Brochure de la solution

Sophos ITDR

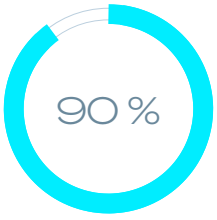
Neutraliser les menaces basées sur l'identité avant qu'elles n'aient un impact sur vos activités.

Sophos Identity Threat Detection and Response (ITDR) bloque les attaques basées sur l'identité en surveillant en continu votre environnement à la recherche de risques liés aux identités et de configurations incorrectes, tout en fournissant une veille sur le Dark Web pour repérer les identifiants compromis.

Menaces liées aux identités : un problème de sécurité croissant

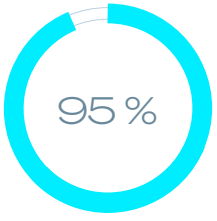
Les contrôles et les accès basés sur les utilisateurs sont au cœur des préoccupations actuelles dans le monde de l'IT et de la cybersécurité. La migration vers le cloud et le télétravail a accru la complexité de la surveillance et de la sécurisation des surfaces d'attaque liées aux identités. Les adversaires exploitent les identités compromises, les failles des infrastructures et les erreurs de configuration pour obtenir un accès non autorisé à des données et des systèmes sensibles. C'est pourquoi il est primordial de détecter les usurpations d'identité et de bloquer les attaques basées sur l'identité pour garantir l'efficacité des opérations de sécurité.

La preuve par les chiffres

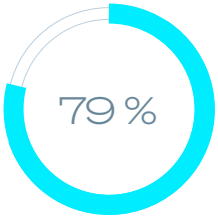


des organisations ont subi au moins une violation liée aux identités au cours de l'année écoulée.[1]

Coût moyen d'un vol de données.[2]



des environnements Microsoft Entra ID présentent une erreur de configuration critique.[3]



des violations de données sont liées aux identités.[4]

Avantages

- **Bénéficiez d'une meilleure visibilité** grâce à une vue centralisée des identités sur l'ensemble de vos systèmes.
- **Identifiez rapidement** les risques liés aux identités et les erreurs de configuration, avec des recommandations exploitables.
- **Analysez en continu** les changements dans la posture liée aux identités.
- **Analysez le Dark Web** à la recherche d'identifiants divulgués.
- **Détectez les activités potentiellement malveillantes** provenant de l'intérieur, d'adresses IP inconnues ou d'emplacements suspects.
- **Répondez rapidement** et avec précision aux menaces liées aux identités.
- **S'intègre à Sophos MDR** pour une investigation et une réponse expertes aux menaces liées aux identités.

La solution Sophos ITDR

Sophos ITDR prévient les attaques basées sur l'identité en surveillant en continu votre environnement à la recherche de risques liés aux identités et de configurations incorrectes (un problème qui touche 95 % des entreprises), tout en fournissant des informations issues du Dark Web sur les identifiants compromis. Identifiez vos risques liés aux identités en quelques minutes, contre plusieurs jours avec des solutions traditionnelles, et évaluez votre surface d'attaque liée à l'identité au fil du temps.

Réduisez votre surface d'attaque liée aux identités

Sophos ITDR analyse en continu votre environnement Microsoft Entra ID afin d'identifier rapidement les erreurs de configuration et les failles de sécurité liées aux identités, et de prioriser les problèmes nécessitant une attention immédiate. Les cybercriminels exploitent ces expositions pour augmenter leurs privilèges et réaliser leurs attaques. Remédiez rapidement aux risques, notamment les lacunes dans les politiques d'accès conditionnel, les comptes orphelins, les comptes disposant de privilèges excessifs et les applications à risque.

Réduisez le risque de fuite ou de vol d'identifiants

Selon les renseignements recueillis par la Counter Threat Unit (CTU) de Sophos X-Ops, le nombre d'identifiants volés proposés à la vente sur l'une des plus grandes marketplaces du Dark Web a plus que doublé au cours de l'année dernière. Sophos ITDR détecte et répond aux menaces liées aux identités qui contournent les contrôles de cybersécurité traditionnels, offrant une protection contre 100 % des techniques 'Credential Access' de MITRE ATT&CK.[5] La solution identifie les comportements utilisateurs à risque, tels que les schémas de connexion inhabituels, et met en évidence l'utilisation d'identifiants volés ou compromis pour accéder à vos systèmes.

Ce que vous obtenez avec Sophos ITDR

Catalogue des identités
Bénéficiez d'une meilleure visibilité grâce à une vue centralisée des identités sur l'ensemble de vos systèmes.

Évaluations continues de la posture liée aux identités
Analysez régulièrement votre environnement Microsoft Entra ID afin d'identifier les erreurs de configuration et les failles de sécurité.

Surveillance des identifiants compromis sur le Dark Web
Effectuez des recherches sur le Dark Web et dans les bases de données issues de vols pour repérer les identifiants divulgués.

