

A man and a woman, both wearing lanyards, are looking at a tablet together in what appears to be a server room. The man is on the left, and the woman is on the right, wearing glasses. The background shows server racks. The image is partially obscured by a white curved shape on the left side.

LIVRE BLANC

Bonnes pratiques pour protéger votre réseau contre les ransomwares

Renforcez votre protection contre les ransomwares et toute autre attaque réseau.

Les ransomwares restent une cybermenace majeure

Les ransomwares restent une menace très répandue, avec de graves conséquences financières, opérationnelles et humaines. En 2024, les ransomwares étaient à l'origine de 70 % des incidents traités par le service Sophos Incident Response dans les petites entreprises et de plus de 90 % dans les moyennes entreprises, ce qui souligne leur prédominance en tant que cybermenace la plus préoccupante à l'heure actuelle.¹ L'impact financier est considérable. Notre enquête annuelle sur l'état des ransomwares a révélé que le coût moyen de rétablissement après une attaque de ransomware s'élève désormais à 1,53 million de dollars, tandis que le montant moyen des rançons versées atteint 1 million de dollars². Au-delà de ces coûts, ces attaques entraînent de graves perturbations opérationnelles et ont des conséquences humaines très lourdes, allant d'une perte de productivité à un stress accru pour les équipes informatiques et de cybersécurité. Ces répercussions montrent bien l'ampleur de la menace et confirment qu'il est urgent de renforcer les défenses contre les ransomwares et de mettre en place des stratégies de récupération. Parallèlement à la protection Endpoint, une pile de sécurité réseau optimisée constitue l'une des défenses les plus efficaces contre les ransomwares. Utilisez ce guide pour explorer les mécanismes d'attaque des ransomwares, les stratégies de prévention et la façon dont vous pouvez optimiser votre réseau pour une sécurité maximale.

Mode opératoire des attaques de ransomware

Il existe de nombreux types d'acteurs malveillants et d'attaques de ransomware. Certaines campagnes sont très ciblées, tandis que d'autres sont purement opportunistes. Les adversaires, aussi appelés cybercriminels ou attaquants, déploient généralement toute une gamme de techniques pour infiltrer les organisations : exploitation de vulnérabilités, utilisation d'identifiants volé ou compromis, envoi d'emails malveillants et de phishing, attaque par force brute, téléchargement passif (drive-by) via des sites web compromis, pour citer les plus courants. Voici pour preuve les propos tenus par un gang de ransomwares ayant attaqué un établissement scolaire au Canada :

« Vous aviez une ancienne vulnérabilité critique Log4j non corrigée sur Horizon, c'est ainsi que nous avons pu pénétrer initialement. Il s'agissait d'un scan effectué en masse ; on ne vous visait pas spécialement. »

90 %

Pourcentage des cyberattaques ciblant les moyennes entreprises qui impliquaient un ransomware.

1,0 M\$

Montant moyen des rançons payées par les entreprises en 2025.

¹ Rapport annuel de Sophos sur les menaces : Cybercrime on Main Street 2025
² L'état des ransomwares 2025 - Sophos

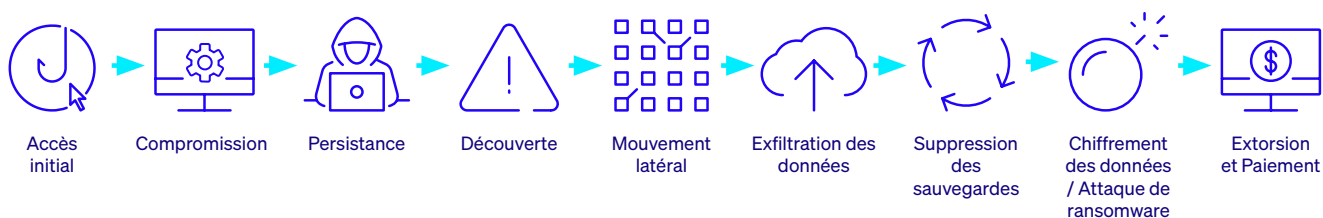
Ces propos mettent également en évidence l'exploitation courante par les attaquants de vulnérabilités non corrigées, qui a été la principale cause première des attaques de ransomware en 2025³.

La hausse des attaques de ransomware au cours des dernières années peut être attribuée en grande partie à l'essor du modèle RaaS ou Ransomware-as-a-Service. Depuis l'avènement du modèle RaaS, un groupe de cybercriminels peut créer un ransomware puis le louer à d'autres adversaires. Cela rend les ransomwares accessibles à un plus grand nombre d'acteurs malveillants que jamais. Tout au long de l'année 2024, les organismes chargés de l'application de la loi du monde entier ont tenté de perturber les activités des fournisseurs de ransomware-as-a-service. Mais à l'instar d'une hydre, dès qu'un groupe est démantelé, d'autres émergent immédiatement pour lui succéder⁴.

