Cartes d'activités

Publié: 2024-03-20

Une carte d'activité est une représentation visuelle dynamique de l'activité du protocole L4-L7 entre les appareils de votre réseau. Vous pouvez voir une disposition 2D ou 3D des connexions des appareils en temps réel pour en savoir plus sur le flux de trafic et les relations entre les appareils.

Les cartes d'activité peuvent vous aider dans les cas d'utilisation suivants :

Effectuez une migration vers un centre de données ou vers le cloud

Dans le cadre de votre stratégie de migration, vous devez déterminer quels services peuvent être désactivés et à quel moment. Une carte dproximative des activités vous aide à identifier les appareils encore connectés afin d'éviter toute interruption de service imprévue pendant le processus de migration. Pour plus d'informations, consultez Planifiez et surveillez votre migration à l'aide de cartes d'activité procédure pas à pas.

Identifiez la cause première d'une application lente

Les applications dépendent souvent de plusieurs niveaux de services au sein d'un réseau. Une carte d'activité peut vous aider à identifier la chaîne de distribution du trafic vers votre serveur dproximatif d'applications lent. Cliquez sur un équipement pour étudier les indicateurs associés, ce qui peut permettre de mieux comprendre la cause première du ralentissement.

Suivez les appareils suspects ou les connexions inattendues

Lors d'un événement de sécurité, une carte d'activités peut vous aider à identifier les appareils concernés en suivant le trafic est-ouest en temps réel associé à un équipement suspect. Dans le cadre d'une stratégie de surveillance quotidienne de la sécurité, vous pouvez créer une carte dactivités pour vous assurer que les appareils n'établissent pas de connexions inattendues avec d'autres appareils.

Voici quelques considérations importantes concernant les cartes d'activités :

- Tu peux créer des cartes d'activités pour les appareils en mode Advanced, Standard, L2 Parent Analysis et Flow Analysis. Vous ne pouvez pas créer de carte dactivités pour les appareils en mode découverte. Pour plus d'informations, voir Priorités d'analyse.
- Si vous créez une carte dactivités pour un équipement ou un groupe déquipements qui n'a aucune activité de protocole pendant l'intervalle de temps sélectionné, la carte apparaît sans aucune donnée. Modifiez l'intervalle de temps ou votre sélection d'origine et réessayez.
- Vous pouvez créer une carte dproximative d'activités à partir d'un console pour visualiser les connexions des équipements entre tous vos capteurs.
- Tu peux enregistrer et partager une carte dactivités, accordant l'accès à la consultation ou à la modification à d'autres utilisateurs ou groupes du système. Vous pouvez également charger une carte d'activités sauvegardée pour modifier les propriétés de la carte.

Pour plus d'informations sur les cartes d'activités, consultez le FAQ sur les cartes d'activités.

Parcourez les cartes d'activités

Après création d'une carte d'activités, vous pouvez commencer à étudier les données. Les sections suivantes fournissent des détails sur la manière d'interagir avec une carte dactivités et de trouver des informations sur les données que vous consultez.

Disposition

Les appareils sont représentés par des cercles et les connexions par des lignes.

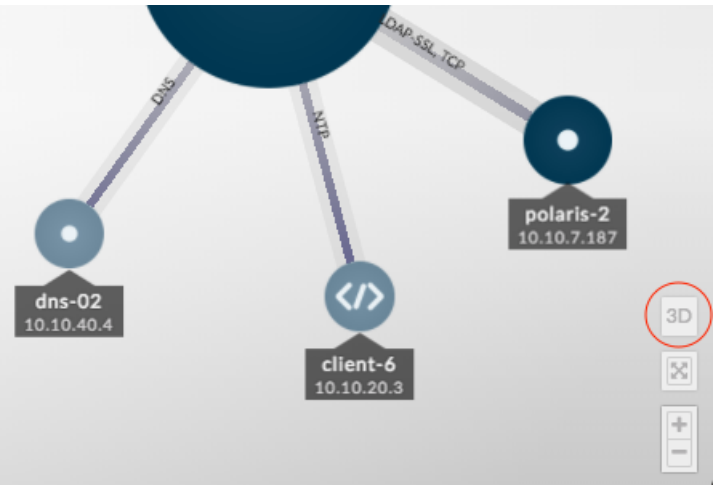
Le placement des appareils est optimisé pour afficher les informations. La mise en page peut changer à mesure que les données relatives à l'activité de l'équipement sont mises à jour en temps réel. Par exemple,

la mise en page est mise à jour à mesure que de nouvelles connexions sont observées ou que les appareils deviennent inactifs.

Note: Lorsque l'intervalle de temps indiqué dans le coin supérieur gauche de la page est défini sur Les 30 dernières minutes, les 6 dernières heures ou le dernier jour, les données de la carte dactivités sont continuellement mises à jour toutes les minutes avec des données en temps réel. Définissez un intervalle de temps personnalisé avec une heure de début et de fin spécifique pour arrêter les mises à jour de mise en page en temps réel.

Disposition 2D ou 3D

Par défaut, les cartes d'activités sont affichées dans une mise en page 2D, mais vous pouvez cliquer sur 3D pour transformer l'affichage en un modèle 3D rotatif. Par exemple, vous souhaiterez peut-être présenter des cartes 3D sur grand écran dans un réseau ou un centre des opérations de sécurité.

