Vue d'ensemble du périmètre

Publié: 2024-02-13

L'aperçu du périmètre affiche des graphiques et des visualisations interactives qui vous aident à surveiller le trafic entrant et sortant de votre réseau via des connexions avec des points de terminaison externes.

Trafic périmétrique

Les graphiques du trafic périmétrique fournissent une vue d'ensemble du trafic des équipements avec des connexions externes.

Trafic entrant

Ce nombre indique le volume total de trafic entrant pendant l' intervalle de temps sélectionné. Cliquez sur le nombre pour afficher le taux de transfert des données en provenance de points de terminaison externes et effectuez une analyse détaillée par site ou par conversation.

Trafic sortant

Ce nombre indique le volume total de trafic sortant pendant l' intervalle de temps sélectionné. Cliquez sur le nombre pour afficher le taux de transfert des données vers des points de terminaison externes et effectuez une analyse détaillée par site ou par conversation.

Appareils acceptant les connexions entrantes

Ce nombre indique le nombre d'appareils qui ont accepté des connexions entrantes en provenance de points de terminaison externes pendant l'intervalle de temps sélectionné. Cliquez sur le nombre pour ouvrir une page de présentation des groupes d'équipements qui affiche la liste des appareils, les données de trafic et l'activité des protocoles.

Connexions entrantes

Ce nombre indique le nombre de connexions entrantes initiées par des points de terminaison externes. Cliquez sur le décompte pour afficher une vue détaillée de ces conversations.

Connexions entrantes suspectes

Ce graphique indique le nombre de connexions initiées par des points de terminaison externes suspects. ExtraHop identifie les points de terminaison suspects via renseignements sur les menaces données. Cliquez sur le graphique pour ouvrir une vue filtrée de ces conversations.

Connexions sortantes suspectes

Ce nombre indique le nombre de connexions initiées par des points de terminaison internes avec des points de terminaison externes suspects. ExtraHop identifie les points de terminaison suspects via renseignements sur les menaces données. Cliquez sur le graphique pour ouvrir une vue filtrée de ces conversations.

Connexions peu communes

(Reveal (x) 360 uniquement) Ce nombre indique le nombre de connexions sortantes de votre réseau vers des adresses IP qui ne sont normalement pas visitées ou qui n'ont jamais été visitées par le passé. Cliquez sur le graphique pour ouvrir une vue filtrée de ces conversations.

Visualisation de Halo

La visualisation Halo fournit deux vues de vos connexions réseau à des points de terminaison externes : les services cloud et les téléchargements volumineux.

Les extrémités externes apparaissent sur l'anneau extérieur avec des connexions aux extrémités internes et apparaissent sous forme de cercles au milieu de la visualisation. Ces visualisations vous permettent de hiérarchiser vos investigation pour les connexions marquées par des détections à haut risque ou pour les appareils de grande valeur.

Pour aider à identifier les points finaux à fort trafic, la taille des cercles intérieurs et extérieurs augmente à mesure que le volume de trafic augmente. Dans certains cas, la taille des cercles intérieurs et des segments de l'anneau extérieur peut être augmentée pour des raisons de lisibilité. Cliquez sur un point de terminaison pour afficher des informations précises sur le trafic.

Cliquez **Services dans le cloud** pour visualiser les connexions entre les terminaux internes et les fournisseurs de services cloud. Les fournisseurs de services cloud et la quantité de données envoyées ou reçues apparaissent dans le panneau d'informations situé à droite. Vous pouvez basculer entre les vues qui affichent **Octets sortants** aux fournisseurs et **Octets entrants** à votre réseau.

Cliquez **Importations volumineuses** pour visualiser les connexions entre les points de terminaison internes et externes où plus de 1 Mo de données ont été transférés en une seule transmission depuis votre réseau vers un point de terminaison externe. Les points de terminaison externes et la quantité de données téléchargées apparaissent dans le panneau d'informations situé à droite.

