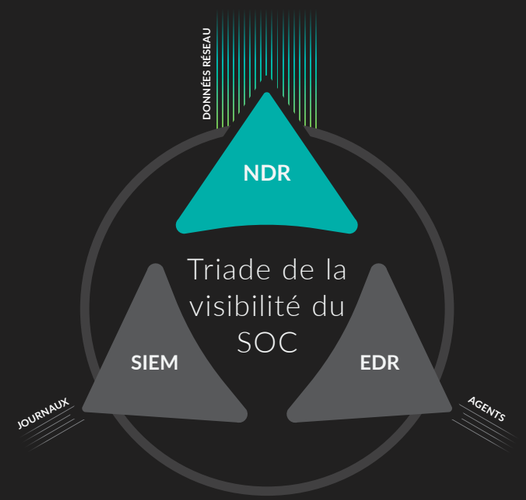
LA NDR CLOUD NATIVE COMPLÈTE LA VISIBILITÉ DU SOC

Dans de nombreux SOC d'entreprise, les données réseau constituent un angle mort. La détection et réponse réseau permet de contextualiser des observations factuelles et ne peut être désactivée ou contournée par les attaquants expérimentés, au contraire des outils basés sur des journaux et des agents. En raison de ces caractéristiques, le réseau constitue la meilleure source de données pour adopter une approche native du cloud de la détection, de l'investigation et de la réponse aux menaces dans les environnements hybrides.



SOURCES DE DONNÉES ET OUTILS

VALEUR POUR LE CLIENT

IDC

VISIBILITÉ COMPLÈTE

95 %
D'amélioration du délai de détection des menaces

DÉTECTION EN TEMPS RÉEL

77 %
D'amélioration du délai de résolution

INVESTIGATION GUIDÉE

59 %
De réduction du temps consacré à la résolution

DÉCOUVRIR L A DÉMO extrahop.com/demo

À PROPOS D'EXTRAHOP NETWORKS

ExtraHop propose des solutions de détection et réponse réseau natives du cloud pour l'entreprise hybride. Notre approche révolutionnaire permet d'analyser l'intégralité des interactions réseau et s'appuie sur un machine learning dans le cloud pour vous offrir une visibilité complète, une détection des menaces en temps réel et une investigation guidée. Nous aidons ainsi les plus grandes entreprises du monde à prendre du recul par rapport aux alertes, aux silos organisationnels et aux technologies à durée de vie limitée. Que vous analysiez des menaces, vous assuriez de la disponibilité d'applications stratégiques ou sécurisiez votre investissement dans le cloud, ExtraHop vous aide à protéger votre entreprise et à donner un nouvel élan à votre activité.

ExtraHop

info@extrahop.com
www.extrahop.com

ExtraHop

Reveal(x) Cloud

Dans le cloud, la clarté est essentielle. Reveal(x) Cloud est une solution de détection et réponse réseau (NDR) SaaS native du cloud. Elle fournit aux équipes SecOps une visibilité complète sur leur environnement cloud, notamment avec la détection en temps réel des menaces, des investigations rapides et des réponses automatisées.

VISIBILITÉ COMPLÈTE

Reveal(x) Cloud offre une visibilité approfondie et continue qui permet aux équipes SecOps d'analyser chaque paquet de données, chaque transaction et chaque application pour protéger leur investissement dans le cloud. Sans visibilité réseau native dans le cloud, les entreprises étaient jusqu'ici limitées aux outils basés sur des journaux ou des agents, ce qui rendait difficiles la détection et l'analyse rapides des menaces complexes.

DÉTECTION EN TEMPS RÉEL

Totalement passive, la solution Reveal(x) Cloud transforme les paquets bruts en métadonnées et permet ainsi d'effectuer des recherches sur l'ensemble du trafic. En alliant détection et catégorisation automatiques des actifs, analyse de la charge utile complète et machine learning pour proposer une détection haute-fidélité des menaces, Reveal(x) Cloud donne aux équipes SecOps travaillant dans le cloud la capacité de surveiller les menaces de manière proactive et d'y répondre.

INVESTIGATION GUIDÉE

Reveal(x) Cloud vous permet d'accéder au paquet associé à un événement de sécurité dans le cloud en quelques clics seulement : les heures passées à collecter et analyser les données des journaux et des agents appartiennent désormais au passé ! Par ailleurs, ses intégrations natives avec AWS EC2, S3, Amazon CloudWatch, CloudTrail et Amazon VPC Flow Logs, ainsi que les partenariats avec des plateformes d'orchestration et de gestion de tickets comme ServiceNow et Phantom accélèrent considérablement l'atténuation des menaces et le délai de réponse.

