Présentation du système ExtraHop

Publié: 2025-02-13

Ce guide explique comment le système ExtraHop collecte et analyse vos données et comment les principaux composants et fonctionnalités du système vous aident à accéder aux détections, aux mesures, aux transactions et aux paquets concernant le trafic sur votre réseau.

Les flux de travail de surveillance des performances réseau vous permettent de surveiller la manière dont les services et les appareils interagissent entre eux et comment les transactions circulent entre la couche liaison de données (L2) et la couche application (L7) de votre réseau. Les workflows de détection et de réponse du réseau vous permettent d' examiner les données détectées, qu'il s'agisse de performances dégradées ou de comportements suspects, et fournissent une visibilité sur les appareils qui ont participé aux tactiques, techniques et procédures (TTP) MITRE ATT&CK associées à des campagnes d'attaque avancées en plusieurs étapes.

Vidéos Consultez la formation associée : Présentation du système ExtraHop

Architecture de plateforme

Le système ExtraHop est personnalisé avec des composants modulaires qui se combinent pour répondre à vos besoins environnementaux uniques.

Modules

Les modules ExtraHop offrent une combinaison de solutions, de composants et de services basés sur le cloud qui offrent de la valeur pour de multiples cas d'utilisation.

Des modules sont disponibles pour la détection et la réponse du réseau (NDR) et la surveillance des performances du réseau (NPM), ainsi que des modules supplémentaires pour les systèmes de détection d'intrusion (IDS) et la criminalistique des paquets.

Les administrateurs peuvent activer le contrôle d'accès basé sur les rôles (RBAC) en accordant aux utilisateurs l'accès au module NDR, au module NPM ou aux deux.

Surveillance des performances du réseau

Le module NPM permet aux utilisateurs privilégiés d'effectuer les types de tâches système suivants.

- Sélectionnez un tableau de bord comme page de destination par défaut.
- Configurez les alertes et les notifications par e-mail pour ces alertes.
- Afficher les détections de performances.

Détection et réponse du réseau

Le module NDR permet aux utilisateurs privilégiés d'effectuer les types de tâches système suivants.

- Consultez la page de présentation de la sécurité.
- Afficher les détections de sécurité.
- Consultez, créez et modifiez des enquêtes.
- Consultez les briefings sur les menaces.

Les utilisateurs autorisés à accéder aux deux modules sont autorisés à effectuer toutes ces tâches. Consultez les Guide de migration pour en savoir plus sur la migration des utilisateurs vers un accès basé sur les rôles à l' aide de ces modules.

Ces modules supplémentaires sont également disponibles pour des cas d'utilisation spécifiques :

Packet Forensics

Le module Packet Forensics peut être combiné au module NDR ou NPM pour fournir une capture, un stockage et une récupération complets des paquets.

Systèmes de détection d'intrusion

Le module IDS doit être combiné au module NDR et fournit des détections basées sur des signatures IDS conformes aux normes de l'industrie. La plupart des capteurs de paquets ExtraHop sont éligibles au module IDS, à condition que le capteur soit autorisé pour le module NDR.

Note: Débit peut être affectée lorsque plusieurs modules sont activés sur la sonde.

Caractéristiques

Le système ExtraHop fournit un ensemble complet de fonctionnalités qui vous permet d'organiser et d'analyser les détections, les mesures, les enregistrements et les paquets associés au trafic sur votre réseau.

L'accès au module et au système est déterminé par privilèges d'utilisateur qui sont gérés par votre administrateur ExtraHop.

Caractéristiques globales

Les fonctionnalités suivantes sont disponibles dans tous les systèmes ExtraHop et ne nécessitent pas de modules spécifiques.

- Vue d'ensemble du réseau
- Vue d'ensemble du périmètre
- Tableaux de bord personnalisés
- Cartes d'activités
- tableau de bord Active Directory
- tableau de bord génératif de l'IA
- Rapports de tableau de bord planifiés
- Suivi des détections
- Actifs
- Disques
- Paquets
- Intégrations (RevealX 360 uniquement)
- Accès à l'API
- Priorités d'analyse
- Catalogue métrique
- Lots
- éléments déclencheurs
- Assistant de recherche IA (actifs et dossiers)

Caractéristiques du module NDR

Les fonctionnalités suivantes sont disponibles dans les systèmes ExtraHop dotés du module Network Detection and Response (NDR).

- Aperçu de la sécurité
- Assistant de recherche IA
- Rapports sur les opérations de sécurité
- Tableaux de bord de sécurité intégrés
- Détections de sécurité
- Carte MITRE
- Enquêtes
- Règles de réglage pour les détections de sécurité
- Règles de notification pour les détections de sécurité et les briefings sur les menaces
- Exposés sur les menaces
- Renseignements sur les menaces

- Analyse de fichiers
- Extraction de fichiers (analyse des paquets requise)

Caractéristiques du module NPM

Les fonctionnalités suivantes sont disponibles dans les systèmes ExtraHop dotés du module Network Performance Management (NPM).