Analyse du comportement des utilisateurs
Surveillez les activités anormales associées au vol d'identifiants ou à des menaces internes.

Détection avancée des menaces liées aux identités
Identifiez rapidement les activités suspectes indiquant des techniques adverses spécifiques à un stade précoce de la chaîne d'attaque.

Actions de réponse aux menaces
Répondez rapidement et avec précision : imposez la réinitialisation des mots de passe, verrouillez les comptes présentant un comportement suspect, et plus encore.

« Sophos ITDR a considérablement amélioré la visibilité sur nos risques liés aux identités. Le fait de disposer d'une vue centralisée au sein de notre plateforme XDR nous permet d'intégrer les risques liés aux identités et aux erreurs de configuration mis en évidence par Sophos ITDR dans tous nos programmes de sécurité, améliorant ainsi la cyber posture globale de notre organisation et réduisant les risques. »

– Directeur de la sécurité des systèmes d'information, Services financiers

« Sophos ITDR identifie les risques dans les zones qui me préoccupaient auparavant au sein d'Azure et de l'écosystème Microsoft, tels que les failles dans les politiques d'accès conditionnel et les applications non sécurisées ou disposant de privilèges excessifs. »

– Responsable de la sécurité des systèmes d'information

Intégré avec Sophos MDR

Sophos ITDR est entièrement intégré à Sophos MDR, le service de détection et de réponse managé le plus réputé sur le marché. Cette association puissante permet aux experts en sécurité de Sophos de surveiller, d'investiguer et de répondre aux menaces liées aux identités en votre nom :

- Sophos ITDR crée automatiquement un Dossier MDR pour les détections de menaces liées aux identités et les résultats à haut risque.
- Les analystes de sécurité de Sophos MDR investiguent ensuite ces dossiers et appliquent des actions de réponse pour neutraliser les menaces.

Exemple : identifiants divulgués sur le Dark Web

- Sophos ITDR repère les identifiants d'un utilisateur mis en vente sur une plateforme populaire du Dark Web.
- Les analystes de Sophos MDR peuvent verrouiller le compte de l'utilisateur et forcer la réinitialisation du mot de passe.

Exemple : utilisation d'identifiants volés

- Sophos ITDR identifie les connexions suspectes provenant de pays, d'appareils et d'adresses IP inconnus.
- Les analystes de Sophos MDR peuvent verrouiller le compte de l'utilisateur compromis et arrêter toutes les sessions actives.

Plus forts ensemble : Sophos ITDR + Microsoft Entra ID

Microsoft Entra ID est essentiellement un outil IAM (Identity and Access Management) qui permet de gérer les identités et les groupes, les contrôles RBAC, les accès privilégiés et les politiques d'accès conditionnel. Fourni dans une console unifiée pour détecter et neutraliser les menaces et les risques liés aux identités, Sophos ITDR va au-delà des fonctionnalités IAM de base avec des contrôles de l'identité, l'évaluation de la posture, la surveillance du Dark Web, la détection avancée des menaces, et bien plus encore. **La combinaison entre Entra ID et Sophos ITDR offre la protection des identités la plus complète pour votre entreprise.**

Licences simples

Sophos ITDR est facile à déployer, à utiliser et à se procurer. Le modèle de licence par abonnement est basé sur le nombre d'utilisateurs et de serveurs de votre organisation. Les tarifs sont ainsi prévisibles. Vous avez la possibilité d'ajouter Sophos ITDR à la solution Sophos XDR ou au service Sophos MDR, selon vos besoins.

- **Complément au service Sophos Managed Detection and Response (MDR) :** les experts en sécurité de Sophos surveillent, investiguent et répondent aux menaces liées aux identités en votre nom.
- **Complément au produit Sophos Extended Detection and Response (XDR) :** votre équipe interne peut bénéficier des outils de détection, d'investigation et de réponse assistés par IA de Sophos grâce à Sophos ITDR.

Gartner

Un 'Customers' Choice' 2025 de Gartner Peer Insights dans la catégorie Extended Detection and Response (XDR).

Un Leader des rapports Overall Grid® de G2 dans les catégories Extended Detection and Response (XDR) et Managed Detection and Response (MDR).

MITRE | ATT&CK® Evaluations

Un Strong Performer dans les évaluations MITRE ATT&CK dans les catégories Managed Services et Enterprise Products.

FROST & SULLIVAN

Un Leader dans l'édition 2025 de Frost & Sullivan Frost Radar™ for Managed Detection and Response.

Pour en savoir plus :

sophos.fr/ITDR

1 - Étude 2024 Identity Defined Security Alliance (IDSA).
2 - IBM, Cost of a Data Breach 2024.
3 - Recherches de l'équipe Sophos de réponse aux incidents.
4 - Identity Defined Security Alliance.
5 - Basé sur les détecteurs disponibles mappés au cadre MITRE ATT&CK.

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

2025-09-15 BR-FR (MP)

SOPHOS