Voici quelques manières d'interagir avec ces visualisations de halo :

- Passez la souris sur les points de terminaison ou les connexions pour afficher les noms d'hôte et les adresses IP disponibles.
- Passez la souris sur les points de terminaison ou les connexions pour mettre en surbrillance les éléments de liste correspondants sur la droite. De même, passez la souris sur les éléments de la liste pour mettre en évidence les points de terminaison et les connexions correspondants dans la visualisation du halo.
- Cliquez sur les extrémités ou les connexions dans la visualisation en halo pour maintenir le focus et afficher des informations précises sur le trafic et les liens correspondant à votre sélection sur la droite.
- Cliquez sur un point de terminaison externe dans la visualisation ou la liste du halo pour afficher le volume total de trafic entrant ou sortant associé au point de terminaison et aux points de terminaison internes connectés.
- Cliquez sur un point de terminaison interne dans la liste pour afficher les propriétés de l'équipement et accéder aux liens vers les informations associées, telles que les détections, les enregistrements ou les paquets.
- Cliquez sur la loupe à côté d'un point de terminaison dans la liste pour afficher les enregistrements associés à ce point de terminaison.
- Au bas de la liste des services cloud, basculez entre les vues qui affichent les octets sortants et les octets entrants sur votre réseau.
- Ajustez l'intervalle de temps pour afficher les connexions à des heures spécifiques, telles que les activités inattendues en soirée ou le week-end.

Visualisation de cartes

L'onglet Géolocalisation fournit une carte du monde du trafic entre les points de terminaison internes et les emplacements géographiques, qui sont surlignés dans une couleur contrastante sur la carte. L'intensité de la couleur contrastante représente le volume de trafic à cette géolocalisation. Les géolocalisations représentées sur la carte sont également répertoriées dans le volet droit.

Cliquez sur une géolocalisation surlignée sur la carte ou dans la liste pour afficher le volume total de trafic entrant ou sortant associé aux points de terminaison internes connectés.

Voici quelques moyens d'interagir avec les détails de géolocalisation et la visualisation de la carte :

- Cliquez sur un point de terminaison interne dans la liste pour afficher les propriétés de l'équipement et accéder aux liens vers les informations associées telles que les détections, les enregistrements ou les paquets.
- Cliquez sur la loupe à côté d'un point de terminaison dans la liste pour afficher les enregistrements associés au point de terminaison.
- Au bas de la liste, basculez entre les vues qui indiquent les octets sortants et les octets entrants sur votre réseau.

- Cliquez sur les commandes situées dans le coin inférieur droit de la carte pour zoomer ou dézoomer ou remettre la carte dans sa position initiale, ou vous pouvez faire pivoter la molette de votre souris.
- Cliquez et faites glisser votre souris sur la carte ou appuyez sur les touches fléchées de votre clavier pour repositionner la vue cartographique.
- Ajustez l'intervalle de temps pour visualiser le trafic à des heures précises, par exemple les activités inattendues le soir ou le week-end.

Sélecteur de site et rapport exécutif

Vous pouvez spécifier les sites à partir desquels vous souhaitez consulter les données sur cette page. Les utilisateurs ayant accès au module NDR peuvent générer un rapport exécutif pour partager les résultats.

Sélecteur de site

Cliquez sur le sélecteur de site en haut de la page pour afficher les données d'un ou de plusieurs sites de votre environnement. Consultez le trafic combiné sur vos réseaux ou concentrez-vous sur un seul site pour retrouver rapidement les données de vos équipements. Le sélecteur de site indique quand tous les sites ou certains d'entre eux sont hors ligne. Étant donné que les données ne sont pas disponibles sur les sites hors ligne, les graphiques et les pages d'équipement associés aux sites hors ligne peuvent ne pas afficher de données ou n'afficher que des données limitées. Le sélecteur de site n'est disponible qu'à partir d'un console.

(Module NDR uniquement) Rapport exécutif

Cliquez **Générer un rapport exécutif** pour créer un fichier PDF. Le rapport exécutif fournit un résumé des principales détections et des principaux risques pour votre réseau au cours de la semaine dernière. Le rapport exécutif ne contient que des informations sur les sites sélectionnés.