- Tableaux de bord de performance intégrés
- Détections de performances
- Règles de réglage pour les détections de performances
- Règles de notification pour les détections de performances
- Alertes

Fonctionnalités de Packet Forensics

Les fonctionnalités suivantes sont disponibles dans les systèmes ExtraHop dotés du module Packet Forensics.

- Capture de paquets
- Assistance pour Packetstore
- Extraction de fichiers (NDR requis)

Caractéristiques de l'IDS

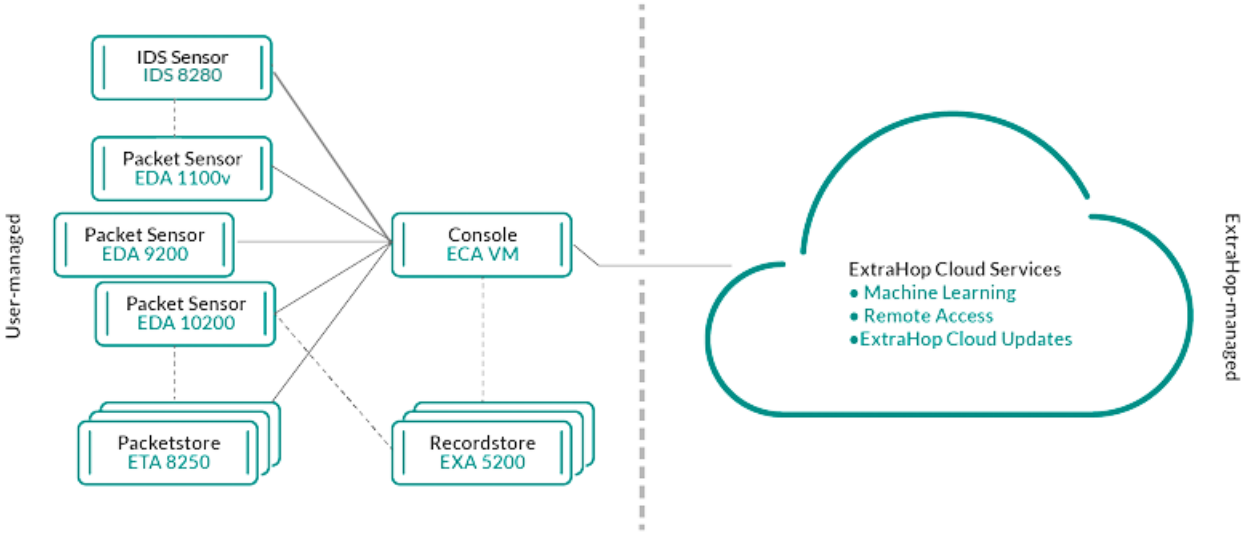
Les fonctionnalités suivantes sont disponibles dans les systèmes ExtraHop dotés du module Intrusion Detection System (IDS).

- Détections IDS

Des solutions

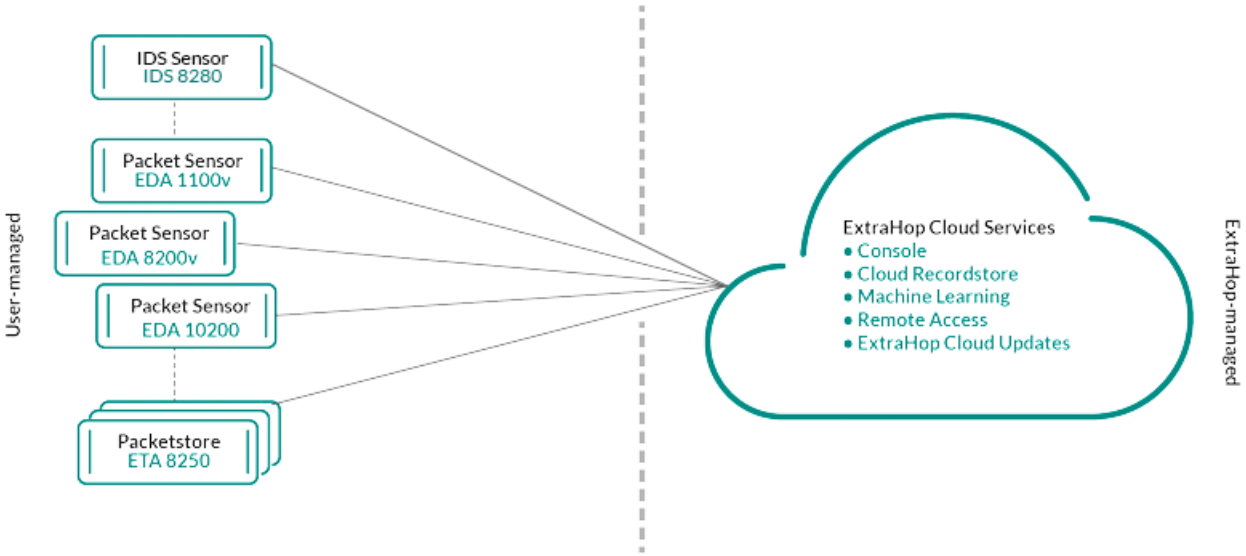
RevealX Enterprise

RevealX Enterprise est une solution autogérée qui comprend capteurs, consoles, les magasins de paquets, les magasins de disques et l'accès aux services cloud ExtraHop.



