Nouveautés : Sophos Cloud Native Security

Sécurité multi-Cloud complète pour les environnements, les charges de travail et les identités

SOPHOS
Cybersecurity delivered.

Une solution de sécurité du Cloud unique et intégrée

Migrer vers des technologies Cloud, telles que les hôtes, les conteneurs, les services de stockage et les infrastructures programmables (IaC), oblige les entreprises à accroître leur visibilité pour se protéger contre les mauvaises configurations, les malwares, les ransomwares, les violations, et bien plus encore.

Sophos Cloud Native Security unifie les outils de sécurité nécessaires pour fournir cette visibilité et rendre vos environnements Cloud robustes, difficiles à compromettre et rapides à récupérer en cas d'incident. Sophos Cloud Native Security combine Sophos Cloud Optix et Sophos Intercept X Advanced for Server XDR en une seule solution intégrée pour Amazon Web Services, Microsoft Azure et Google Cloud Platform,

À partir de l'interface de gestion de la console Sophos Central, vous pouvez chasser les menaces sur vos environnements multi-Cloud, recevoir des détections priorisées des incidents et bénéficier d'événements de sécurité automatiquement connectés afin d'optimiser les temps d'investigation et de réponse — le tout depuis un seul écran.

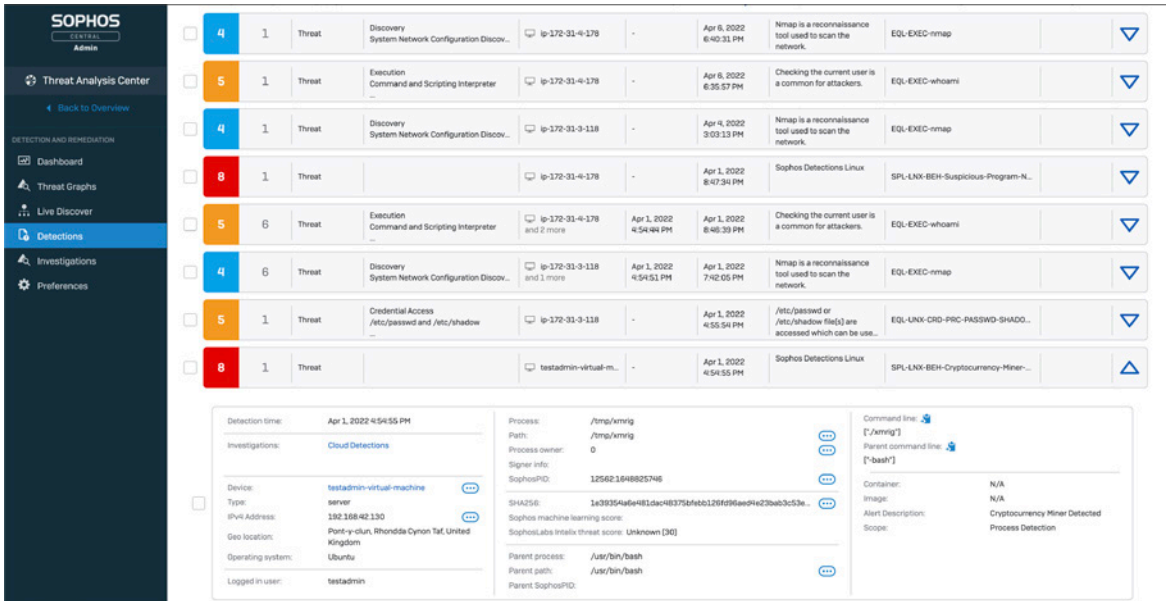
Protection des serveurs : la nouvelle évolution de Sophos

Pour sécuriser vos charges de travail de serveur dans le Cloud public, Sophos a étendu sa protection éprouvée pour Windows aux déploiements Linux, l'un des systèmes d'exploitation les plus prolifiques dans le Cloud.

L'offre Cloud Workload Protection de Sophos a connu une évolution majeure avec l'ajout de capacités pour Linux et les conteneurs. Celles-ci apportent une nouvelle protection contre les exploits et les comportements malveillants au runtime, ce qui permet de détecter en temps réel les incidents de sécurité sophistiqués se produisant sur Linux.

Sophos Cloud Native Security offre les fonctionnalités nécessaires pour protéger sur le long terme votre infrastructure et vos données dans le Cloud.