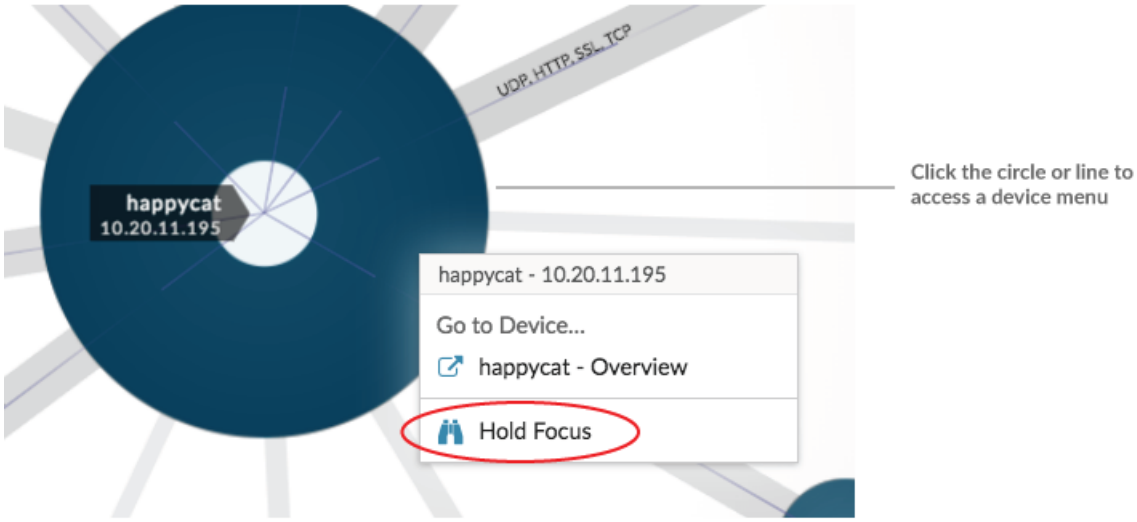


Repositionnement, rotation et zoom

Effectuez un zoom avant ou arrière sur une carte à l'aide des commandes situées dans le coin inférieur droit de la page ou zoomez avec la molette de votre souris. Cliquez et faites glisser votre souris pour repositionner une carte 2D ou faire pivoter une carte 3D.

