# Sophos XDR


## Intercept X Advanced with XDR, Intercept X Advanced for Server with XDR

Intercept X est la seule solution XDR du secteur qui synchronise les protections natives des postes de travail, des serveurs, du pare-feu, de la messagerie, du Cloud et d'O365. Obtenez une vue globale de l'environnement de votre organisation avec le plus riche ensemble de données et une analyse approfondie pour la détection, l'investigation et la réponse aux menaces, tant pour les équipes SOC dédiées que pour les administrateurs informatiques.

## Lancez des requêtes pour les opérations IT et la chasse aux menaces

Obtenez rapidement les réponses à vos questions critiques. Les administrateurs informatiques et les professionnels de la cybersécurité verront une réelle valeur ajoutée pour leurs opérations informatiques et leurs actions de chasse aux menaces quotidiennes.

## Commencez par la meilleure protection

Intercept X bloque les attaques avant qu'elles ne surviennent. Vous bénéficiez ainsi d'une meilleure protection et vous passez moins de temps à analyser les incidents qui auraient dû être automatiquement bloqués. Vous avez également accès à des informations détaillées sur les menaces, vous permettant d'intervenir rapidement et avec discernement.

## Sachez où concentrer vos efforts

Concentrez-vous sur les problèmes importants grâce à une liste de détections suspectes et de configurations vulnérables classées par ordre de priorité et comprenant des informations clés pour une investigation plus approfondie. Choisissez parmi une bibliothèque de modèles pré-écrits pour lancer une grande variété de requêtes sur les opérations informatiques et la chasse aux menaces, ou créez les vôtres.

## Réduire les temps d'investigation et de réponse

Les investigations guidées par l'IA vous permettent de comprendre rapidement la portée et la cause d'un incident et de minimiser le temps de réponse. Accédez aux appareils pour obtenir leur état en temps réel et jusqu'à 90 jours de données historiques ou 30 jours de données historiques dans le data lake.

## Visibilité à partir de différents produits

Obtenez une visibilité maximale sur votre organisation grâce à l'intégration native d'Intercept X, Intercept X for Server, Sophos Firewall, Sophos Email, Sophos Mobile, Cloud Optix et des données Microsoft Office 365.

## Prise en charge multi-plateforme et multi-OS

Inspectez votre environnement qu'il soit dans le Cloud, sur site ou virtuel à travers les déploiements Windows, macOS, Linux, Amazon Web Services, Microsoft Azure, Google Cloud Platform et Oracle Cloud Infrastructure.

## Avantages principaux

- Obtenez les réponses à vos questions critiques relatives aux opérations informatiques et à la traque des menaces
- Tirez profit d'une liste priorisée de détections et d'investigations guidées par l'IA
- Prenez des mesures correctives à distance sur les appareils qui vous intéressent
- Obtenez une vue d'ensemble de l'environnement informatique de votre entreprise et, si nécessaire, accédez à des informations plus détaillées
- Intégrations natives des données des postes de travail, serveurs, pare-feux, messageries, Cloud, mobiles et O365
- Accédez à une bibliothèque de requêtes pré-écrites et personnalisables

SOPHOS

# Cas d'usages

## Opérations informatiques

- Pourquoi une machine est-elle lente ?
- Quels appareils ont des vulnérabilités connues, des services inconnus ou des extensions de navigateur non autorisées ?
- Des programmes en cours d'exécution devraient-ils être supprimés ?
- Identifier les appareils non gérés, invités et IoT
- Pourquoi la connexion au réseau du bureau est-elle lente ? Quelle application en est la cause ?
- Revenir 30 jours en arrière pour détecter toute activité inhabituelle sur un appareil disparu ou détruit
- Localisez les appareils mobiles qui ne sont pas corrigés ou dont les logiciels sont obsolètes

## Chasse aux menaces

- Quels sont processus qui tentent d'établir une connexion réseau sur des ports non standards ?
- Afficher les processus qui ont récemment modifié des fichiers ou des clés de registre
- Lister les indices de compromission (IoC) mappés au cadre MITRE ATT&CK
- Prolonger l'investigation jusqu'à 30 jours sans remettre un appareil en ligne
- Utiliser les détections ATP et IPS du pare-feu pour analyser les hôtes suspects
- Comparer les informations de l'en-tête de l'email, les algorithmes de hachage SHA et autres IoC pour identifier le trafic vers un domaine malveillant
- Identifier les utilisateurs dont les tentatives d'authentification ont échoué à plusieurs reprises

# Que contient Sophos XDR ?

| | XDR (Extended Detection and Response) |
|---|---|
| Sources de données multi-produits | ✓ |
| Détection, investigation et réponse multi-produits | ✓ |
| Liste de détections priorisée et investigations guidées par l'IA | ✓ |
| Sophos Data Lake | ✓ |
| Durée de conservation du Data Lake | 30 jours |
| Informations d'état en temps réel | ✓ |
| Durée de conservation des données sur le disque | Jusqu'à 90 jours |
| Bibliothèque de modèles pour la chasse aux menaces et les opérations IT | ✓ |
| Capacités de protection Intercept X | ✓ |

Pour plus de détails sur les licences, veuillez consulter les guides de gestion des licences pour Intercept X et Intercept X for Server.

## Essai gratuit

Évaluation gratuite de 30 jours sur sophos.fr/intercept-x

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



22-01-06 DS-FR (MP)

SOPHOS