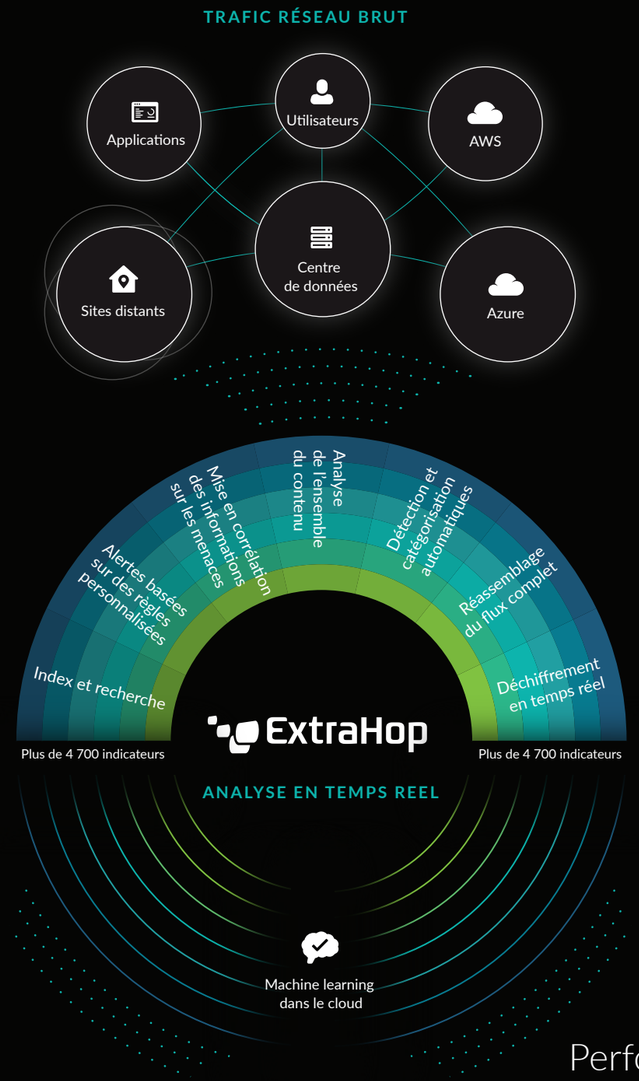


Sécurité

Détection des menaces haute-fidélité
Hygiène et conformité
Détection des actifs stratégiques
Investigation des menaces en un clic
Réponse automatisée via SOAR

RÉSULTATS POUR L'ENTREPRISE

Performance

Analyses d'applications en temps réel
Détection des anomalies par machine learning
Mappage des dépendances applicatives
Visibilité et hygiène de bout en bout
Investigation guidée

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

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

ExtraHop

Reveal(X) de ExtraHop

Détection et réponse réseau pour l'entreprise hybride

Reveal(x) est le seul produit d'analyse du trafic réseau proposant l'envergure, la rapidité et la visibilité dont les équipes de sécurité des entreprises ont besoin pour détecter les menaces, y répondre, et prendre du recul par rapport au bruit généré par des architectures réseau hybrides toujours plus complexes, les applications conteneurisées et le cloud.

VISIBILITÉ COMPLÈTE

Reveal(x) détecte et catégorise automatiquement chaque appareil communiquant sur le réseau et procède à un déchiffrement hors bande en temps réel pour permettre aux équipes de sécurité de voir les attaques masquées et les détails essentiels des transactions sans compromettre pour autant la conformité et la confidentialité. Grâce à une visibilité latérale complète, du centre de données au cloud en passant par la périphérie, vous comprendrez chaque facette de votre entreprise.

DÉTECTION EN TEMPS RÉEL

Reveal(x) intercepte les menaces en temps réel en extrayant plus de 4 700 caractéristiques des données de communication qui sont ensuite exploitées par notre moteur de machine learning dans le cloud et nos détections basées sur des règles personnalisables. Reveal(x) identifie automatiquement les actifs stratégiques et compare les groupes de pairs pour proposer des détections haute-fidélité associées à des scores de risque et des informations sur les menaces. Vous êtes ainsi en mesure de hiérarchiser vos efforts et de réagir en toute confiance.