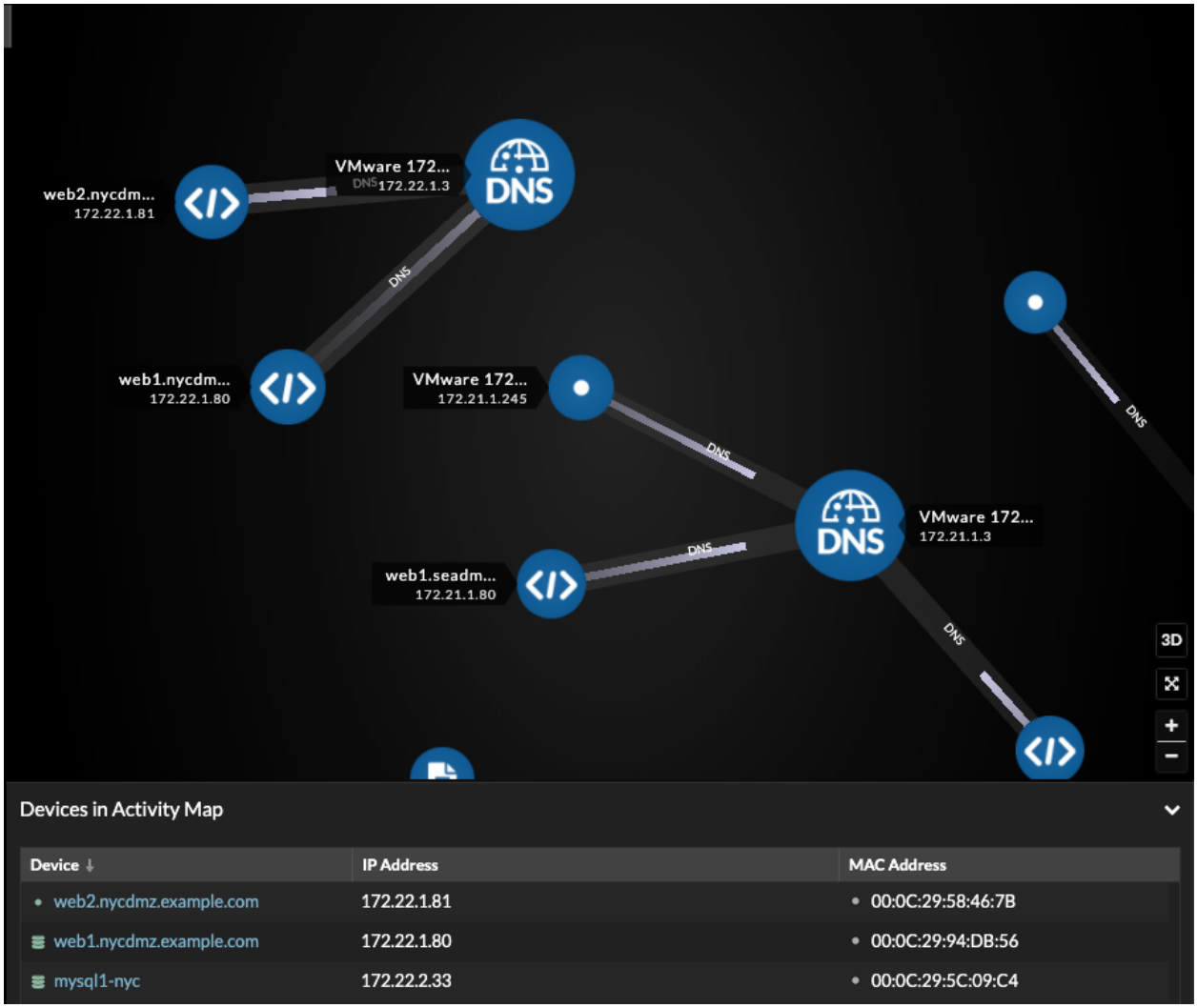
Restez concentré

Cliquez sur n'importe quel équipement et sélectionnez **Maintenez le focus**. Vous pouvez ensuite repositionner ou faire pivoter, en fonction de votre mise en page, et zoomer ou dézoomer sur la carte tout en vous concentrant sur l'équipement sélectionné et ses homologues immédiats.



Afficher la liste des équipements

Cliquez **Appareils dans la carte d'activité** au bas de la page pour afficher la liste de tous les appareils, leurs noms, adresses IP et adresses MAC. Cliquez sur le nom d'un équipement pour accéder à la page de l'équipement.

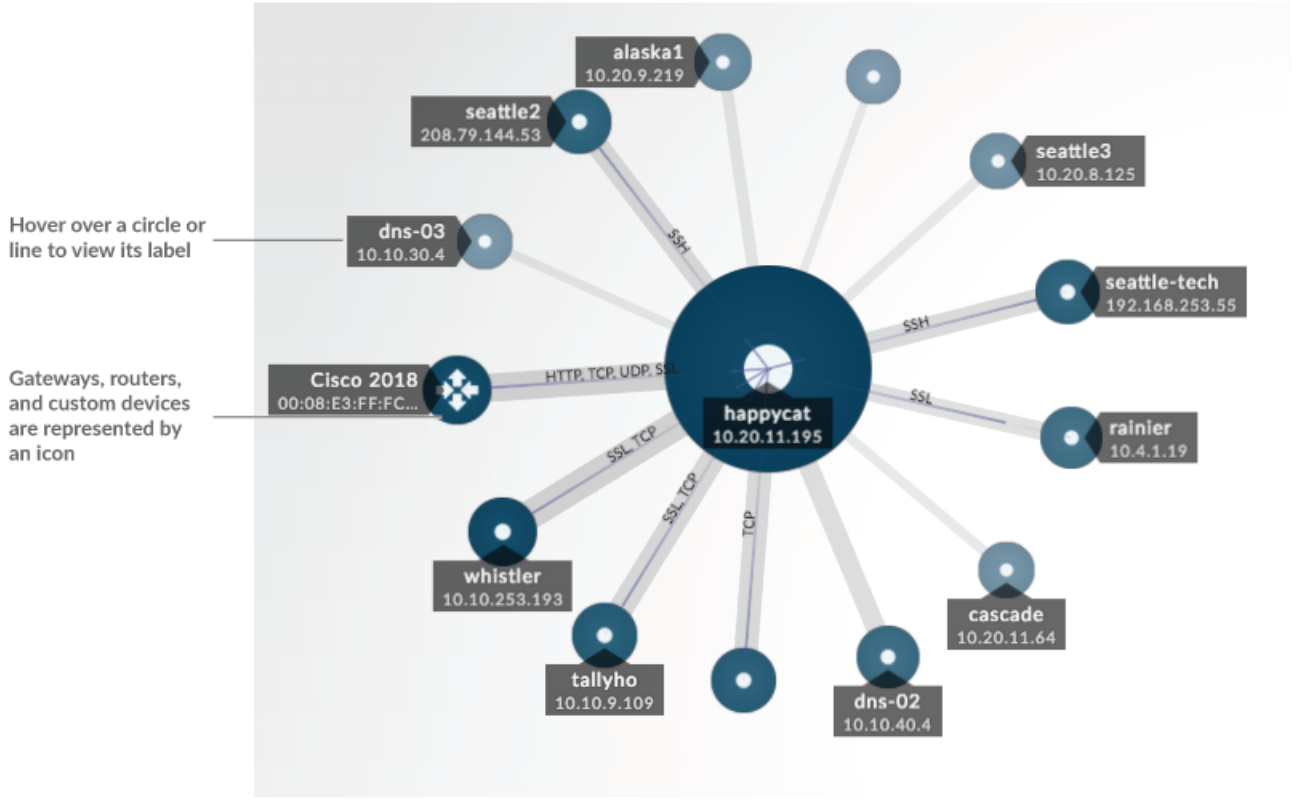


Étiquettes et icônes

Les étiquettes circulaires contiennent des informations telles que le nom d'hôte, l'adresse IP ou l'adresse MAC de l'équipement.

