sophos, vous bénéficiez d'avantages accrus qui découlent de cet écosystème intégré : le partage des données, la gestion centralisée dans une console unique, la réponse automatisée, des informations plus approfondies… Tous ces éléments qui travaillent ensemble renforcent votre protection et améliorent l'efficacité de votre équipe informatique.



Protéger le secteur de la santé : l'écosystème de cybersécurité Sophos

Pour en savoir plus sur la façon dont Sophos sécurise les établissements de santé et pour discuter de vos besoins, contactez votre représentant Sophos ou demandez à être rappelé par l'un de nos spécialistes en sécurité.

Demandez à l'un de nos spécialistes de vous rappeler dès aujourd'hui !

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.

© Copyright 2021. 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 de sociétés mentionnés sont des marques ou des marques déposées appartenant à leurs propriétaires respectifs.

2021-05-05 (SB-NP)

SOPHOS