INVESTIGATION GUIDÉE

Le workflow de Reveal(x) vous permet d'accéder au paquet associé à un événement de sécurité en quelques clics seulement : les heures passées à collecter et analyser manuellement les données appartiennent désormais au passé ! Les réponses instantanées permettent de réagir sans délai, en toute confiance. Nos intégrations efficaces avec des outils de sécurité comme Phantom, Splunk, Palo Alto et bien d'autres vous aident à prendre du recul par rapport au bruit des alertes, à automatiser les investigations et à agir suffisamment rapidement pour protéger vos clients.

DITES ADIEU À L'INCERTITUDE

Reveal(x) propose des détections en temps réel mappées à chaque étape du déroulement des attaques. Notre solution vous indique également les étapes à suivre et vous fournit des liens vers des cadres de sécurité de référence comme MITRE ATT&CK et le top 20 des contrôles de sécurité du CIS. Grâce à ce contexte, vous repérerez les menaces réelles jusqu'à 95 % plus rapidement.

Commande et contrôle	Reconnaissance	Exploitation	Mouvement latéral	Action sur objectif
Activité sortante	Analyses des ports	Empoisonnement LLMNR	Activité RDP/SSH suspecte	Ransomware
Adresses IP/URI suspectes	Énumération des utilisateurs	Chevauchement de fragments IP	Anomalies des groupes de pairs	Données chiffrées
Connexions suspectes	Tentatives de connexion	Attaques par force brute via RDP	Accès aux partages et fichiers	Transfert de données externes
Géolocalisation anormale	Recherches DNS inverses	Activité CIFS suspecte	Échecs de transactions	Exfiltration de bases de données
Plus de détections	Plus de détections	Plus de détections	Plus de détections	Plus de détections

UTILISATIONS DANS UNE OPTIQUE DE SÉCURITÉ PROACTIVE

DÉTECTER LES MENACES

Détection des failles et réponse
Détectez les menaces et renforcez ou automatisez les réponses

Sécurité hybride
Bénéficiez d'une détection et d'une réponse unifiées dans le cloud et sur site

Détection des menaces internes
Détectez, limitez et documentez les comportements risqués et malveillants

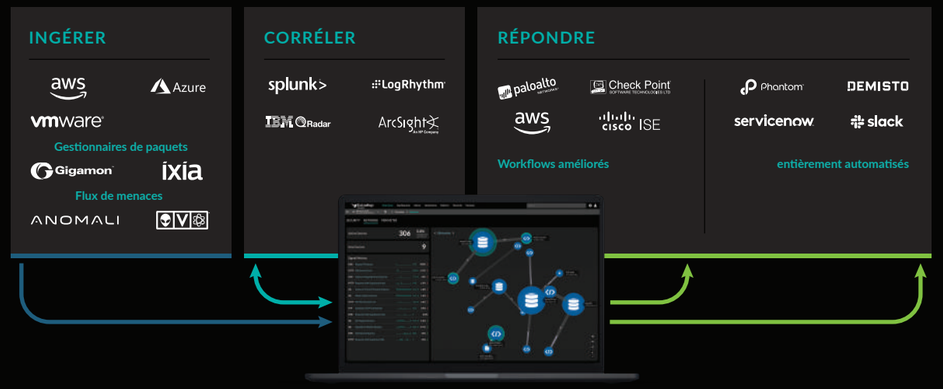
AMÉLIORER VOTRE APPROCHE

Productivité du SOC et du NOC
Partagez des données et intégrez des outils pour optimiser les performances des équipes