Les étiquettes de ligne contiennent les noms des protocoles associés à la connexion de l'équipement et à la direction du trafic circulant entre les appareils, qui sont affichés sous forme d'impulsions animées. Spécifique rôles de l'équipement sont représentés par une icône.

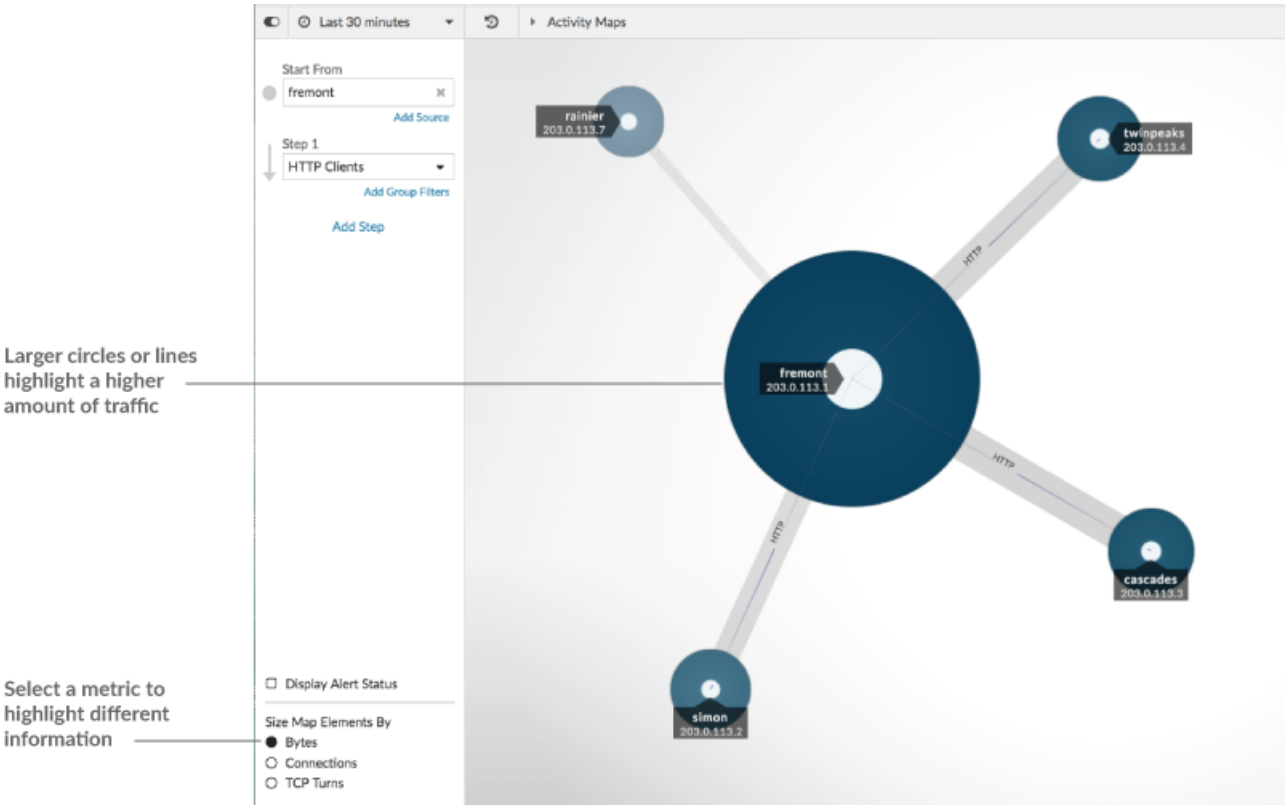
Pour optimiser l'affichage des informations, toutes les étiquettes ne sont pas affichées. Passez le pointeur de la souris sur un cercle ou une ligne pour afficher son étiquette, comme illustré dans la figure suivante.



Note: Les rôles des appareils sont automatiquement attribués à un équipement en fonction du type de trafic observé par le système ExtraHop pour cet équipement. Pour plus d'informations, voir Modifier le rôle d'un équipement.

Taille du cercle et de la ligne

La taille des objets sur la carte correspond à une valeur métrique, qui permet de mettre en évidence les zones d'activité accrue, telles que le nombre d'octets, ou le volume de trafic, associés à la connexion d'un équipement.



Au bas du volet de gauche, vous pouvez sélectionner une autre métrique pour les éléments cartographiques :