RevealX 360

RevealX 360 est une solution logicielle en tant que service (SaaS) qui comprend capteurs et packetstores et comprend un espace de stockage des enregistrements basé sur le cloud avec Standard Investigation, un console, et accès aux services cloud ExtraHop.



Composantes

Chaque solution propose un ensemble de composants en fonction de vos besoins environnementaux : capteurs, magasins de paquets, magasins de disques et console pour une gestion centralisée et des vues de données unifiées.

Capteurs de paquets

Les capteurs de paquets capturent, stockent et analysent les données métriques relatives à votre réseau. Plusieurs niveaux d'analyse, de collecte et de stockage des données sont disponibles en fonction de la taille de la sonde. Ces capteurs sont disponibles dans les modules NPM et NDR en tant qu'options physiques, virtuelles et basées sur le cloud, dans des tailles adaptées à vos besoins d'analyse.

Capteurs IDS

Les capteurs du système de détection d'intrusion (IDS) s'intègrent aux capteurs de paquets pour générer des détections basées sur la signature IDS standard de l'industrie. Les capteurs IDS sont déployés en tant que module complémentaire au module NDR. Les capteurs IDS sont une appliance physique associée à une sonde réseau d'analyse de paquets et sont disponibles pour les environnements RevealX 360 ou RevealX Enterprise.

Capteurs de débit

Les capteurs de flux sont disponibles pour RevealX 360 uniquement et collectent exclusivement les journaux de flux VPC afin que vous puissiez voir le trafic géré par les services AWS SaaS.

Disquaires

Les magasins de disques intègrent des capteurs et consoles pour stocker les enregistrements de transactions et de flux qui peuvent être interrogés depuis l'ensemble du système ExtraHop. Les magasins d'enregistrements peuvent être déployés en tant qu'options physiques ou virtuelles autonomes et peuvent être pris en charge en tant que connexions tierces à Splunk ou BiqQuery depuis RevealX Enterprise. RevealX 360 avec Standard Investigation fournit un espace de stockage des enregistrements entièrement hébergé et basé sur le cloud. Les magasins de disques sont disponibles dans des packages avec les modules NPM et NDR.

Magasins de paquets

Les magasins de paquets s'intègrent à des capteurs et consoles pour fournir PCAP en continu et un espace de stockage suffisant pour des enquêtes plus approfondies et des besoins en matière de criminalistique. Les Packetstores peuvent être déployés en tant qu'options physiques ou virtuelles autonomes et sont disponibles en tant que module complémentaire Packet Forensics pour les modules NPM et NDR.

Consoles

Les consoles fournissent une interface basée sur un navigateur qui fournit un centre de commande pour tous les composants connectés. Consoles peuvent être déployés en tant qu'options autonomes virtuelles ou basées sur le cloud pour RevealX Enterprise et sont inclus dans RevealX 360.

Le tableau suivant donne un aperçu des options disponibles pour chaque solution.

	RevealX Enterprise		RevealX 360	
	Physique	Virtuel/Cloud	Physique	Virtuel/Cloud
sonde à paquets	ANNÉE 1200 ÉD. 6200 ÉD. 8200 ÉD. 8320 ÉD. 9200 ÉD. 9300 ÉD. 10200 ÉD. 10300	AWS EDA 1100 v EDA 1100v Azure GCP EDA 1100 V GCP EDA 6320v GCP EDA 8370 V KVM Linux EDA 1100 v VMware EDA 1100 v VMware EDA 6100 v AWS EDA 6100v EDA 6100v Azure AWS EDA 8200v RevealX Ultra AWS à 1 Gbit/s et 10 Gbit/s	ANNÉE 1200 ÉD. 6200 ÉD. 8200 ÉD. 8320 ÉD. 9200 ÉD. 9300 ÉD. 10200 ÉD. 10300	AWS EDA 1100 v EDA 1100v Azure GCP EDA 1100 V GCP EDA 6320v GCP EDA 8370 V KVM Linux EDA 1100 v VMware EDA 1100 v AWS EDA 6100v EDA 6100v Azure VMware EDA 6100 v AWS EDA 8200v RevealX Ultra AWS à 1 Gbit/s et 10 Gbit/s