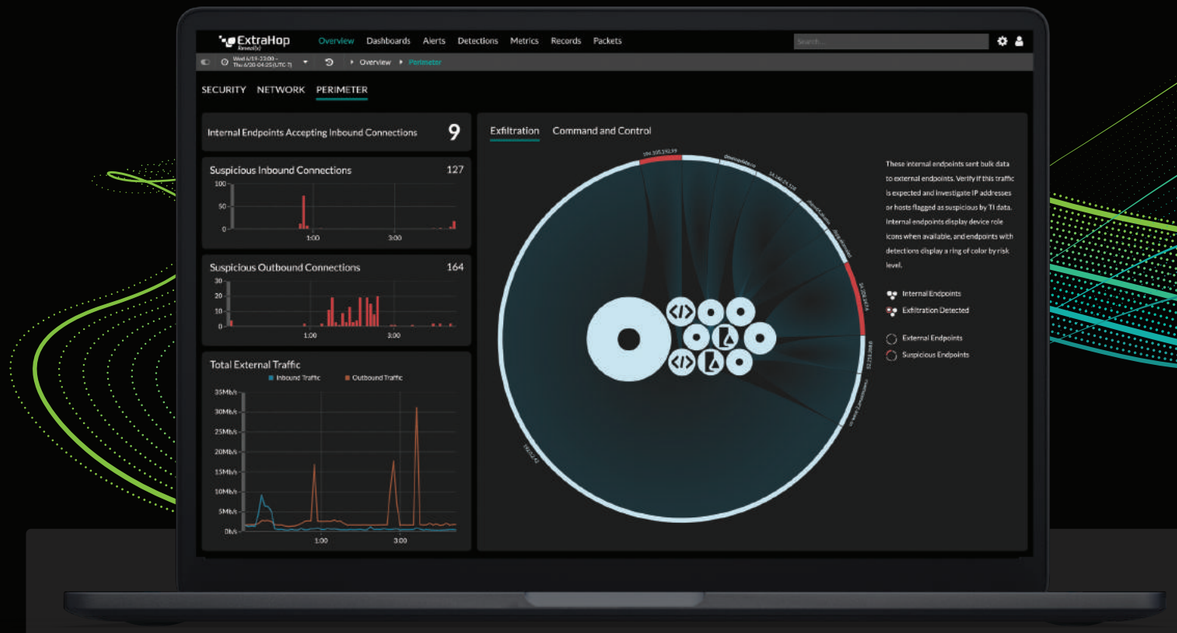
Approche Red Team/résultats des audits
Recherchez ou validez des inquiétudes et vulnérabilités

Hygiène informatique
Réalisez l'inventaire des appareils, auditez le chiffrement et mettez hors service les actifs vous faisant courir un risque

DOPEZ LA PUISSANCE DE VOS OUTILS D'ENTREPRISE



Les intégrations aux logiciels d'entreprise accélèrent et automatisent les réponses, ce qui permet à votre équipe de réduire le temps consacré à la résolution des incidents de sécurité de 59 %. Pour consulter la liste de nos intégrations, rendez-vous sur **www.extrahop.com/platform/integrations**



FONCTIONNALITÉS DE REVEAL(X)

Inventaire automatisé
Reveal(x) tient un inventaire à jour grâce à la détection et la catégorisation automatiques de chaque actif communiquant sur le réseau.

Déchiffrement du protocole PFS
Reveal(x) déchiffre les protocoles SSL/TLS 1.3 avec PFS de manière passive et en temps réel pour vous permettre de détecter les menaces cachées dans votre trafic chiffré.

Investigation automatisée
Reveal(x) enrichit chaque détection de contexte, d'une évaluation du risque, d'informations sur l'attaque et de conseils experts pour vous permettre de réagir en toute confiance.

Détections de groupes de pairs
En classant automatiquement les appareils dans des groupes de pairs très spécifiques, Reveal(x) est en mesure de repérer les comportements étranges avec un minimum de faux positifs.

Machine learning dans le cloud
Grâce à la modélisation prédictive et à un machine learning dans le cloud s'appuyant sur plus de 4 700 caractéristiques, Reveal(x) détecte, hiérarchise et fait apparaître les menaces en corrélation avec vos actifs stratégiques.

Orchestration des réponses en toute confiance
Reveal(x) gère la détection et l'investigation tandis que de puissantes intégrations avec des solutions comme Phantom et Palo Alto vous permettent de mettre en place des workflows de réponse automatisés et améliorés.

NOS CLIENTS VONT DROIT À L'ESSENTIEL

IDC

95 % D'AMÉLIORATION DU DÉLAI DE DÉTECTION

77 % D'AMÉLIORATION DU DÉLAI DE RÉSOLUTION

59 % DE RÉDUCTION DU TEMPS CONSACRÉ À LA RÉSOLUTION

25 % DE MENACES DE SÉCURITÉ SUPPLÉMENTAIRES IDENTIFIÉES