Dès lors que ces derniers accèdent à l'environnement de leurs victimes, ils passent alors plusieurs jours, plusieurs semaines, voire plusieurs mois à explorer le réseau, à élever leurs privilèges, à exfiltrer des données ou à installer des malwares. En 2024, le temps de séjour médian des attaques de ransomware était de quatre jours⁵ — un délai crucial, qui laisse aux défenseurs la possibilité d'identifier et d'expulser les intrus avant qu'ils ne mènent à bien leur attaque.

Cependant, quand ils ont des objectifs précis, les adversaires ne perdent pas de temps. En effet, ils cherchent souvent à découvrir le plus vite possible les serveurs Active Directory pour les compromettre, ce qui se produit généralement dans les 11 heures suivant la première intrusion⁶. Une fois le serveur Active Directory compromis, les attaquants peuvent obtenir des privilèges élevés et déployer des ransomwares et d'autres outils à partir d'une « source fiable ». Les attaquants recherchent également activement l'emplacement des sauvegardes. S'ils y parviennent, ils tenteront d'accéder au système, puis de supprimer et de désactiver le processus de sauvegarde juste avant de lancer l'attaque de ransomware. La raison est simple : une entreprise qui ne parvient pas à récupérer ses données à partir d'une sauvegarde sera plus susceptible de payer la rançon.

Mode opératoire classique d'une attaque de ransomware :



³ L'état des ransomwares 2025 - Sophos

⁴ Rapport annuel de Sophos sur les menaces : Cybercrime on Main Street 2025

⁵ Le rapport Active Adversary 2025 de Sophos

⁶ Le rapport Active Adversary 2025 de Sophos

Vulnérabilités exploitées

La principale cause des attaques de ransomware en 2025.

4 jours

Temps de séjour médian des attaques de ransomware.

« Protocole RDP » ou « Protocole de Déploiement de Ransomware » ?

Le RDP (Remote Desktop Protocol) a été utilisé dans 91 % des cyberattaques prises en charge par l'équipe de réponse aux incidents de Sophos en 2024⁷.

Le RDP et les outils de partage de bureau, tels que Virtual Network Computing (VNC), sont précieux pour gérer les systèmes à distance. Toutefois, sans mesures de protection adéquates, les adversaires sont susceptibles de les exploiter pour élever leurs privilèges, voler des identifiants, se déplacer latéralement, installer des portes dérobées, créer de faux comptes et échapper à la détection.

Il est donc essentiel d'empêcher les attaquants d'utiliser le RDP pour les accès externes et internes, et les mouvements latéraux. Malgré les progrès réalisés par les entreprises pour s'assurer que le RDP n'est pas exposé vers l'extérieur, les adversaires continuent d'utiliser ce protocole pour se déplacer sur le réseau de l'entreprise.

Utilisation de l'IA par les attaquants

Les adversaires ont commencé à utiliser l'IA générative pour créer des emails de spam et de phishing. Les grands modèles linguistiques (LLM), tels que ChatGPT, peuvent être exploités pour générer du contenu grammaticalement correct et adapté spécifiquement à chaque cible, contournant ainsi les filtres de contenu qui utilisent des signatures virales pour détecter les spams et les attaques de phishing. Ce type de contenu convaincant généré par l'IA permet de piéger l'utilisateur et de l'inciter à cliquer sur un lien qui le redirige vers un site web malveillant dans le but de récupérer ses identifiants. Fort de ces données, l'adversaire peut ensuite accéder à votre environnement en se faisant passer pour un utilisateur légitime.

91 %

Pourcentage de cyberattaques impliquant le RDP.

⁷ Le rapport Active Adversary 2025 de Sophos

Bonnes pratiques pour protéger votre réseau contre les ransomwares

Maintenant que nous avons fait un rapide tour d'horizon du fonctionnement des attaques de ransomware et des acteurs malveillants, voici trois bonnes pratiques pour renforcer les défenses de sécurité de votre réseau :

1. Réduisez votre exposition, c'est-à-dire votre surface d'attaque.
2. Inspectez et protégez le trafic réseau lorsqu'il entre dans votre réseau.
3. Identifiez et bloquez toutes les menaces qui parviennent à s'introduire dans le réseau.