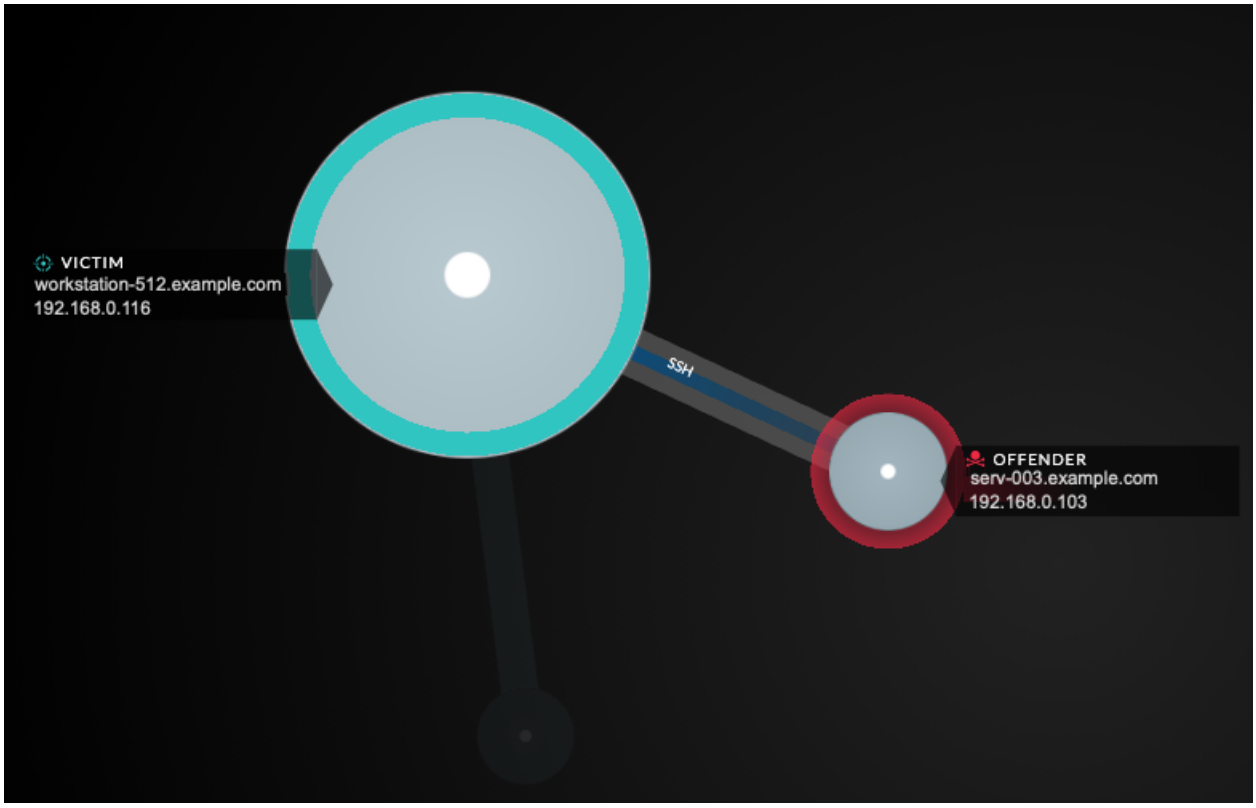
- **Octets:** Consultez tous les appareils qui transmettent ou reçoivent des données pendant l'intervalle de temps.
- **Connexions:** Afficher uniquement les appareils qui ont établi une nouvelle connexion au moins une fois pendant l' intervalle de temps.
- **TCP tourne:** Consultez uniquement les appareils qui ont basculé entre la transmission et la réception de données au moins une fois pendant l'intervalle de temps.

Couleur

Le bleu et le gris sont les couleurs par défaut des cercles et des lignes. Ces couleurs par défaut sont optimisées pour afficher les informations sur une carte. Toutefois, vous pouvez appliquer différentes couleurs à votre carte pour mettre en évidence le niveau de gravité d'une alerte ou indiquer à quel moment la connexion d'un équipement a été établie.

Détections

Détections associés à un équipement sur la carte apparaissent autour du cercle sous forme d'impulsions animées, appelées marqueurs de détection. La couleur du pouls est rouge si l' équipement est le délinquant et bleu sarcelle si l'équipement est victime de la détection. Le statut du participant apparaît également sur l'étiquette de l'équipement.



Note: Les détections par apprentissage automatique nécessitent un connexion aux services cloud ExtraHop.