- Protégez tout. Cloud, datacenter, hôte, conteneur, Windows ou Linux.
- Améliorez les performances et le temps de fonctionnement grâce à une protection légère des hôtes Linux et Windows via un agent, ou une API pour Linux.
- Identifiez les incidents de sécurité sophistiqués se produisant au runtime sur Linux et les conteneurs sans avoir à déployer de module de noyau.
- Sécurisez vos hôtes et vos travailleurs distants Windows contre les ransomwares, les exploits et les menaces inédites.
- Contrôlez les applications, verrouillez les configurations et surveillez les modifications apportées aux fichiers système Windows critiques.
- Optimisez les investigations et la réponse aux menaces avec Sophos XDR (Extended Detection and Response) afin de prioriser et de connecter les événements.



Exemple de détection des menaces au runtime dans la console Sophos Central.

Options de déploiement de Cloud Workload Protection

Gestion dans Sophos Central — L'agent Linux léger fournit aux équipes de sécurité les informations essentielles dont elles ont besoin pour analyser et répondre aux comportements à risque, aux exploits et aux malwares ciblant Windows et Linux — depuis une seule console. En surveillant l'hôte, cette option de déploiement permet aux équipes de gérer leurs solutions Sophos à partir d'une seule et même interface. Elles peuvent ainsi passer en toute transparence de la chasse aux menaces au nettoyage et à la gestion.

Intégration par API — Sophos Linux Sensor est une option de déploiement très flexible qui offre les meilleures performances possibles. Le capteur utilise des API pour intégrer la détection des menaces au runtime dans les environnements hôtes et les conteneurs avec vos outils de réponse aux menaces. Il offre un plus grand niveau de contrôle afin de créer des ensembles de règles personnalisées contenant uniquement les détections comportementales au runtime nécessaires pour répondre à des cas d'usages de sécurité spécifiques.

En plus de l'agent Linux, Sophos Linux Sensor fournit :

- Plus de détections : Accès à des détections supplémentaires pour l'exploitation des applications et des systèmes.
- Configuration et réglage : Options permettant de modifier les listes d'autorisation et de blocage pour les détections par défaut.
- Réglage des ressources : Options de configuration permettant d'optimiser l'utilisation des ressources de l'hôte.

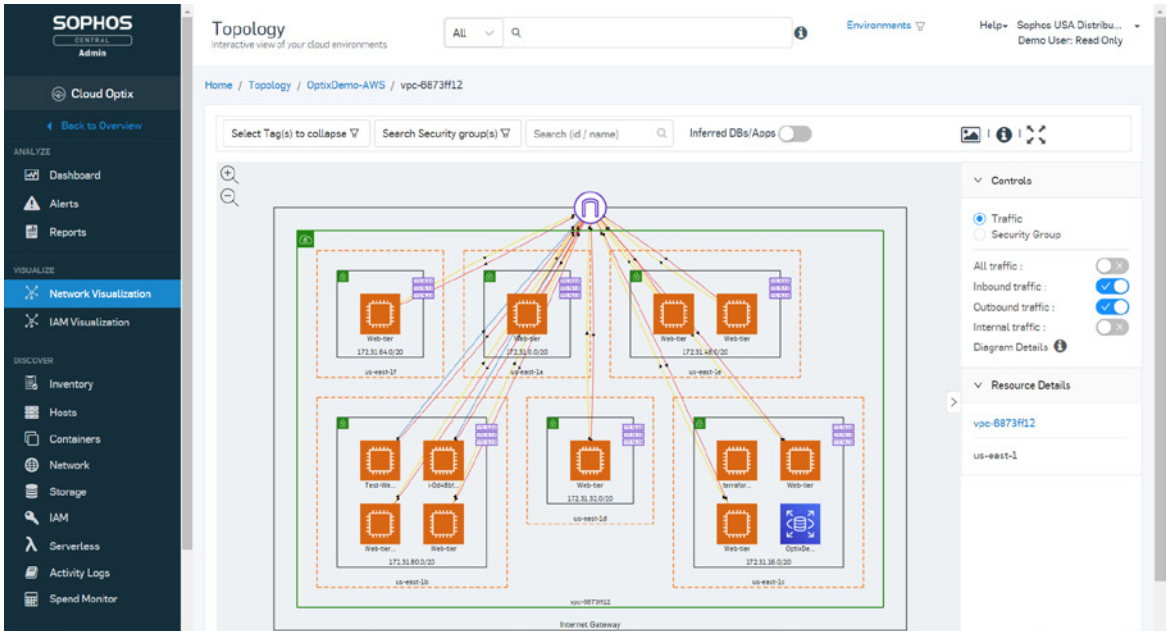
Une meilleure visibilité des actifs à protéger