Réduisez votre exposition, c'est-à-dire votre surface d'attaque

Toute infrastructure réseau exposée à l'Internet public devient par nature une cible potentielle pour les attaquants. Par conséquent, la première bonne pratique consiste à minimiser cette exposition autant que possible. Nous vous recommandons fortement de :

1. Consolider votre infrastructure réseau

La plupart des entreprises disposent d'un pare-feu protégeant leur réseau. Beaucoup disposent également d'un concentrateur VPN ou de passerelles réseau supplémentaires. Réduisez cette infrastructure autant que possible. Évoluez vers un pare-feu qui intègre l'accès à distance et qui remplace au minimum tout concentrateur VPN que vous utilisez, mais qui vous permette idéalement de passer à l'accès réseau Zero Trust (ZTNA). Vous trouverez plus d'informations à ce sujet dans la suite de ce document.

2. Corriger le firmware et le maintenir à jour

Les vulnérabilités non corrigées ont été la principale cause des attaques de ransomware en 2024⁸. C'est pourquoi il est essentiel de maintenir votre pare-feu et tout autre firmware de votre infrastructure à jour. Vérifiez régulièrement (au moins une fois par mois) si des mises à jour de firmware sont disponibles et programmez leur application à des moments opportuns. Assurez-vous que votre fournisseur de pare-feu est en mesure d'appliquer automatiquement des correctifs à distance qui ne nécessitent pas d'interruption de service pour les correctifs de sécurité importants.

⁸ L'état des ransomwares 2025

Les fonctionnalités clés à rechercher au moment de choisir un pare-feu :

- Pas d'accès Internet prêt à l'emploi
- Sécurité dès la conception (Secure by design)
- Correctifs et mises à jour automatiques
- Accès à la surveillance côté fournisseur

Le saviez-vous ?

Même si toutes les attaques de ransomware réussies ont des conséquences négatives, celles qui commencent par l'exploitation de vulnérabilités non corrigées sont particulièrement agressives. En 2024, les organisations touchées par des attaques de ransomware ayant commencé de cette manière ont signalé des coûts de rétablissement 4 fois plus élevés et des délais de rétablissement plus longs par rapport à celles ayant commencé avec des identifiants compromis⁹.

3. Veiller à ce que votre infrastructure réseau soit sécurisée dès sa conception

Veillez à ce que tous les produits d'infrastructure réseau exposés à Internet, tels que votre pare-feu, soient sécurisés dès leur conception. Optez pour un pare-feu spécialement conçu et renforcé pour résister aux attaques. Les principales caractéristiques à rechercher sont les suivantes :

- Pas d'accès à Internet par défaut : le pare-feu ne doit pas proposer d'accès à Internet par défaut et doit offrir des contrôles d'accès granulaires pour gérer ce qui est exposé.
- Conception renforcée : elle doit intégrer des mécanismes de sécurité tels que l'authentification multifacteur (MFA) et la conteneurisation de tout service ou portail exposé, empêchant ainsi les attaquants d'exploiter les vulnérabilités potentielles.
- Correctifs automatisés : Comme mentionné ci-dessus, les correctifs automatisés sont fondamentaux. Pour faire face aux menaces émergentes, le pare-feu doit être capable de recevoir des mises à jour rapidement, sans nécessiter de mises à jour majeures du firmware ni avoir à planifier de temps d'arrêt.
- Surveillance proactive : La surveillance par l'éditeur de l'ensemble de sa base de clients déployée peut permettre d'identifier les attaques et d'y répondre beaucoup plus rapidement.

4. Minimiser l'exposition des serveurs et des applications à Internet

Si vous utilisez des outils de bureau à distance (RDP ou VNC) ou si un système de votre réseau est directement accessible via Internet pour la gestion à distance, désactivez immédiatement cet accès. Comme nous l'avons mentionné, ce type d'exposition est l'un des principaux moyens utilisés par les attaquants pour entrer dans les réseaux. Examinez les règles NAT de votre pare-feu et assurez-vous qu'aucun élément n'est exposé. Utilisez une solution ZTNA pour protéger vos serveurs et vos systèmes admin et les rendre invisibles aux attaquants tout en fournissant un accès à distance sécurisé à ceux qui en ont besoin.

⁹ Vulnérabilités non corrigées : le vecteur d'attaque de ransomware le plus agressif - Sophos

5. Remplacer le VPN d'accès à distance par le ZTNA

Le modèle d'accès réseau Zero Trust, ou ZTNA (Zero Trust Network Access), remplace aujourd'hui le VPN d'accès à distance. Il élimine la confiance inhérente et l'accès large qu'offre le VPN, en utilisant plutôt les principes du Zero Trust (confiance zéro) : « ne faites confiance à rien ni personne, vérifiez tout ». Le ZTNA améliore la sécurité, facilite la gestion et procure une meilleure visibilité et une meilleure expérience utilisateur que le VPN d'accès à distance.