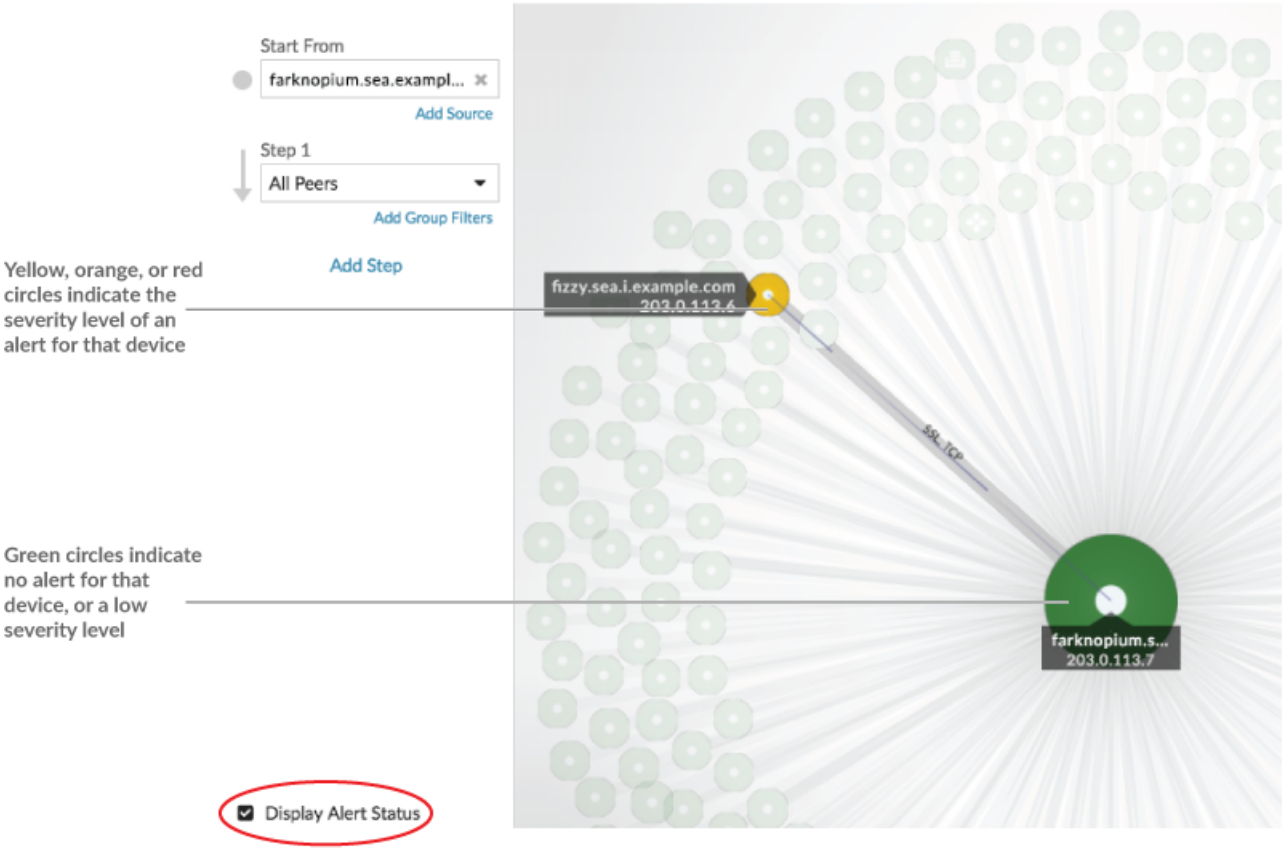
Cliquez sur un cercle avec un marqueur de détection pour afficher et naviguer vers les détections associées ou Page de présentation de l'appareil.

Si les marqueurs de détection n'apparaissent pas sur vos cartes d'activité comme prévu, ils peuvent être désactivés. Tu peux activer ou désactiver les marqueurs de détection à partir du **Utilisateur** menu.

État de l'alerte (accès au module NPM requis)

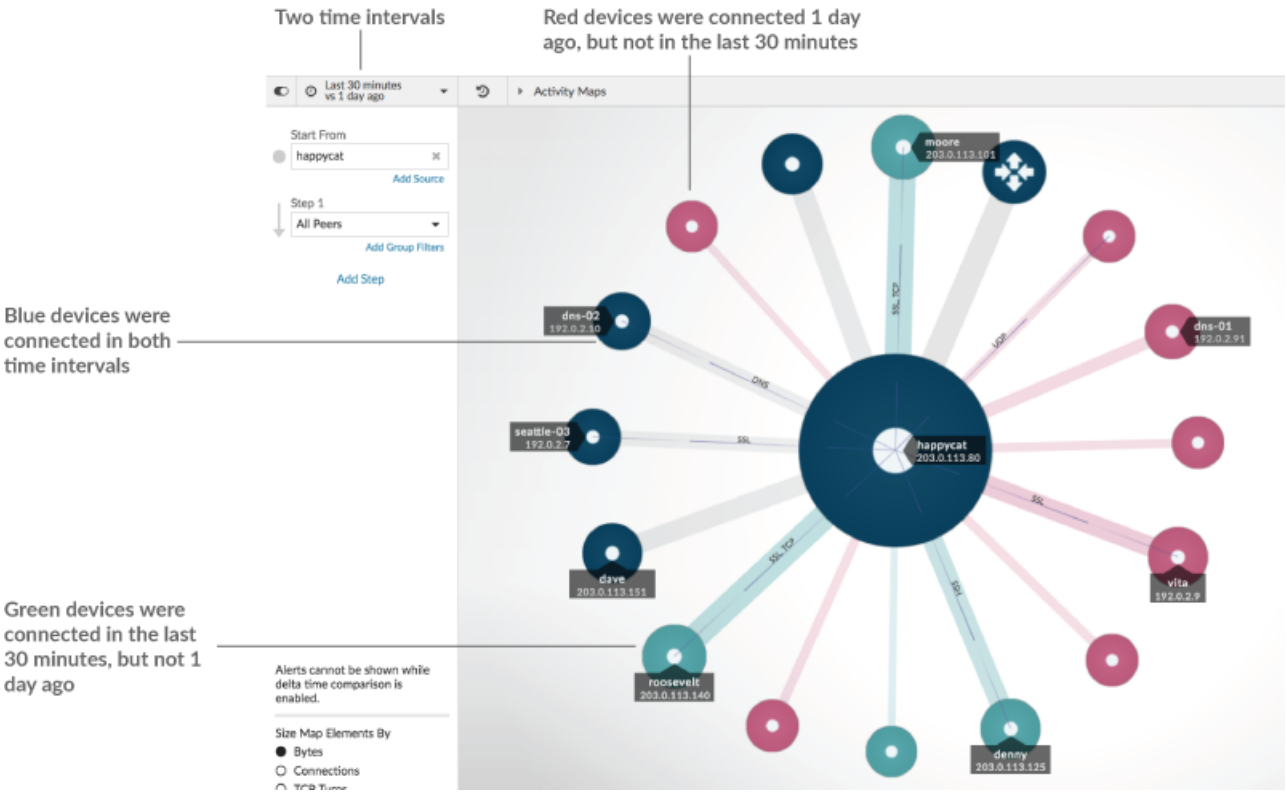
Pour voir le niveau de gravité d'une alerte pour un équipement sur votre carte, sélectionnez **Afficher le statut de l' alerte** dans le coin inférieur gauche ou sur la page, comme le montre la figure suivante. La couleur du cercle correspond alors à l'état le plus sévère pour toutes les alertes attribuées à un équipement pendant l'intervalle de temps. Si aucune alerte n'est attribuée à un équipement ou si le niveau d'alerte est informatif, la couleur du cercle par défaut est le vert.