	RevealX Enterprise		RevealX 360	
		RevealX Ultra GCP 1 Gbit/s et 10 Gbit/s		RevealX Ultra GCP 1 Gbit/s et 10 Gbit/s
sonde IDS	ID 8280 ID 9380	IDS 1280v pour VMware IDS 6280 v pour VMware	ID 8280 ID 9380	IDS 1280v pour VMware IDS 6280 v pour VMware
sonde de débit	N/A	N/A	N/A	EFC 1291v AWS (PVC) EFC 1292 v (NetFlow)
Magasin de paquets	ET 6150 ÉTÉ 8250	AWS ETA 1150 v ETA 1150v Azure GCP ETA 1150 V VMware ETA 1150 v VMWare ETA 6150v	ET 6150 ÉTÉ 8250	AWS ETA 1150 v ETA 1150v Azure GCP ETA 1150 V VMware ETA 1150 v VMWare ETA 6150v Inclus dans les abonnements Ultra
Disquaire	EXAMEN 5200	AWS EXA 5100 v EXA 5100 v Azure Hyper-V EXA 5100 V KVM Linux EXA 5100 v	N/A	Inclus dans les abonnements Premium et Ultra

	RevealX Enterprise		RevealX 360	
		VMWare EXA 5100 v		
Console	N/A	LOIS DE LA CEA ECA Azure ECA GCP ECA Hyper-V KVM ECA Linux ECA VMware	N/A	Inclus dans tous les abonnements

Services cloud ExtraHop

Services cloud ExtraHop met automatiquement à jour les capteurs en fonction des nouvelles détections et des renseignements sur les menaces critiques, ainsi que des améliorations apportées aux fonctionnalités, et permet aux équipes chargées de votre compte d'accéder à une assistance à distance et à des services professionnels.

Analyse des capteurs intelligents

Le système ExtraHop propose une interface basée sur un navigateur avec des outils qui vous permettent d' explorer et de visualiser les données, d'étudier les résultats dans des flux de travail ascendants et descendants, et de personnaliser la manière dont vous collectez, visualisez et partagez les données de votre réseau. Les utilisateurs avancés peuvent automatiser et écrire des scripts pour les tâches administratives et les tâches utilisateur via API REST ExtraHop et personnalisez la collecte de données via API ExtraHop Trigger, qui est un outil IDE JavaScript.

Au cœur du système ExtraHop se trouve un sonde qui capture, stocke et analyse les données métriques relatives à votre réseau et propose différents niveaux d'analyse, de collecte et de stockage des données en fonction de vos besoins. Sondes sont dotés d'un espace de stockage prenant en charge 30 jours de rétrospective métrique. Notez que la rétrospective réelle varie en fonction des modèles de trafic, des taux de transaction, du nombre de points de terminaison et du nombre de protocoles actifs.

Les consoles font office de centre de commande avec des connexions à plusieurs capteurs, des magasins de disques et des magasins de paquets répartis dans les centres de données et les succursales. Tous les déploiements de RevealX 360 incluent une console ; RevealX Enterprise peut déployer des variantes virtuelles ou cloud.

Les consoles fournissent des vues de données unifiées sur tous vos sites et vous permettent de synchroniser certaines configurations avancées (telles que déclencheurs et alertes) et paramètres (paramètres de réglage, priorités d'analyse, et disquaires).

Les sections suivantes décrivent les principaux composants fonctionnels du système ExtraHop et la manière dont ils fonctionnent ensemble.

Types de capteurs

Le type de sonde vous déployez détermine le type de données collectées, stockées et analysées.

Données filaires
Les capteurs de paquets et les capteurs du système de détection d'intrusion (IDS) observent passivement les paquets non structurés via un miroir de ports ou tapent et stockent les données dans la banque de données locale. Les données des paquets sont soumises à un traitement de flux en temps réel qui transforme les paquets en données filaires structurées selon les étapes suivantes :

1. Les machines à états TCP sont recréées pour effectuer un réassemblage complet.
2. Les paquets sont collectés et regroupés en flux.
3. Les données structurées sont analysées et traitées de la manière suivante :
   - Les transactions sont identifiées.
   - Les appareils sont automatiquement découverts et classés en fonction de leur activité.
   - Des métriques sont générées et associées à des protocoles et à des sources, et les données métriques sont ensuite agrégées en cycles métriques.
4. Au fur et à mesure que de nouvelles métriques sont générées et stockées et que la banque de données est pleine, les plus anciennes métriques existantes sont remplacées selon le principe du premier entré, premier sorti (FIFO).

Données de flux
Un flux est un ensemble de paquets qui font partie d'une connexion unique entre deux terminaux. Flux capteurs sont disponibles pour RevealX 360 et offrent une visibilité continue du réseau sur la base des journaux de flux VPC afin de sécuriser les environnements AWS. Les journaux de flux VPC vous permettent de capturer des informations sur le trafic IP entrant et sortant des interfaces réseau de votre VPC et sont enregistrés sous forme d'enregistrements de journaux de flux, qui sont des événements de journal composés de champs décrivant le flux de trafic. Ces données de journal vous permettent de rechercher des menaces à l'aide de détections avancées par apprentissage automatique.

Les journaux de flux sont ingérés, dédupliqués, puis regroupés en flux. Les flux sont ensuite enrichis avec des données (telles que des adresses MAC) demandées à partir des API AWS EC2.

Les flux sont ensuite analysés et traités de la manière suivante :

- Les appareils sont automatiquement découverts et classés en fonction de leur activité observée sur des ports spécifiques.
- Les métriques L2-L4 de base sont générées et agrégées en cycles métriques.
- Les types d'enregistrement ExFlow sont générés et publiés.

