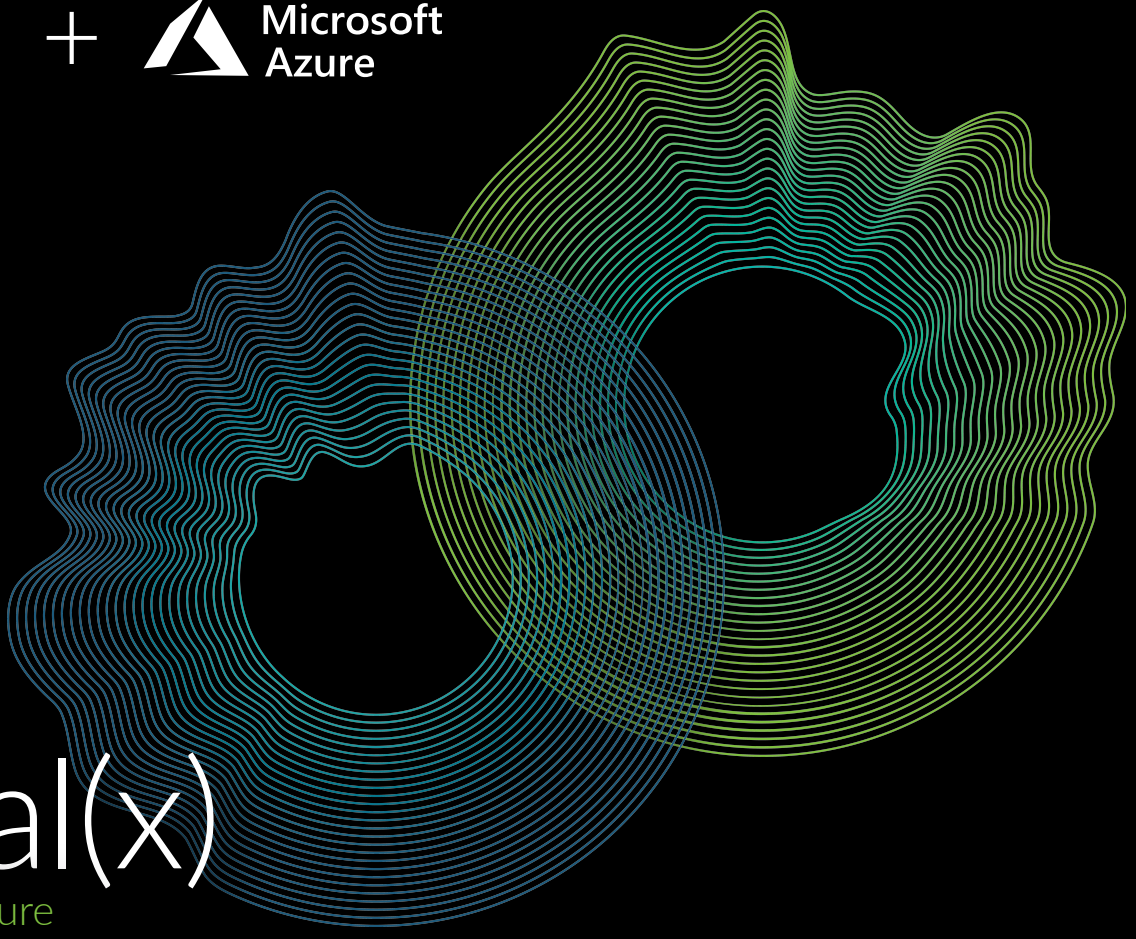
ExtraHop + Microsoft Azure



Reveal(x)

pour Microsoft Azure

Protégez les applications et données de votre environnement Microsoft Azure avec une détection et réponse réseau (NDR) dans le cloud.

SÉCURISEZ VOTRE INVESTISSEMENT DANS LE CLOUD AZURE

Alors que les entreprises migrent de plus en plus d'applications stratégiques dans le cloud afin de profiter d'une évolutivité et d'une efficacité supérieures, les équipes du SOC se doivent d'adapter la sécurité à cette évolution.

ExtraHop Reveal(x) pour Azure offre une visibilité, une détection des menaces, une investigation et une réponse à l'intérieur du périmètre qui vous permettent de sécuriser les applications et données de votre environnement hybride.

Détection des menaces dans le cloud

ExtraHop Reveal(x) pour Azure cible les trois principales catégories de menaces pesant sur les environnements cloud : les erreurs de configuration, les accès non autorisés et les API non sécurisées. Reveal(x) associe des informations approfondies sur les contenus, le décodage des transactions et les données d'événement d'Azure Security Center pour identifier les événements d'intérêt, comme les instances malveillantes, les systèmes de journalisation désactivés et les exécutions de fichiers suspectes. ExtraHop Reveal(x) pour Azure détecte et catégorise le moindre octet passant par votre environnement.