Pour examiner l'alerte, cliquez sur le cercle, puis sélectionnez le nom de l'équipement dans Accédez à l'appareil... section. Sur la page de protocole de l'appareil, faites défiler la page jusqu'à voir la page Alertes.



Comparaison des intervalles de temps

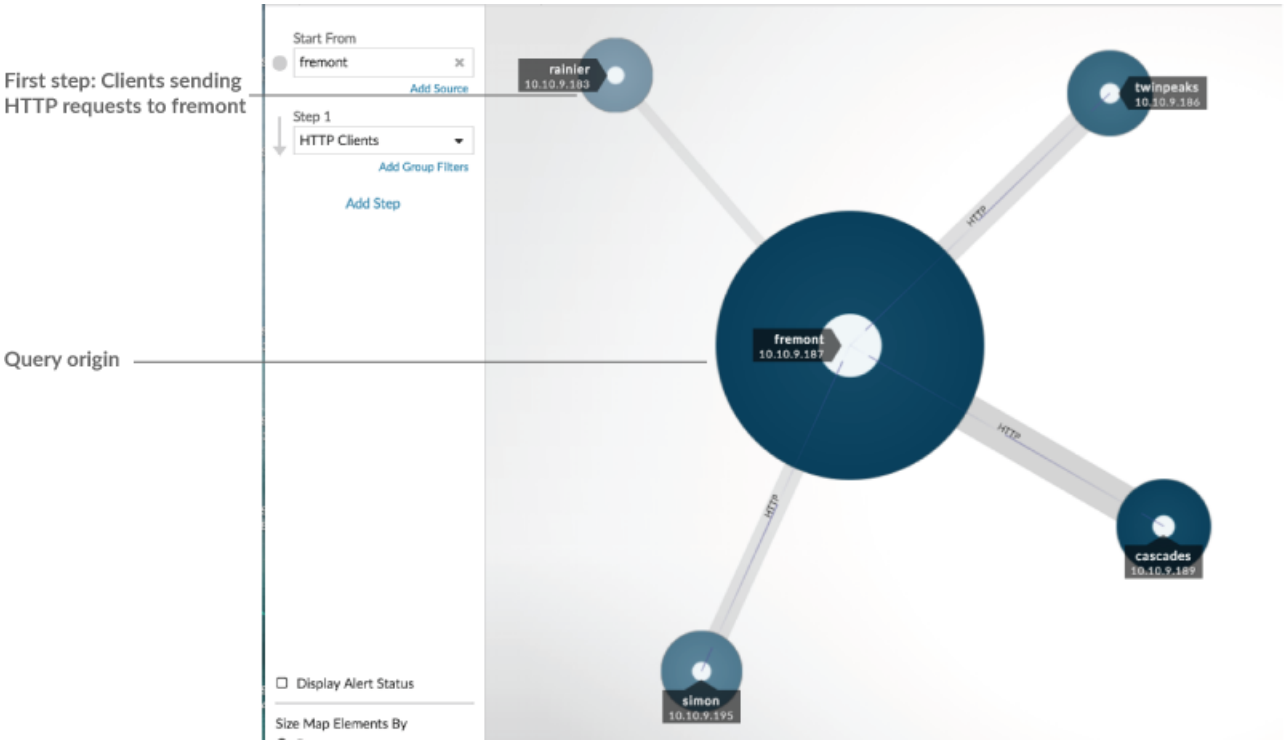
Lorsque vous comparez deux intervalles de temps pour trouver des deltas métriques, les différentes couleurs de la carte vous aident à déterminer à quel moment les connexions des équipements ont été établies ou à quel moment l'activité du protocole d'un équipement a changé. Par exemple, après avoir créé une comparaison entre **Hier** et le **Les 30 dernières minutes**, les nouvelles connexions à un équipement ou les activités qui apparaissent uniquement au cours de l'intervalle de temps le plus récent apparaissent en vert. Les connexions ou activités précédentes à l'équipement qui n'apparaissent que dans l'intervalle de temps précédent sont rouges. Les connexions des appareils qui n'ont pas changé entre les intervalles de temps sont bleues. Dans la figure suivante, les nouvelles connexions établies au cours des trente dernières minutes sont représentées par des cercles et des lignes verts.