Métriques, enregistrements et paquets

Les capteurs ExtraHop collectent et stockent plusieurs niveaux d'interaction réseau sous forme de métriques. Les métriques sont des observations agrégées concernant les interactions entre les points de terminaison au fil du temps. Les packetstores collectent et stockent les données brutes transférées entre deux points de terminaison sous forme de paquets. Magasins de disques collectez et stockez des enregistrements, qui sont des informations structurées sur les transactions, les messages et les flux réseau.

Vous pouvez visualiser et interroger toutes ces interactions à partir de capteurs individuels ou d'un console qui est lié à un déploiement complexe de capteurs, de magasins de paquets et de magasins de disques.

Par exemple, lorsqu'un client envoie une requête HTTP à un serveur Web, voici le contenu de chaque type de données :

- Le paquet contient les données brutes qui ont été envoyées et reçues lors de l' interaction.
- L'enregistrement associé contient les métadonnées horodatées relatives à l' interaction : date à laquelle la demande a eu lieu, adresse IP du client et du serveur, URI demandé, éventuels messages d'erreur.
- La métrique associée (requêtes HTTP) contient un agrégat de cette interaction avec les autres interactions observées au cours de la période spécifiée, telles que le nombre de demandes effectuées,

le nombre de demandes réussies, le nombre de clients ayant envoyé des demandes et le nombre de serveurs ayant reçu les demandes.

Les métriques et les enregistrements peuvent être personnalisés pour extraire et stocker des métadonnées spécifiques à l'aide de JavaScript déclencheurs. Alors que le système ExtraHop est terminé 4600 métriques intégrées, vous souhaiterez peut-être créer un métrique personnalisée qui collecte et agrège les erreurs 404 uniquement à partir de serveurs Web critiques. Et vous souhaiterez peut-être maximiser votre espace de stockage d'enregistrements uniquement collecte des transactions survenues via un port suspect.

Découverte des appareils

Une fois qu'un équipement est découvert, le système ExtraHop commence à collecter des métriques en fonction du niveau d'analyse configuré pour cet équipement. Tu peux Trouvez un équipement par leur adresse MAC, leur adresse IP ou leur nom (tel qu'un nom d'hôte observé à partir du trafic DNS, le nom NetBIOS, le nom du Cisco Discovery Protocol (CDP), le nom DHCP ou un nom personnalisé que vous avez attribué à l'équipement).

Le système ExtraHop peut découvrir et suivre les appareils par leur adresse MAC (L2 Discovery) ou par leur adresse IP (L3 Discovery). L2 Discovery offre l'avantage de suivre les métriques d'un équipement même si l'adresse IP est modifiée ou réattribuée par le biais d'une requête DHCP. Par défaut, le système ExtraHop est configuré pour L2 Discovery.

Les adresses IPv4 et IPv6 des appareils sont découvertes à partir des messages ARP (Address Resolution Protocol), des réponses du protocole NDP (Neighbor Discovery Protocol), des diffusions locales ou du trafic de multidiffusion du sous-réseau local. L'adresse MAC et l'adresse IP des appareils apparaissent dans les résultats de recherche sur l'ensemble du système avec les informations relatives à l'équipement.

Découverte L2

Dans L2 Discovery, le système ExtraHop crée une entrée d'équipement pour chaque adresse MAC locale découverte via le fil. Les adresses IP sont mappées à l'adresse MAC, mais les métriques sont stockées avec l'adresse MAC de l'équipement même si l'adresse IP change.

Les adresses IP observées en dehors des domaines de diffusion surveillés localement sont agrégées sur l'un des routeurs entrants de votre réseau. Si un équipement envoie une demande DHCP via un routeur agissant en tant qu'agent de relais DHCP, le système ExtraHop détecte et mappe l'adresse IP à l'adresse MAC de l'équipement. Si l'adresse IP de l'équipement change lors d'une demande ultérieure via l'agent de relais DHCP, le système ExtraHop met à jour son mappage et continue de suivre les métriques de l'équipement par adresse MAC.