Données de transactions enrichies

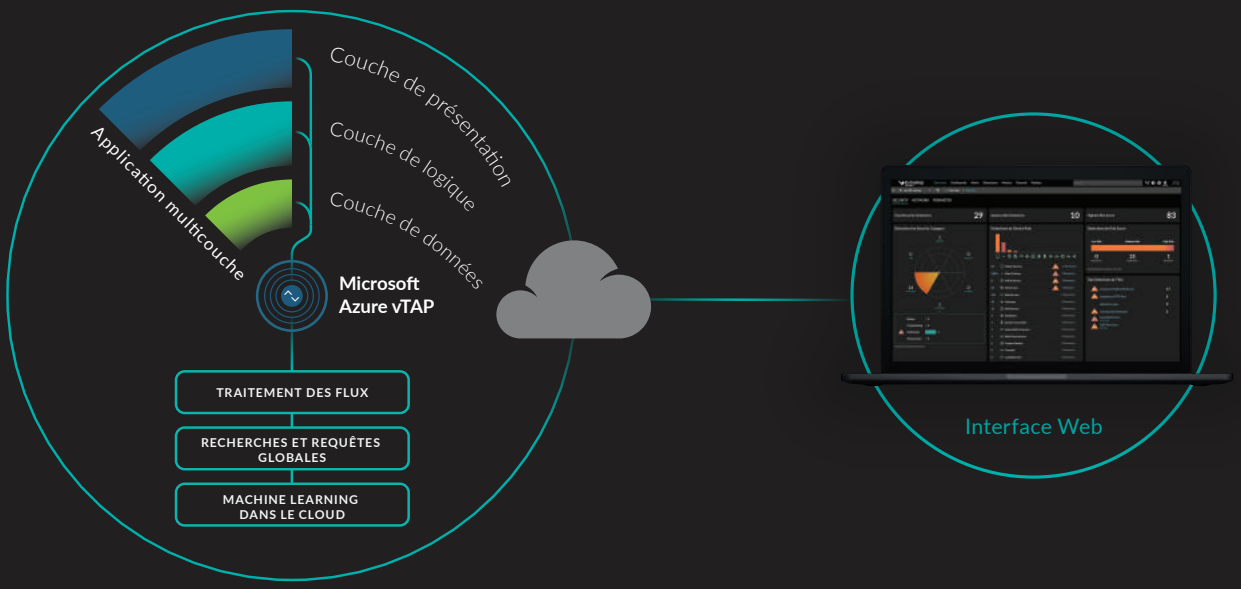
ExtraHop est le seul fournisseur à convertir l'ensemble des données en lignes en un enregistrement totalement indexé de tous les éléments de chaque transaction. Jamais autant de données empiriques n'avaient pu être réunies jusqu'ici. Nous proposons l'ensemble de données contextualisées et factuelles le plus vaste et le plus riche du marché pour vous permettre de répondre aux questions essentielles posées par les équipes de sécurité et opérationnelles. Aucune autre source ne propose des informations aussi étendues, riches et pertinentes que celles issues de nos données.

Responsabilité partagée

Aucune autre plateforme ne propose la visibilité requise pour mettre en œuvre efficacement des modèles de responsabilité partagée et prioriser l'utilisation des ressources de sécurité (analystes du SOC, infrastructure de sécurité) selon les actifs stratégiques disponibles et le risque. Les fournisseurs de service cloud s'appuient sur un modèle de responsabilité partagée qui fait porter la majeure partie de la responsabilité de la sécurité à l'entreprise. La visibilité offerte par Reveal(x) pour Azure permet ainsi d'alléger le fardeau des équipes SecOps.

FONCTIONNEMENT

Reveal(x) s'appuie sur Microsoft Azure Virtual Network Tap (vTAP) pour combiner analyse en temps réel du trafic réseau et événements de sécurité d'Azure Security Center. Les analystes disposent ainsi de tout ce dont ils ont besoin pour prendre les mesures adéquates en toute confiance.



FONCTIONNALITÉS CLÉS

Reveal(x) combine analyses du trafic réseau et événements de sécurité d'Azure Security Center. Les analystes disposent ainsi de tout ce dont ils ont besoin pour prendre les mesures adéquates en toute confiance.

- **Déchiffrement hors bande**
  Déchiffrez et analysez l'ensemble du trafic SSL/TLS 1.3 en temps réel.
- **Décodage des transactions**
  Décodez plus de 70 protocoles pour accélérer la détection des menaces, les investigations et les réponses.
- **Machine learning dans le cloud**
  Exploitez plus de 5 000 caractéristiques des données en lignes pour mettre en place un modèle de détection comportementale.

VISIBILITÉ COMPLÈTE

Collectez et traitez toutes vos données réseau en temps réel pour l'ensemble de votre entreprise sans dégrader l'analyse : la moindre transaction, la moindre workload est prise en compte, partout et à tout moment.

DÉPLOIEMENT TRANSPARENT

En se déployant automatiquement sur les nouveaux environnements cloud via Azure vTAP, Reveal(x) ne met qu'une seconde pour commencer de manière autonome à identifier les menaces dans les zones d'ombre du cloud.

À PROPOS D'EXTRAHOP NETWORKS

ExtraHop compte parmi les plus grands fournisseurs de solutions de détection et réponse réseau natives du cloud pour l'entreprise hybride. Visibilité complète, détection des menaces en temps réel et investigation basée sur un machine learning dans le cloud… ExtraHop permet aux équipes de sécurité des plus grandes entreprises, notamment du Crédit Suisse, de The Home Depot, de Caesars Entertainment et de Liberty Global, de prendre du recul par rapport aux alertes, silos organisationnels et technologies à durée de vie limitée afin d'accélérer les investigations et d'unifier les politiques des environnements hybrides. L'objectif ? Mettre l'activité et la sécurité sur la même longueur d'onde en donnant la priorité au cloud. Découvrez la puissance d'ExtraHop grâce à notre démo interactive en ligne à l'adresse www.extrahop.com/demo.

ExtraHop

520 Pike Street, Suite 1600
Seattle, WA 98101
877-333-9872 (téléphone)
206-274-6393 (fax)
info@extrahop.com
www.extrahop.com