SOPHOS
Cybersecurity delivered.

Les principaux contrôles anti-ransomwares et comment Sophos peut vous aider

La lutte contre les ransomwares ne cesse de s'intensifier. La proportion d'organisations touchées par un ransomware a presque doublé en 12 mois, passant de 37 % en 2020 à 66 % en 2021. Les adversaires parviennent également de plus en plus souvent à chiffrer des données, avec 65 % des attaques ayant abouti au chiffrement de données en 2021*.

Pour réussir à bloquer les ransomwares, il faut prévenir à la fois les attaques sophistiquées manuelles, exécutées par des adversaires expérimentés, et les modèles d'attaques Ransomware-as-a-Service dont la popularité s'accroît chaque jour, étendant considérablement la portée des ransomwares en réduisant le niveau de compétence requis pour déployer une attaque.

Ce guide passe en revue les principaux contrôles de cybersécurité qui réduisent l'exposition et l'impact des ransomwares et la manière dont Sophos peut vous aider.

Une présentation des solutions Sophos. Avril 2022

CYBER CONTRÔLE	COMMENT SOPHOS PEUT VOUS AIDER	DÉTAILS
Chasse aux menaces proactive pour détecter et neutraliser les attaques manuelles avant le déploiement du ransomware	Sophos XDR (Extended Detection and Response)	Permet aux organisations de chasser les menaces et de les neutraliser au travers de l'ensemble de leur environnement. Les détections peuvent provenir des postes, des serveurs, des charges de travail Cloud, du pare-feu, de la messagerie, des environnements de Cloud public, des mobiles, de Microsoft 365, etc.
	Sophos MTR (Managed Threat Response)	Service managé de chasse aux menaces, de détection et de réponse fourni par une équipe d'experts Sophos disponible 24 h/24, 7 j/7 et 365 j/an. Des connecteurs intégrés à une gamme de solutions informatiques et de sécurité (y compris Microsoft 365) étendent la visibilité de nos opérateurs sur l'ensemble du parc informatique du client, ce qui augmente les capacités à se défendre contre les attaques.
Blocage automatique des ransomwares avant qu'ils ne puissent se déployer	Sophos Endpoint et Sophos Workload Protection	Offre des capacités avancées de protection contre les ransomwares qui neutralisent l'ensemble de la chaîne d'attaque, notamment : › Le Deep Learning de l'intelligence artificielle pour prévenir à la fois les ransomwares connus et inconnus. › La protection anti-exploit qui bloque les exploits et les techniques utilisées pour distribuer les malwares, voler les identifiants et échapper à la détection. › Le contrôle des applications, pour empêcher l'exécution d'applications sur les charges de travail Cloud, qui pourraient être exploitées par les attaquants afin de propager des attaques. › Le verrouillage du serveur, qui prend une configuration des charges de travail Cloud connue et sûre, et verrouille cet état afin d'empêcher l'exécution de programmes non autorisés. › La technologie anti-ransomware, qui détecte et annule le chiffrement non autorisé, en stoppant les processus avant qu'ils ne puissent se propager sur votre réseau. Protège à la fois contre les ransomwares ciblant les fichiers et ceux ciblant le secteur de démarrage principal (MBR).
	Sophos Email	Analyse automatiquement tous les processus de fichiers, l'activité des fichiers, l'activité du registre et les connexions réseau pour bloquer les ransomwares et d'autres formes de malwares. La protection avancée contre le phishing, l'analyse des URL et la protection post-livraison garantissent que seuls les expéditeurs sûrs atteignent votre boîte de réception. Si l'état de menace des emails livrés change, ils sont automatiquement supprimés.
	Sophos Firewall	Protège contre les sites compromis et les téléchargements malveillants grâce à l'inspection renforcée du Machine Learning et de la technologie de sandboxing afin d'identifier même les attaques de ransomware inédites.