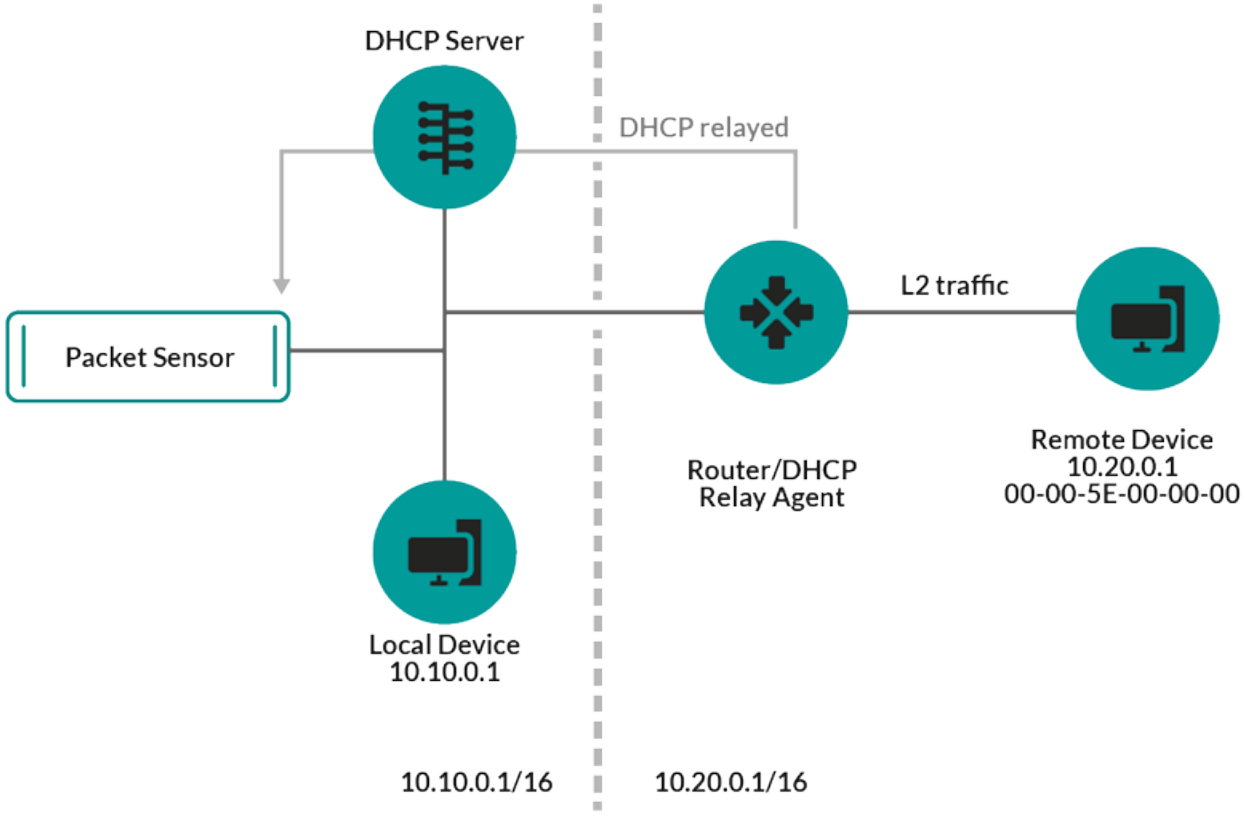


Figure 1: L'adresse MAC et l'adresse IP de l'équipement distant sont découvertes.

Si aucun agent de relais DHCP n'est configuré, les périphériques distants peuvent être découverts par leur adresse IP via Découverte L3 à distance.

L3 Discovery

Dans L3 Discovery, le système ExtraHop crée et lie deux entrées pour chaque équipement local découvert : une entrée parent L2 avec une adresse MAC et une entrée enfant L3 avec les adresses IP et l'adresse MAC.

Voici quelques considérations importantes concernant la découverte de la L3 :

- Si le proxy ARP est activé sur un routeur, le système ExtraHop crée un équipement L3 pour chaque adresse IP pour laquelle le routeur répond aux demandes ARP.
- Si un proxy ARP est configuré sur votre réseau, le système ExtraHop peut détecter automatiquement les appareils distants.
- Les métriques L2 qui ne peuvent pas être associées à un équipement enfant L3 particulier (par exemple, le trafic de diffusion L2) sont associées à l'équipement parent L2.

Découverte L3 à distance

Si le système ExtraHop détecte une adresse IP à laquelle aucun trafic ARP ou NDP n'est associé, cet équipement est considéré comme un équipement distant. Les appareils distants ne sont pas automatiquement découverts, mais vous pouvez ajouter une plage d'adresses IP distantes et découvrir les appareils situés en dehors du réseau local. Une entrée d'équipement est créée pour chaque adresse IP observée dans la plage d' adresses IP distantes. (Les appareils distants ne possèdent pas d'entrées parent L2.)