Pour réduire la totalité de votre surface d'attaque sur l'ensemble des environnements AWS, Azure et GCP vous devez aller plus loin que la protection et la détection des menaces dans le Cloud. C'est pourquoi Sophos Cloud Native Security consolide et simplifie votre sécurité avec un seul outil qui inclut : la gestion de la posture de sécurité du Cloud (CSPM), la gestion de la posture de sécurité de Kubernetes (KSPM), ainsi que la gestion de l'infrastructure programmable (IaC), la gestion des droits des infrastructures Cloud et la surveillance des dépenses du Cloud.

Visibilité, gouvernance et conformité multi-Cloud

Gagnez en efficacité avec des outils de remédiation et de visibilité sans agent pour les environnements AWS, Azure, GCP, Kubernetes, les infrastructures programmables (IaC) et Docker Hub dans une seule console.

- Obtenez une vue d'ensemble grâce aux inventaires des actifs et aux visualisations exportables de la topologie du réseau, disponibles à la demande.
- Intégrez tous vos fournisseurs de services Cloud dans une seule console, dont Azure Advisor, Azure Sentinel, AWS Security Hub, Amazon GuardDuty, AWS CloudTrail, AWS IAM Access Analyzer, Amazon Detective, Amazon Inspector, AWS Systems Manager et AWS Trusted Advisor.
- Bloquez le Shadow IT grâce à la découverte automatique des actifs et à la visualisation des déploiements des agents de protection des charges de travail et des pare-feux de Sophos.
- Prévenez et gérez les risques liés à la configuration pour les hôtes, les conteneurs, le serverless, les services de stockage et de bases de données, ainsi que les groupes de sécurité réseau.
- Surveillez et maintenez en continu de hauts niveaux de sécurité et de conformité grâce à des politiques de sécurité qui s'adaptent automatiquement à votre environnement. Vous économisez ainsi des semaines d'efforts grâce à des rapports prêts pour vos audits. Les normes incluent : critères CIS, ISO 27001, EBU R 143, FEDRAMP FIEC, RGPD, HIPAA, PCI DSS, SOC2 et les bonnes pratiques de Sophos.
- Surveillez vos dépenses de Cloud pour les services AWS et Azure depuis le même écran pour une meilleure visibilité. Obtenez des recommandations de Sophos pour optimiser les dépenses des fournisseurs de Cloud, ou intégrez la solution avec les services AWS Trusted Advisor ou Azure Advisor.
- Réduisez la surproduction d'alertes et détectez rapidement les problèmes critiques avec des alertes codées par couleur vous indiquant clairement les étapes de remédiation à suivre.