Il élimine les clients VPN vulnérables, s'appuie sur l'authentification multifacteur (MFA) et l'intégrité de l'appareil pour contrôler les accès. Et il ne donne accès qu'à des applications réseau spécifiques, permettant ainsi de micro-segmenter votre réseau. Recherchez un pare-feu qui intègre le ZTNA afin d'obtenir une solution de passerelle unique — gérée depuis une console unique, et idéalement avec un agent unique sur l'appareil de l'utilisateur qui combine protection Endpoint et ZTNA.

6. Activez la MFA et les clés d'accès, et utilisez des mots de passe complexes.

La MFA ajoute une couche de protection essentielle au-delà du mot de passe, bloquant les adversaires qui s'appuient sur des identifiants volés ou achetés. Activez la MFA sur toutes les applications et tous les services, et lorsque cela est possible, utilisez des clés d'accès résistantes au phishing.

Les clés d'accès remplacent les mots de passe par des clés cryptographiques associées à l'appareil, vérifiées par des données biométriques ou un code PIN sécurisé, ce qui rend les comptes plus difficiles à compromettre et plus faciles d'accès pour les utilisateurs.

Si la MFA et les clés d'accès ne sont pas disponibles, assurez-vous d'utiliser des mots de passe robustes et uniques. Un mot de passe faible et prévisible peut permettre aux attaquants d'accéder à votre réseau en quelques secondes. Choisissez toujours des mots de passe uniques d'au moins 12 caractères, qui combinent lettres majuscules et minuscules, chiffres et symboles, comme « Ju5te.C0mM3çA!». Vous pouvez également envisager d'utiliser une phrase de passe composée de mots sans rapport entre eux ou faciles à mémoriser, comme « PurpleMountainRace37! ».

Plus important encore, ne réutilisez jamais le même mot de passe sur différents sites web, connexions ou appareils. L'utilisation d'identifiants uniques permet de limiter les dégâts en cas de compromission.

Inspectez votre trafic réseau et protégez-le dès son entrée dans votre réseau

Autre vecteur d'attaque couramment utilisé par les adversaires : s'implanter sur votre réseau par le biais du trafic web et de messagerie quotidien qui traverse votre infrastructure. Si les outils web et de messagerie sont essentiels pour toute entreprise et ne peuvent être tout bonnement isolés, il est toutefois possible de s'assurer que ce trafic est inspecté et protégé de manière adéquate. Voici quelques bonnes pratiques recommandées pour sécuriser le trafic de votre réseau :

1. Inspecter le trafic chiffré

Plus de 90 % du trafic réseau est chiffré. C'est une bonne chose pour le respect de la confidentialité, mais c'est aussi un défi pour la sécurité, car la détection des menaces classique ne peut pas voir à l'intérieur des flux de trafic chiffrés. Les attaquants profitent de cet angle mort de la sécurité. La plupart des pare-feux peineront sous la charge supplémentaire que représente le déchiffrement et l'inspection de ces 90 % de trafic chiffré. Choisissez un pare-feu spécialement adapté au monde fortement chiffré d'aujourd'hui, qui est capable de déterminer intelligemment les flux de trafic qui nécessitent un déchiffrement et ceux qui n'en ont pas besoin. Il doit déchiffrer et inspecter efficacement le trafic sans compromettre les performances globales du réseau, tout en étant capable d'identifier les menaces chiffrées. Mieux encore, procurez-vous un pare-feu qui n'a pas besoin de déchiffrer le trafic pour détecter les menaces chiffrées.

2. Utiliser un système de prévention des intrusions (IPS)

De nombreux systèmes de votre réseau peuvent présenter des vulnérabilités non corrigées. Il peut s'agir de systèmes Windows ou Linux, d'appareils connectés (IoT) comme des caméras, de systèmes de contrôle industriel, ou de tout ce qui se connecte à votre réseau — avec ou sans fil. Chaque pare-feu comprend une technologie permettant de détecter les attaques réseau qui tentent d'exploiter les vulnérabilités : c'est ce qu'on appelle un système de prévention des intrusions ou IPS. Malheureusement, de nombreuses organisations ne l'utilisent tout simplement pas. Assurez-vous d'utiliser un IPS sur tous les flux de trafic de votre réseau, en particulier ceux qui proviennent d'Internet, mais aussi en interne pour détecter les attaquants potentiels qui peuvent déjà se trouver sur votre réseau.