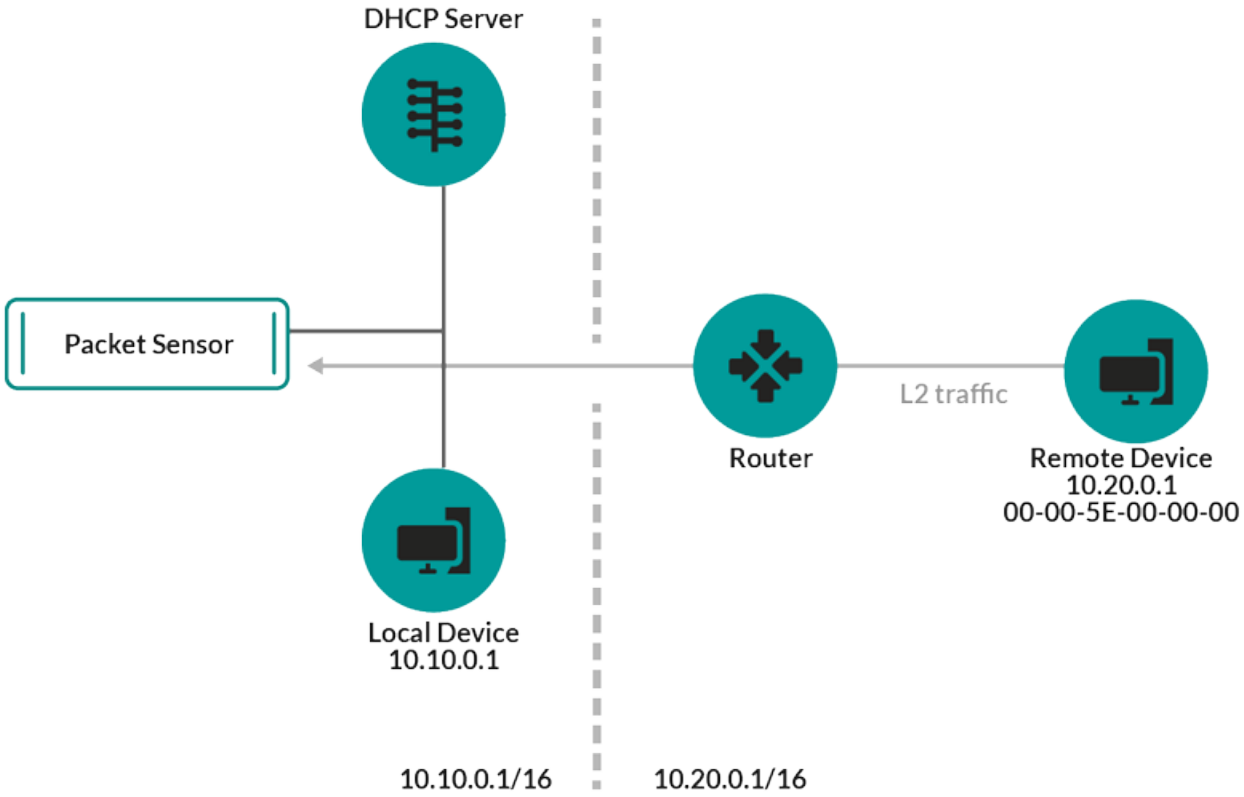


Figure 2: Seule l'adresse IP de l'équipement distant est découverte.

Voici quelques recommandations concernant le moment où configurer Remote L3 Discovery :

- Les appareils de vos clients se trouvent sur un segment du réseau qui n'est pas directement connecté.
- Votre organisation dispose d'un bureau distant sans système ExtraHop sur site, mais les utilisateurs de ce site accèdent aux ressources du centre de données central qui sont directement surveillées par un système ExtraHop . Les adresses IP du site distant peuvent être découvertes en tant que périphériques.
- Un service cloud ou un autre type de service hors site héberge vos applications distantes et possède une plage d'adresses IP connue. Les serveurs distants compris dans cette plage d'adresses IP peuvent être suivis individuellement.

Découverte du VPN

Découverte du VPN permet au système ExtraHop de corréler les adresses IP privées RFC-1918 attribuées aux clients VPN avec leurs adresses IP externes publiques. Cette visibilité accrue sur le trafic nord-sud réduit les obstacles lors de l'enquête sur les incidents de sécurité et les problèmes de performance impliquant des clients VPN externes. (Cette fonctionnalité nécessite une passerelle VPN assignée manuellement par l'utilisateur.)

Empreinte logicielle

Dans le système ExtraHop, les empreintes digitales du système d'exploitation (OS) et du logiciel offrent une valeur de sécurité significative en permettant une identification et une classification précises des équipements. Cette visibilité granulaire permet aux équipes de sécurité de détecter les menaces et d'y répondre plus efficacement et d'améliorer la recherche des menaces et les réponses aux incidents.

L'empreinte digitale logicielle fonctionne en faisant correspondre les champs du réseau observés passivement à une collection organisée d'empreintes digitales stockées dans notre base de données afin de permettre une correspondance performante. Ces empreintes digitales sont mises à jour dans le cloud et transmises aux capteurs de paquets via les services cloud ExtraHop.

Le système ExtraHop observe de manière opportuniste les empreintes digitales qui apparaissent naturellement sur le réseau, contrairement à d'autres produits qui recherchent activement ces informations. Le système ExtraHop possède actuellement plus de 45 champs réseau (via différents protocoles) qui sont surveillés passivement pour identifier le système d'exploitation et les logiciels de l'équipement. Ces champs vont des en-têtes de serveur HTTP aux sujets de certificat X.509, en passant par les fournisseurs DHCP et bien d'autres encore.

Déduplication des trames logicielles

Le système ExtraHop supprime les trames et paquets L2 et L3 dupliqués lorsque les métriques sont collectées et agrégées à partir de l'activité de votre réseau par défaut.