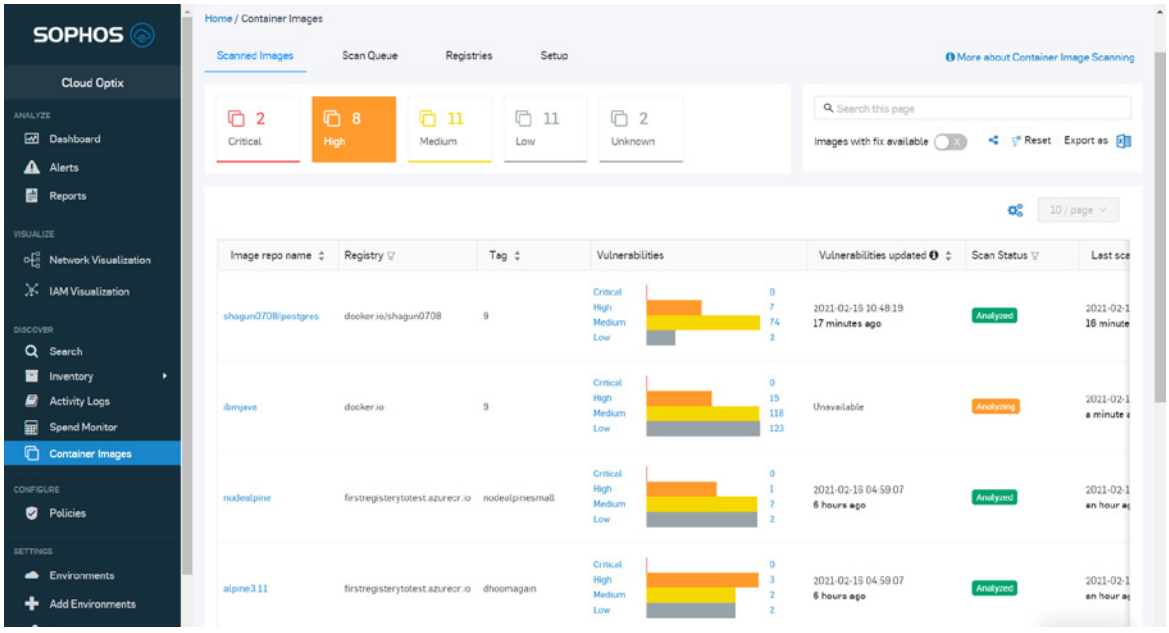


Exemple de visualisation de la topologie du réseau pour AWS avec analyse des groupes de sécurité.

Réduisez les risques sans ralentir vos processus DevOps

Assurez un développement informatique rapide et sécurisé grâce à avec des contrôles intégrés de la configuration et de la conformité de la sécurité — à n'importe quel stade du pipeline de développement.

- Détectez automatiquement les mauvaises configurations, les secrets, mots de passe et clés intégrés dans les fichiers modèles de Terraform, AWS CloudFormation, Ansible, Kubernetes et Azure Resource Manager.
- Empêchez le déploiement de conteneurs présentant des vulnérabilités au niveau du système d'exploitation et identifiez les correctifs disponibles, grâce à la prise en charge des registres Amazon ECR, ACR, Docker Hub, des environnements IaC et des images dans le processus de développement.
- Intégrez GitHub et Bitbucket en toute transparence pour recevoir les résultats des analyses à la demande dans la console Cloud Optix ou utilisez l'API REST pour analyser les modèles d'infrastructure programmable (IaC) et les images de conteneurs à n'importe quel stade du développement.

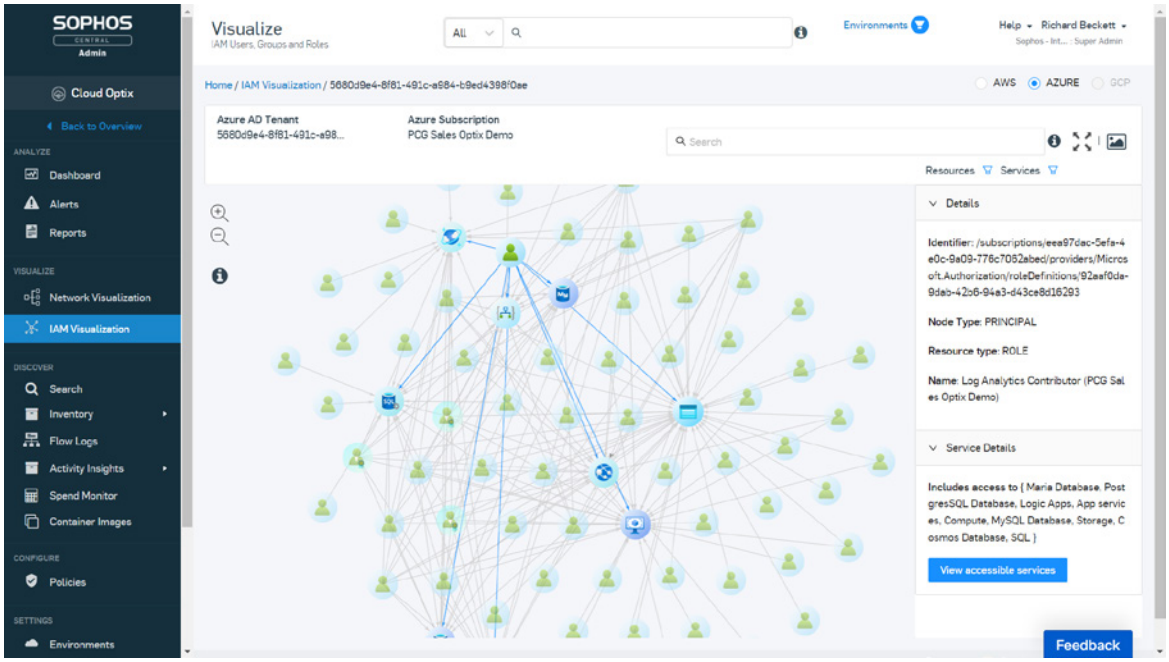


Exemple de résumé des résultats de l'évaluation des vulnérabilités de l'analyse des images de conteneurs.