3. Utiliser une protection contre les menaces zero-day

De nombreuses attaques utilisent des logiciels malveillants incorporés dans des fichiers que des utilisateurs vont télécharger à leur insu sur le web. Ces menaces inédites sont appelées « zero-day ». Vous ne pouvez pas compter sur l'analyse antivirus traditionnelle pour détecter ce type de menaces. Vous avez besoin d'une analyse des menaces qui exploite l'IA ou le Machine Learning formés sur des millions d'échantillons afin d'identifier les menaces nouvelles et émergentes.

90 %

Le volume du trafic réseau chiffré, source de difficultés pour les équipes chargées de la sécurité.

Assurez-vous que l'inspection de votre pare-feu inclut l'analyse zero-day. Idéalement, elle devrait être effectuée en temps réel dans le Cloud pour décharger votre pare-feu de ce traitement intensif et pour bénéficier instantanément du partage mondial des renseignements sur les menaces.

4. Implémenter des mesures de sécurité robustes pour la messagerie et apprendre aux utilisateurs à repérer les emails de phishing

Nous connaissons tous quelqu'un qui a un jour cliqué sans le savoir sur un lien malveillant dans un email qui semblait légitime. Bien que cela reste un vecteur d'attaque populaire pour les cybercriminels, il existe des protections efficaces et des mesures éducatives pour lutter contre ce problème.

Recherchez une solution de sécurité des messageries capable de filtrer de manière proactive les emails malveillants des boîtes de réception des utilisateurs. Même si certains emails parviennent à passer, la solution doit permettre de les supprimer rétroactivement ou de réécrire les URL pour permettre des vérifications au moment du clic. Recherchez un produit de sécurité des messageries qui inclut des fonctions permettant de tester la capacité des utilisateurs à reconnaître les attaques de phishing et qui propose une formation sur les éléments à surveiller.

Identifiez et bloquez toutes les menaces qui parviennent à s'introduire dans le réseau

Malgré tous vos efforts, il est prudent de partir du principe qu'un jour ou l'autre, un attaquant s'introduira dans votre réseau. C'est là que l'identification et le temps de réponse deviennent critiques, et pourtant, c'est là que la plupart des solutions de sécurité réseau laissent à désirer. Vous devriez rechercher des solutions qui peuvent vous aider à :

1. Segmenter votre réseau

Si un attaquant parvient à pénétrer votre réseau, l'une des choses qu'il cherchera à faire sera de se déplacer. Pour limiter tout mouvement et détecter un attaquant le plus tôt possible, il vous faudra micro-segmenter votre réseau. Assurez-vous que votre réseau est segmenté en plusieurs zones réduites ou VLAN qui sont connectés via des switchs et des points d'accès gérés, et via votre pare-feu où l'IPS inspecte ce flux de trafic. Utilisez également le ZTNA pour l'accès à distance pour micro-segmenter efficacement vos applications.

88 %

Le pourcentage d'attaques de ransomware qui se produisent en dehors des heures de bureau.

2. Identifier instantanément les adversaires à travers de multiples vecteurs

Lorsqu'un attaquant s'introduit dans votre réseau, une détection rapide est essentielle. Sachant que 88 % des attaques de ransomware se produisent en dehors des heures de bureau classiques¹⁰, vous avez besoin d'une solution de cybersécurité qui fonctionne 24 h/24 pour détecter les adversaires en temps réel et partager immédiatement les renseignements sur les menaces. Cette capacité doit faire plus que simplement alerter les administrateurs, elle doit permettre une communication transparente entre tous les produits de sécurité afin de garantir une réponse et un confinement rapides et coordonnés. Optez pour une suite de solutions entièrement intégrées, comprenant des pare-feux, des solutions Endpoint, des switches, des réseaux sans fil, le ZTNA et la sécurité des messageries. Veillez également à ce que votre pare-feu intègre la fonctionnalité NDR (Network Detection and Response). Ces outils doivent pouvoir partager des renseignements sur les menaces avec votre équipe de sécurité mais aussi entre eux, afin de mettre en œuvre des réponses automatisées pour neutraliser les attaques, même au plein milieu de la nuit.

3. S'adapter et répondre automatiquement aux menaces actives

Lorsqu'une menace est détectée — que ce soit par vous, un analyste de sécurité, vos postes, votre pare-feu ou tout autre élément de votre système de cybersécurité — vous avez besoin d'une réponse immédiate et coordonnée pour la contenir et la neutraliser. Pour y parvenir, choisissez un pare-feu (et des solutions de sécurité intégrées) capable de :

- **Répondre automatiquement aux menaces actives** sans intervention manuelle, en contenant l'attaque dès sa découverte.
- **Bloquer les menaces de manière dynamique** sans nécessiter de nouvelles règles de pare-feu ou l'intervention d'un administrateur.
- **Travailler en toute transparence avec d'autres outils de sécurité**, tels que des solutions Endpoint ou ZTNA, garantissant une défense coordonnée qui empêche les mouvements latéraux et isole la menace.