CYBER CONTRÔLE	COMMENT SOPHOS PEUT VOUS AIDER	DÉTAILS
Identifie et comble les failles de sécurité pour durcir votre environnement, par exemple les appareils non corrigés, les machines non protégées, etc.	Sophos XDR (Extended Detection and Response)	Identifie les logiciels et systèmes obsolètes et non pris en charge. Permet d'accéder à toutes les applications de l'appareil, aux informations sur la version, aux hachages de fichiers SHA256, aux informations sur les correctifs et à leurs journaux, y compris l'historique d'exécution des applications, les connexions réseau, les processus parents/enfants, etc. Comprend des requêtes pour vérifier les applications installées par rapport aux informations sur les vulnérabilités en ligne, et des requêtes pour identifier les faiblesses de la posture de sécurité dans les paramètres du registre.
	Sophos ZTNA	Permet un accès à distance sécurisé et granulaire aux systèmes et aux applications, en éliminant la surface d'attaque et le potentiel de déplacement latéral des attaques.
Verrouille le protocole RDP (Remote Desktop Protocole) pour empêcher les adversaires de l'utiliser pour obtenir un accès	Sophos Firewall	Permet aux équipes informatiques de gérer et de verrouiller facilement le RDP.
	Sophos ZTNA	Permet un accès distant sécurisé au RDP et à d'autres applications sans exposer ces systèmes à des attaques.
	Sophos Cloud Optix	Identifie de manière proactive les ports RDP exposés via des évaluations de référence en matière de sécurité du Cloud public. Des mesures correctives guidées indiquent aux administrateurs comment corriger ces erreurs de configuration.
	Sophos XDR (Extended Detection and Response)	Détecte les connexions RDP et enregistre l'activité. Le terminal distant permet aux administrateurs d'activer/désactiver la politique RDP. Offre une visibilité sur la politique RDP sur tous les appareils gérés et détecte les modifications apportées à celle-ci.
Planification de la réponse aux cyber-incidents pour minimiser l'impact si une attaque se produit.	Sophos Rapid Response	Fournit une réponse ultra rapide aux incidents, 24 h/24 et 7 j/7, assurée par des experts Sophos.
	Sophos MTR (Managed Threat Response)	Service managé de chasse aux menaces, de détection et de réponse fourni par une équipe d'experts disponible 24 h/24 et 7 j/7.
Formation de sensibilisation à la cybersécurité et tests de phishing	Sophos Phish Threat	Améliore la vigilance en matière de sécurité et éduque les utilisateurs grâce à des simulations d'attaques de phishing, des formations automatisées à la sécurité et un reporting complet. L'intégration avec Sophos Email permet aux équipes de sécurité d'identifier efficacement et d'accélérer la formation des utilisateurs qui ont été avertis ou empêchés de visiter un site Web en raison de leur profil de risque.

CYBER CONTRÔLE	COMMENT SOPHOS PEUT VOUS AIDER	DÉTAILS
Identification et prévention des vulnérabilités dans les environnements Cloud afin d'éviter toute exploitation par des adversaires	Sophos Cloud Optix	Identifie et prévient de manière proactive les failles de sécurité, les rôles IAM sur-privilégiés et les mauvaises configurations d'accès au réseau dans les environnements de Cloud public avec l'intégration d'Amazon Inspector, notamment les ports de machines virtuelles exposés à Internet, la connexion root à distance activée ou les versions de logiciels vulnérables installées. Obtention de l'état des correctifs pour les machines virtuelles Amazon avec l'intégration à AWS Systems Manager. Étend les analyses de sécurité aux pipelines CI/CD avec l'analyse de l'infrastructure programmable (IaC) tout en analysant les registres des conteneurs sur Azure, AWS et Docker Hub pour détecter les vulnérabilités du système d'exploitation.

Pour discuter de votre cyber-résilience et de la manière dont Sophos peut vous aider à renforcer vos défenses contre les ransomwares, contactez un représentant Sophos.

** L'état des ransomwares 2022, Sophos, enquête auprès de 5 600 professionnels de l'informatique dans 31 pays.*

Apprenez-en plus sur les ransomwares et sur la façon dont Sophos peut vous aider à protéger votre organisation.

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 2022. 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.

2022-04-08 (SB-NP)

SOPHOS