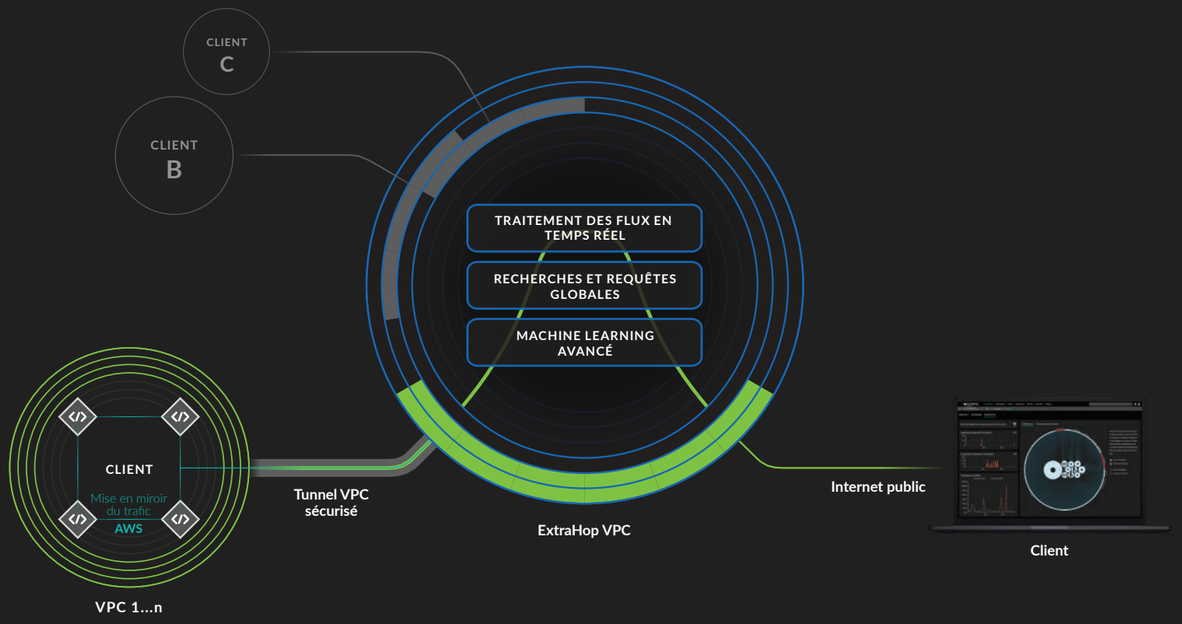
SÉCURITÉ NATIVE DU CLOUD POUR L'ENTREPRISE HYBRIDE

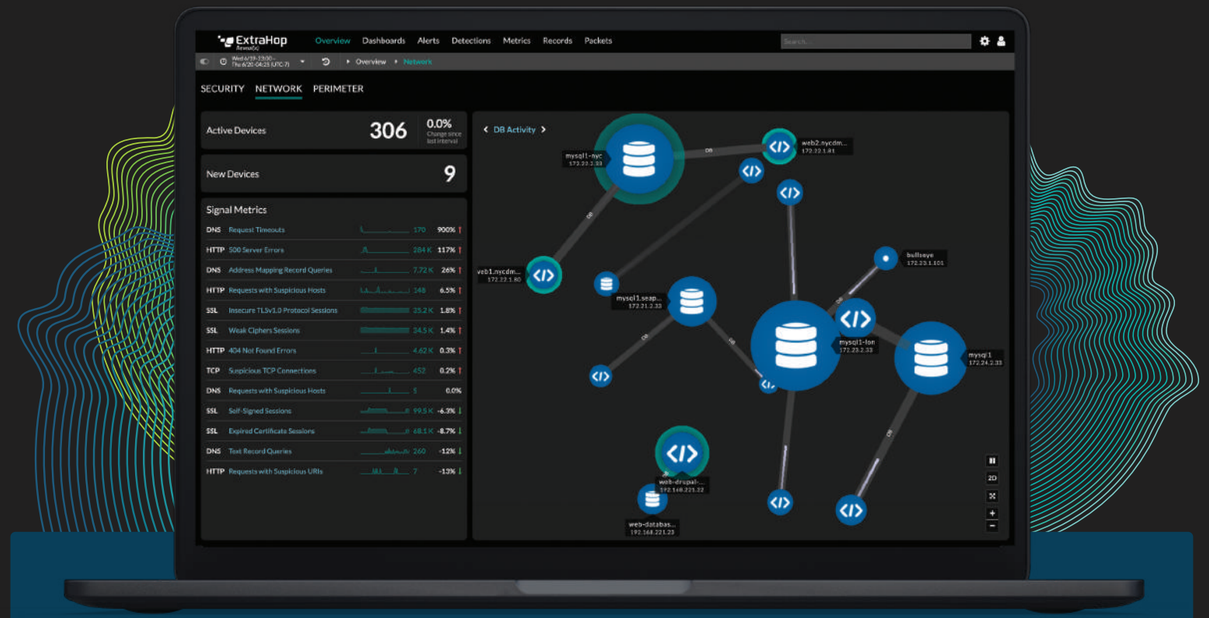
Solution SaaS de détection des menaces et réponse