Appliquez le principe du moindre privilège

Gérez les identités avant qu'elles ne soient exploitées en appliquant le principe du moindre privilège avec la gestion des droits de l'infrastructure Cloud pour l'ensemble de vos environnements multi-Cloud.

- Assurez-vous que toutes les identités n'effectuent que les actions nécessaires à leur travail et rien de plus.
- Repérez les modèles et les lieux d'accès inhabituels des utilisateurs pour identifier une utilisation abusive ou un vol d'identifiants.
- Mettez en évidence les rôles IAM Microsoft Azure orphelins, non gérés et obsolètes utilisés pour accéder aux environnements.
- Visualisez les rôles IAM d'AWS complexes et imbriqués pour identifier et prévenir rapidement les rôles IAM surprivilégiés.
- Utilisez SophosAI pour connecter des anomalies à haut risque dans le comportement des utilisateurs dans l'environnement AWS afin de prévenir toute violation.

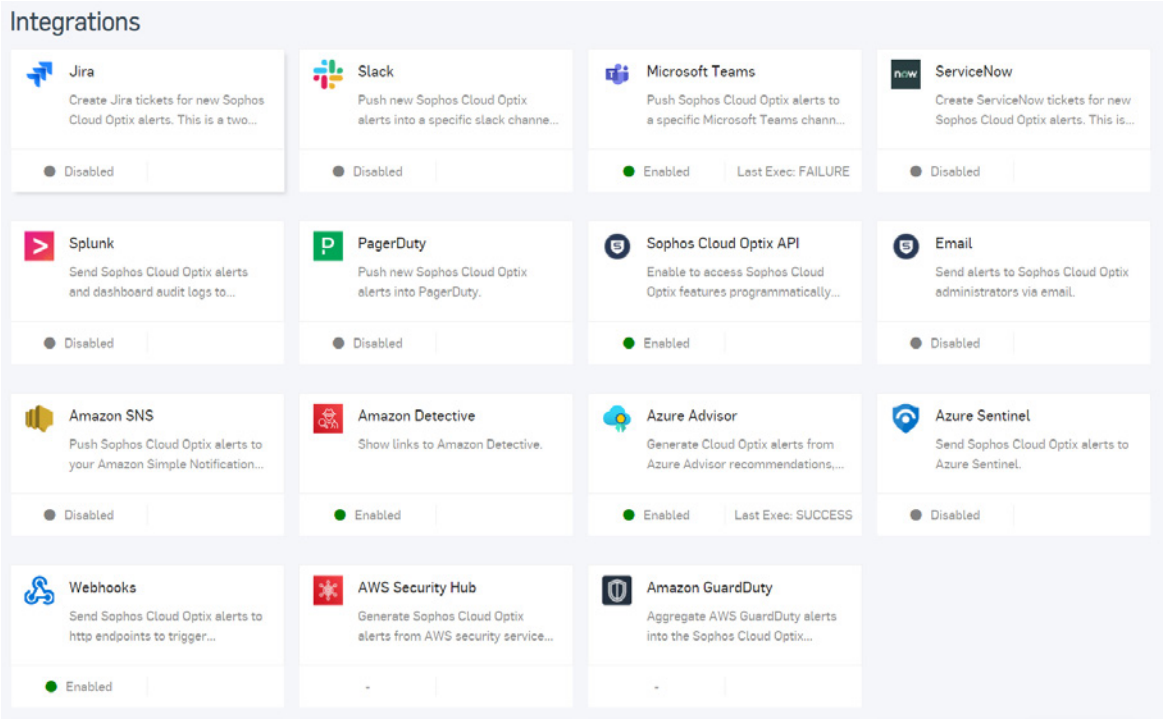


Exemple de la visualisation IAM de Sophos pour Microsoft Azure.

Optimisez les opérations de sécurité et améliorez la collaboration

Augmentez l'agilité de votre organisation avec des alertes sur la posture de sécurité des environnements Cloud intégrées aux outils SIEM, de collaboration et de flux de travail que vous utilisez déjà.

- Opérations de sécurité : Intégrez Splunk, Azure Sentinel, et PagerDuty pour recevoir des notifications instantanées concernant les événements de sécurité et de conformité.
- Outils de collaboration : Envoyez des alertes instantanées à Slack, Microsoft Teams ou Amazon Simple Notification Service (SNS).
- Gestion du flux de travail : Intégrez la réponse aux alertes dans vos flux de travail habituels en créant des tickets JIRA et ServiceNow à partir de Sophos Central avec une intégration bidirectionnelle pour éviter les doublons.