Utilisez plusieurs couches de technologies de sécurité pour vous protéger contre les ransomwares

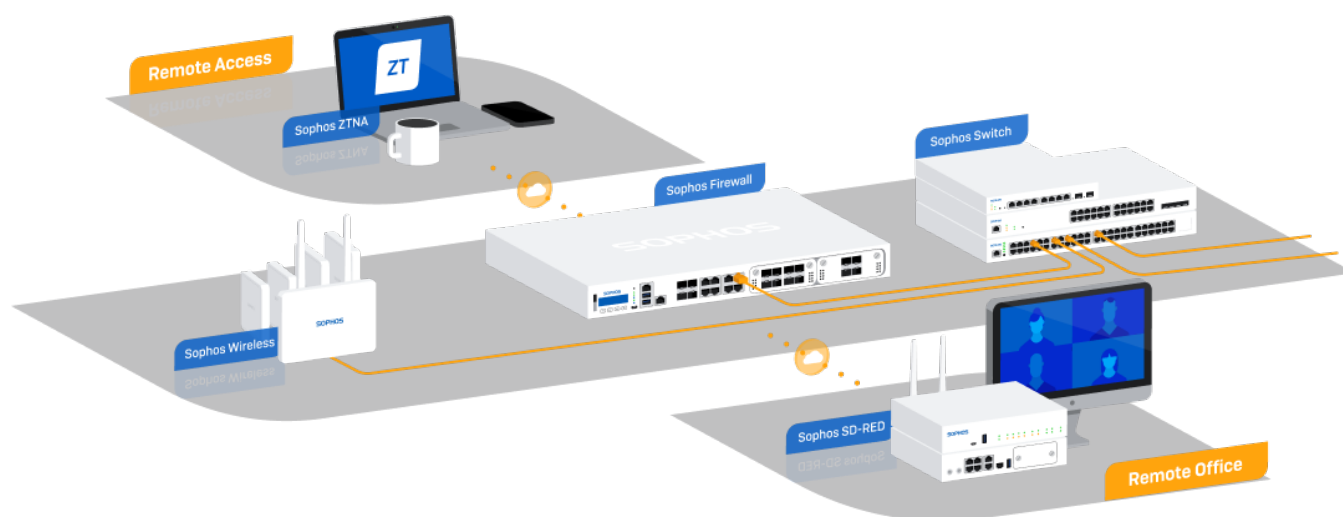
Comme le dit le proverbe : « mieux vaut prévenir que guérir ». Il est bien plus facile de stopper les problèmes à un stade précoce que de réparer les dégâts ultérieurement. La protection de votre organisation contre les ransomwares bénéficie d'une approche de sécurité informatique en couches, où plusieurs technologies travaillent ensemble pour créer une défense et une visibilité. En commençant par un pare-feu et une protection Endpoint, les organisations peuvent ajouter des couches supplémentaires en fonction de l'évolution des besoins, renforçant ainsi la protection et la visibilité au fil du temps.

Par exemple :

- **Un produit NDR (Network Detection and Response)** permet de détecter les appareils non protégés et d'identifier les adversaires qui se déplacent latéralement sur votre réseau. La solution NDR offre une visibilité sur le trafic du réseau interne que les pare-feux ne peuvent pas voir. Assurez-vous que votre prochain pare-feu intègre ce type de fonctionnalités.
- **Une plateforme XDR (Extended Detection and Response)** peut fournir des capacités de chasse aux menaces, d'investigation et de neutralisation. Elle peut également s'intégrer à vos autres solutions de sécurité informatique, offrant ainsi une visibilité sur l'ensemble des contrôles de sécurité à partir d'une plateforme unique.
- **Un service MDR** offre une surveillance 24/7 et une chasse aux menaces orchestrée par des experts spécialisés dans la détection et la réponse aux cyberattaques, que les solutions technologiques à elles seules ne peuvent pas prévenir. Votre service MDR doit offrir une réponse complète aux incidents pour intercepter, contenir et éliminer complètement les adversaires sans coûts supplémentaires. Un service MDR doit s'intégrer à vos outils de cybersécurité existants pour offrir une visibilité complète sur l'ensemble de votre environnement. Il offre également le plus haut niveau de protection contre les attaques de ransomware pilotées par des humains.
- **Une solution de gestion de la surface d'attaque (EASM/IASM) ou de gestion des vulnérabilités (VM)** peut être utilisée pour identifier et prioriser les vulnérabilités. Cela vous permet d'identifier et d'appliquer les correctifs manquants avant que les adversaires ne puissent les exploiter.
- **Une solution ITDR (Identity Threat Detection and Response)** peut être utilisée pour repérer les erreurs de configuration et les politiques de sécurité faibles dans les systèmes de gestion d'identité, de même que pour réaliser une veille sur le Dark Web pour identifier les identifiants volés ou fuités et qui pourraient être utilisés par des attaquants.
- **Les services de tests de sécurité proactifs**, comme les tests d'intrusion, évaluent les contrôles et les politiques comme le ferait un attaquant, ce qui aide à repérer les failles dans votre environnement, à renforcer vos défenses et à améliorer votre résilience.