Le État de santé du système La page contient des graphiques qui affichent les paquets dupliqués L2 et L3 qui ont été supprimés par le système ExtraHop. La déduplication fonctionne par défaut sur les ports 10 Gbit/s.

déduplication L2

La déduplication L2 supprime les trames Ethernet identiques, où l'en-tête Ethernet et la charge utile doivent correspondre. Le système ExtraHop vérifie la présence de doublons et supprime uniquement le paquet immédiatement précédent dans le monde entier si le doublon arrive à moins d'une milliseconde du paquet d'origine. La duplication L2 n'existe généralement que si le même paquet est vu dans le flux de données, ce qui est généralement lié à un problème de port de duplication.

déduplication L3

La déduplication L3 supprime les paquets TCP ou UDP avec des champs d'identification d'adresse IP identiques sur le même flux, où seul le paquet IP doit correspondre. Le contenu de tous les en-têtes qui précèdent l' en-tête IP en cours de vérification peut être différent. La déduplication L3 n'est actuellement prise en charge que pour IPv4, et non pour IPv6. Le système ExtraHop recherche les doublons et supprime uniquement le paquet immédiatement précédent du flux si le doublon arrive à moins d'une milliseconde du paquet d'origine et si le paquet se déplace dans la même direction. Pour qu'un paquet soit dédupliqué, aucun autre paquet ne peut être reçu entre les deux paquets dupliqués. En outre, les paquets doivent avoir la même longueur et le même champ d'identification d'adresse IP, et les paquets TCP doivent également avoir la même somme de contrôle TCP.

Par défaut, les flux entre les VLAN sont activés, et comme la déduplication L3 fonctionne sur une base par flux, la déduplication L3 supprime le même paquet traversant différents VLAN. La déduplication L3 est souvent le résultat de la mise en miroir du même trafic sur plusieurs interfaces du même routeur, et ce trafic peut apparaître sous forme de retransmissions TCP superflues dans le système ExtraHop.

Détection des menaces

Le système ExtraHop offre à la fois un apprentissage automatique et des fonctionnalités basées sur des règles détections qui identifient les menaces actives ou potentielles, les faiblesses du réseau vulnérables aux exploits et les configurations sous-optimales susceptibles de dégrader les performances du réseau.

En outre, graphiques, visualisations, et cartes d'activité des équipements permettre une chasse proactive aux menaces.

Réglage de la détection

Réduisez le bruit et faites uniquement apparaître les détections critiques en ajoutant des informations sur votre réseau qui permettent d'identifier les paramètres connus tels que les domaines fiables et les scanners de vulnérabilités.

En outre, vous pouvez créer des règles d'exceptions qui masquent des détections ou des participants spécifiques et réduisent davantage les bruits indésirables.

Localité du réseau
Par défaut, tout équipement doté d'une adresse IP RFC1918 (incluse dans un bloc CIDR 10/8, 172.16/12 ou 192.168/16) est classé sur le système en tant que périphérique interne.

Cependant, étant donné que certains environnements réseau incluent des adresses IP non conformes à la RFC1918 dans leur réseau interne, vous pouvez modifier la classification interne ou externe des adresses IP depuis la page Localités du réseau.

Renseignements sur les menaces
Le système ExtraHop comprend des renseignements sur les menaces flux d'ExtraHop et Crowdstrike Falçon qui sont mis à jour via le cloud à mesure que de nouvelles menaces sont découvertes. Vous pouvez également ajouter des collections de menaces auprès d'un tiers.

Exposés sur les menaces
Exposés sur les menaces fournir des informations sur les menaces imminentes qui ciblent les réseaux. Les détections mises à jour, les requêtes ciblées sur les enregistrements et les paquets, ainsi que les appareils concernés sont présentés comme point de départ de votre investigation, accessibles depuis le Aperçu de la sécurité page.

Intégrations
RevealX 360 propose plusieurs intégrations tierces qui peuvent améliorer la gestion de la détection et des réponses et fournir une meilleure visibilité sur le trafic réseau.

Cortex XSOAR

Exportez les détections ExtraHop, exécutez des playbooks de réponse et interrogez les détails de l'équipement dans Cortex XSOAR.

Crowd Strike

Consultez les détails sur les appareils CrowdStrike et conservez ces appareils depuis le système ExtraHop.

Microsoft 365

Importez les détections et les événements Microsoft 365, surveillez les mesures Microsoft 365 dans des tableaux de bord intégrés et affichez les détails des événements à risque dans les enregistrements.

Décryptage du protocole Microsoft

Déchiffrez le trafic via les protocoles Microsoft tels que LDAP, RPC, SMB et WSMan pour améliorer la détection des attaques de sécurité dans votre environnement Microsoft Windows.

QRadar

Exportez et visualisez les détections ExtraHop dans votre QRadar SIEM.

Solution SIEM de sécurité d'entreprise Splunk

Exportez et visualisez les détections ExtraHop dans votre Splunk SIEM.

Splunk SOAR

Exportez et visualisez les détections, les métriques et les paquets ExtraHop dans votre solution Splunk SOAR.