Exemples d'intégrations Sophos courantes permettant de gérer la posture de sécurité du Cloud.

Des partenariats qui renforcent votre équipe

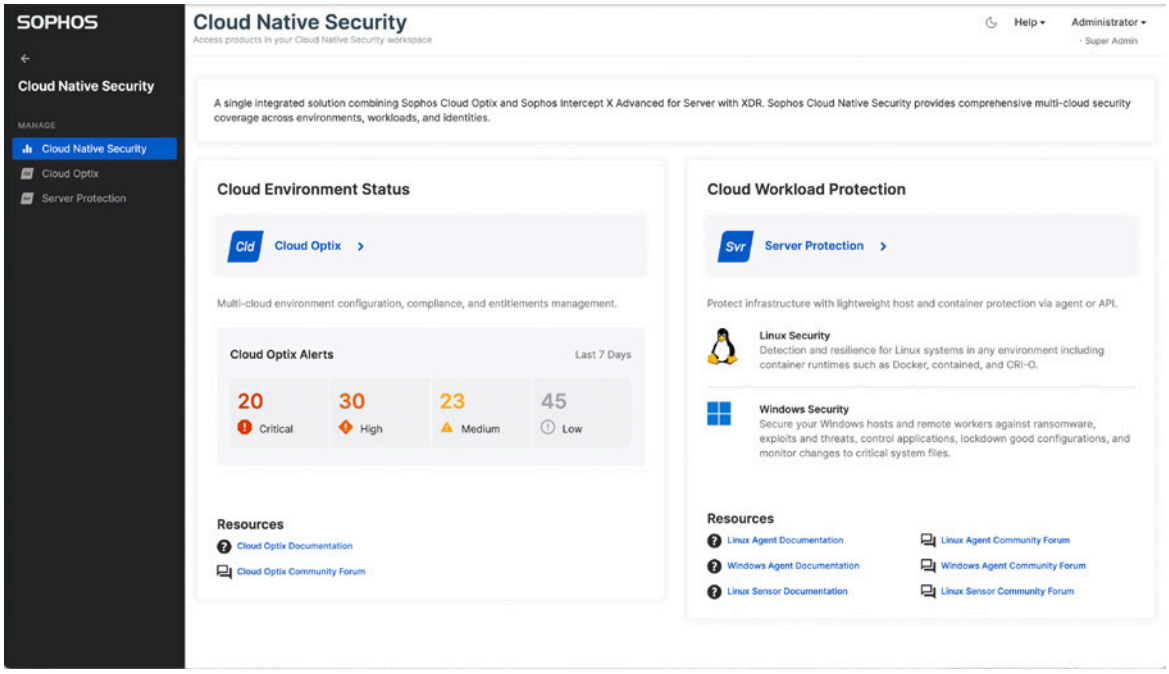
Gérez la protection comme vous l'entendez : avec votre propre équipe de sécurité, avec l'aide d'un partenaire Sophos ou avec le service Sophos Managed Detection and Response (MDR) qui surveille et répond aux attaques 24 h/24 et 7 j/7.

Le service managé Sophos MDR est le complément parfait de Sophos Cloud Native Security. Notre équipe MDR collabore avec vos équipes, surveille votre environnement 24/7/365, répond aux menaces potentielles, recherche des indicateurs de compromission et fournit une analyse détaillée des événements (notamment ce qui s'est passé, où, quand, comment et pourquoi), afin d'empêcher les menaces sophistiquées de compromettre vos données et vos systèmes.

Disponibilité de Sophos Cloud Native Security

Cette nouvelle offre groupée est disponible pour tous les clients et peut être mise à niveau à partir d'Intercept X Essentials for Server, Intercept X Advanced for Server ou Intercept X Advanced for Server with XDR.

Une fois l'offre activée dans Sophos Central, les clients et partenaires verront apparaitre un nouvel élément « CNS » dans la barre de navigation de gauche. C'est à partir de ce lien que vous accéderez au nouveau tableau de bord récapitulatif Cloud Native Security, à partir duquel vous pourrez accéder aux produits Sophos Cloud Optix et Intercept X Advanced for Server with XDR.



Exemple du tableau de bord Sophos Cloud Native Security dans la console de gestion Sophos Central.

Essai gratuit dès aujourd'hui

Évaluation gratuite de 30 jours
sur sophos.fr/cloud

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

22-07-06 FR (DD)

SOPHOS