Sophos protège votre réseau contre les ransomwares

Sophos fournit tout ce dont vous avez besoin pour sécuriser votre réseau contre les ransomwares et toute autre attaque. Avec Sophos, vous bénéficiez d'une pile de cybersécurité intégrée qui comprend des solutions de pare-feu, ZTNA, switch, sans fil, RED (Remote Edge Device), une protection de la messagerie et une protection Endpoint Next-Gen pour tous vos appareils et serveurs.



Et tout est géré à partir d'une seule plateforme de gestion dans le Cloud : Sophos Central, qui rassemble les informations sur les menaces provenant de nos solutions et de nos experts, pour une réponse aux menaces automatique.

Ce niveau d'intégration et de synchronisation est unique à Sophos, vous ne le trouverez nulle part ailleurs, et c'est sans doute le composant le plus critique de toute réponse à une attaque active.

La Sécurité Synchronisée en action

Lorsqu'un hôte compromis est détecté, Sophos Firewall l'isole immédiatement tandis que vos postes sains gérés par Sophos ignorent automatiquement le trafic provenant de cet appareil. De plus, vos Switch et points d'accès abandonneront les paquets provenant de l'hôte compromis, et Sophos ZTNA empêchera tout appareil compromis de se connecter à vos appareils. Une menace active est immédiatement et automatiquement isolée sur le réseau, et n'aura nulle part où aller.

Aperçu de la sécurité réseau de Sophos

Sophos Firewall

Sophos Firewall et les appliances de la série XGS vous aident à protéger votre réseau contre les ransomwares en implémentant de bonnes pratiques dès le départ :

- **La sécurité dès la conception (Secure by design) :** Non seulement nous avons investi massivement pour que Sophos Firewall soit le pare-feu le plus sécurisé sur le marché, mais nous travaillons sans relâche pour en faire une cible des plus difficiles à atteindre pour les cybercriminels, tout en protégeant votre réseau et votre organisation contre les attaques futures grâce à une surveillance proactive. Sophos Firewall est sans équivalent sur le marché, car il fournit automatiquement des correctifs de sécurité à distance qui ne nécessitent aucune interruption de service.
- **ZTNA intégré :** Sophos Firewall comprend une passerelle ZTNA intégrée, qui vous permet d'évoluer aisément du VPN traditionnel vers le Zero Trust sans avoir à déployer quoi que ce soit de plus. En outre, la solution ZTNA est gérée depuis la même console Cloud que votre pare-feu, pour faciliter la sécurisation et la segmentation de vos applications et de vos accès à distance.
- **Protection contre les menaces zero-day optimisée par IA :** Sophos Firewall intègre des technologies d'IA avancées pour identifier les attaques de ransomwares sophistiquées et les bloquer avant qu'elles n'entrent dans votre réseau. Nous utilisons une combinaison d'IA avancée et de Machine Learning qui ont été entraînés sur des millions d'échantillons, ainsi qu'une technologie de sandboxing en temps réel pour identifier des menaces inédites.
- **NDR intégré :** Sophos Firewall intègre des fonctionnalités NDR, une première dans le secteur. Et mieux encore, toutes les analyses complexes par IA sont effectuées dans le Cloud plutôt que sur votre pare-feu, ce qui améliore la détection des attaques actives sans pour autant impacter vos performances.
- **Réponse active aux menaces :** Sophos Firewall peut identifier instantanément un adversaire actif sur le réseau en se basant sur diverses sources de renseignements sur les menaces et coordonner une réponse aux menaces synchronisée afin d'isoler automatiquement une menace active avant qu'elle ne devienne un véritable problème.

Sophos ZTNA

Sophos ZTNA connecte de manière transparente vos utilisateurs aux applications et aux systèmes dont ils ont besoin pour faire leur travail, tout en offrant une segmentation, une sécurité et une visibilité accrues par rapport aux VPN d'accès à distance traditionnels.