Le cloud s'est avéré être un moteur formidable de croissance pour les entreprises et les services informatiques. Toutefois, pour les équipes SecOps, il présente le défaut d'accroître considérablement la surface d'attaque et expose ainsi l'entreprise à des risques nouveaux et inconnus. Malgré cette difficulté, de nombreuses entreprises choisissent tout de même l'évolutivité et la flexibilité du cloud. Néanmoins, les limites des outils de sécurité actuels, qui s'appuient généralement sur des journaux ou des agents, rendent difficiles la détection et l'investigation rapides des menaces complexes en raison de l'absence de visibilité continue sur l'ensemble des clouds privés virtuels.

Avec Reveal(x) Cloud, les entreprises peuvent adopter une approche native du cloud en matière de protection de leur surface d'attaque hybride. Reveal(x) Cloud propose des outils de détection des menaces, d'investigation et de réponse pour les workloads AWS dans le périmètre, ce qui permet aux équipes SecOps de débusquer les instances malveillantes et d'éliminer les risques posés par les erreurs de configuration, les API non sécurisées et les accès non autorisés. Reveal(x) Cloud est une solution Saas qui peut être déployée instantanément et sans agents. Elle permet une détection immédiate des actifs, une détection des menaces en temps réel et une réponse basée sur le machine learning.

Fonctionnement





FONCTIONNALITÉS DE REVEAL(X) CLOUD

Hygiène et conformité
Mettez en balance l'activité malveillante et le caractère stratégique des actifs pour configurer des alertes haute-fidélité permettant aux équipes de se concentrer sur les menaces posant le plus de risques.

Adoptez la vitesse du cloud
Fournissez une visibilité latérale pour assurer une détection des menaces et des réponses à des vitesses atteignant 25 Gbit/s par VPC.

Investigation et réponse automatisées
Automatisez les paramètres de sécurité et limitez la prolifération des outils en les intégrant à AWS CloudTrail, Amazon CloudWatch et VPC Flow Logs, aux systèmes d'orchestration, etc.

Gestion des identités et des accès
Analysez les charges utiles d'Active Directory pour signaler automatiquement les indicateurs de collecte d'identifiants et les attaques par force brute.

Décodage des protocoles des couches applicatives
Analysez et décodez le contenu et la charge utile des applications basées sur le cloud à grande échelle.

Déchiffrement à grande échelle
Déchiffrez le trafic chiffré SSL et TLS de manière passive et en temps réel afin d'assurer le maintien de la conformité avec une visibilité totale sur les menaces chiffrées.

UTILISATIONS DE REVEAL(X) CLOUD

Depuis une seule et même plateforme, les équipes de sécurité peuvent appliquer des contrôles sur les workloads sur site et dans le cloud, mais également implémenter des politiques de sécurité et de détection des menaces unifiées.

Détection des violations
Mappage des dépendances
Détection des menaces
Analyse du trafic chiffré
Conformité et audit
Analyse informatique
Inventaire et configuration
Évaluation des vulnérabilités
Recherche des menaces

INTÉGRATIONS

Amazon CloudTrail
Amazon CloudWatch
VPC FlowLogs
QRadar
DEMISTO
A PALO ALTO NETWORKS COMPANY
Phantom