- **Micro-segmentez et sécurisez vos applications :** Sophos ZTNA fournit une micro-segmentation de pointe pour offrir un accès sécurisé aux applications — qu'elles soient hébergées sur site, dans un datacenter ou dans votre infrastructure de Cloud public — en les rendant invisibles au monde extérieur.
- **Bloquez les ransomwares et autres menaces :** Avec le ZTNA, les ransomwares et autres menaces ne peuvent plus se propager sur le réseau à partir d'un appareil utilisateur compromis. Les utilisateurs et les appareils ne disposent que d'un accès explicite, basé sur des politiques de sécurité, à des applications spécifiques. Cela élimine le problème de confiance implicite et d'accès large au réseau inhérent au VPN.
- **Bloquez l'accès aux appareils compromis :** Sophos ZTNA permet à vos travailleurs distants d'accéder de manière sécurisée et transparente aux applications et aux données dont ils ont besoin. Si l'appareil d'un utilisateur est compromis, son accès aux applications sera automatiquement coupé pour empêcher les mouvements latéraux, et ce jusqu'à ce qu'il soit nettoyé.

Sophos Switch et points d'accès sans fil

Sophos Switch et les points d'accès Sophos sont étroitement intégrés à Sophos Firewall et au reste de la plateforme de cybersécurité Sophos, offrant une réponse aux menaces automatisée et une gestion à partir d'une console unique :

- **Réponse active aux menaces :** Sophos Switch et les points d'accès Sophos prennent également en charge la réponse active aux menaces (Active Threat Response) pour stopper net les adversaires actifs. Un appareil compromis peut être instantanément bloqué au niveau du switch ou du point d'accès pour empêcher les mouvements latéraux, même sur le même segment de LAN.
- **Console de gestion unique :** Sophos Switch et les points d'accès Sophos sont tous gérés à partir de Sophos Central, tout comme vos pare-feux, ZTNA et d'autres solutions Sophos, afin d'offrir une visibilité optimale et une gestion aisée.

Sophos Email

Sophos Email est une solution complète de sécurité des messageries qui protège contre les attaques de phishing et la compromission de la messagerie professionnelle (BEC) :

- **Protection contre les attaques de phishing et les attaques BEC** : Sophos Email se fonde sur le traitement du langage naturel (NLP) et l'analyse comportementale pour détecter les tentatives de phishing et supprimer les emails malveillants. Cette solution renforce davantage la sécurité des boîtes de réception en analysant de manière proactive les comportements suspects des expéditeurs, les anomalies dans les en-têtes et les tentatives d'usurpation d'identité à l'aide des validations SPF, DKIM et DMARC.
- **Protection des URL Time-of-Click et contrôle antimalware** : L'analyse multicouche des logiciels et des URL malveillants protège les utilisateurs contre les menaces liées aux emails. La protection Time-of-Click valide les URL au moment où l'utilisateur clique dessus, plutôt qu'au moment où l'email est reçu, pour mieux protéger contre les menaces en constante évolution. De plus, les charges utiles malveillantes intégrées dans les pièces jointes ou les liens sont détectées et bloquées avant qu'ils ne soient en mesure de causer des dommages.
- **Sensibilisation et formation à la sécurité** : Sophos Phish Threat est une plateforme de simulation d'attaques de phishing et de formation à la cybersécurité qui facilite l'identification des utilisateurs à risque et renforce la sensibilisation à la sécurité grâce à des simulations d'attaques de phishing et à des indicateurs de performance exploitables.



Conclusion

Les ransomwares continuent d'évoluer et sont toujours aussi efficaces pour forcer les organisations touchées à payer une rançon. Votre objectif est d'empêcher les adversaires de pénétrer dans votre organisation, et de les détecter et de les éjecter rapidement s'ils y parviennent. Veillez à suivre les bonnes pratiques de sécurité réseau décrites dans le présent rapport, assurez la formation continue des utilisateurs et restez vigilant face aux menaces et aux adversaires présents dans votre environnement.

Une approche multicouche de la cybersécurité, avec une détection et une réponse 24/7, donne à votre organisation les meilleures chances de se protéger contre les ransomwares et les menaces les plus récentes.

Pour découvrir comment Sophos peut vous aider à optimiser vos défenses contre les ransomwares, contactez un conseiller ou visitez le site www.sophos.fr.

Êtes-vous prêt à évaluer votre programme de cybersécurité ?

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

Sophos France

Tél. : +33 134 34 80 00

Email : info@sophos.fr