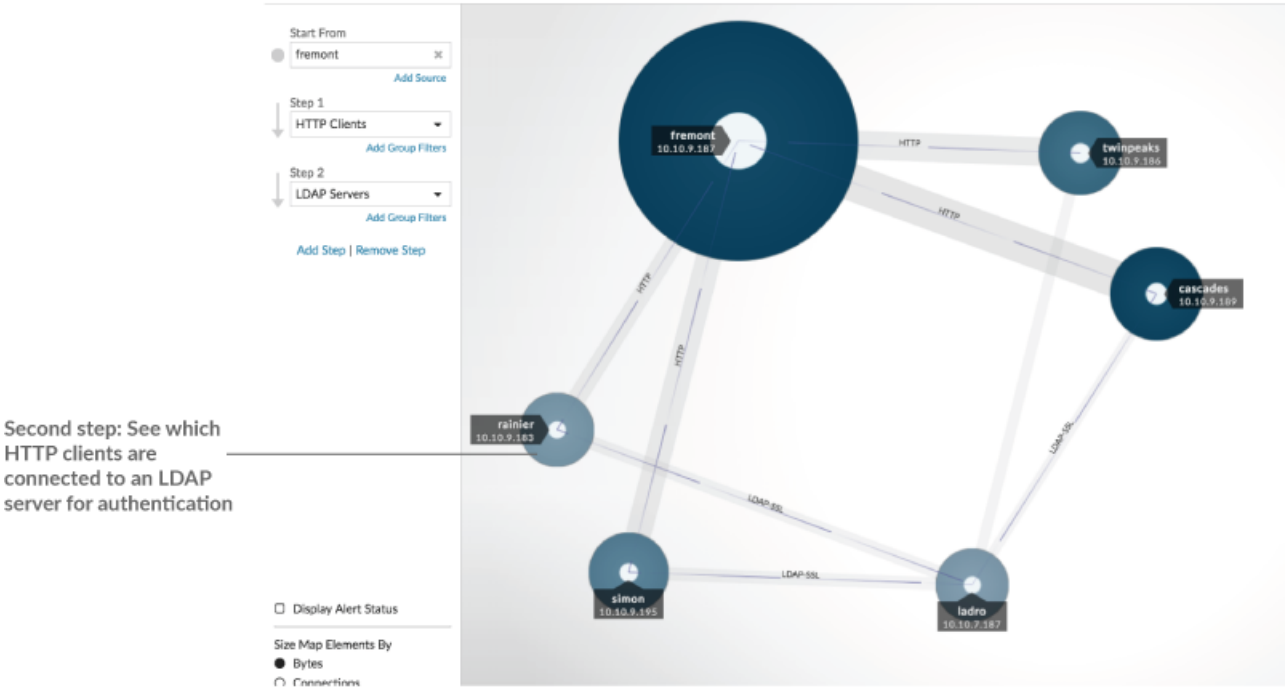
Note: Si tous les périphériques sont d'une seule couleur, par exemple le vert, cela signifie que la requête n'a pas produit de résultats dans l'intervalle de temps précédent. Par exemple, l'équipement d'origine n'avait aucune activité de protocole au cours de l'intervalle de temps précédent.

Ajouter des étapes et des filtres à une carte

Une étape est un niveau de connexions entre les appareils. Les appareils de chaque étape ont une relation avec les appareils de l'étape précédente. Ces relations sont définies par leur activité protocolaire.



Ajoutez une nouvelle étape à une carte dactivités pour ajouter une autre couche d'informations à votre carte. Cliquez sur la liste déroulante correspondant à une étape spécifique, puis sélectionnez une activité de protocole.



Vous pouvez également filtrer les appareils en une étape en fonction de leur appartenance au groupe. Par exemple, si vous sélectionnez des serveurs HTTP mais que vous souhaitez uniquement voir vos serveurs de

test sur la carte, vous pouvez filtrer les serveurs HTTP en fonction d'un groupe déquipements, tel que Mes serveurs de test.

Pour plus d'informations sur la façon d'ajouter des étapes et des filtres à une carte, voir Création d'une carte dactivitiés.

Gérez les cartes d'activités

Les options suivantes pour gérer votre carte dactivités sont disponibles dans le menu de commandes situé dans le coin supérieur droit :

- Enregistrez et partagez une carte dactivités
- Charger et gérer une carte dactivités enregistrée
- Exporter la carte dactivités sous forme de fichier PDF, PNG ou SVG

Meilleures pratiques pour étudier les données des cartes dactivités

Si vous trouvez sur votre carte un équipement qui mérite d'être étudié, plusieurs options s'offrent à vous pour recueillir plus d'informations sur cet équipement.

Trouvez les appareils récemment connectés

Cliquez sur l'intervalle de temps dans le coin supérieur gauche de la page, puis sur **Comparez**. Vous pouvez voir comment les connexions des équipements ont changé entre deux intervalles de temps différents.

Pour plus d'informations, voir Comparaison des intervalles de temps.

Accédez aux pages de protocole pour trouver l'activité métrique associée

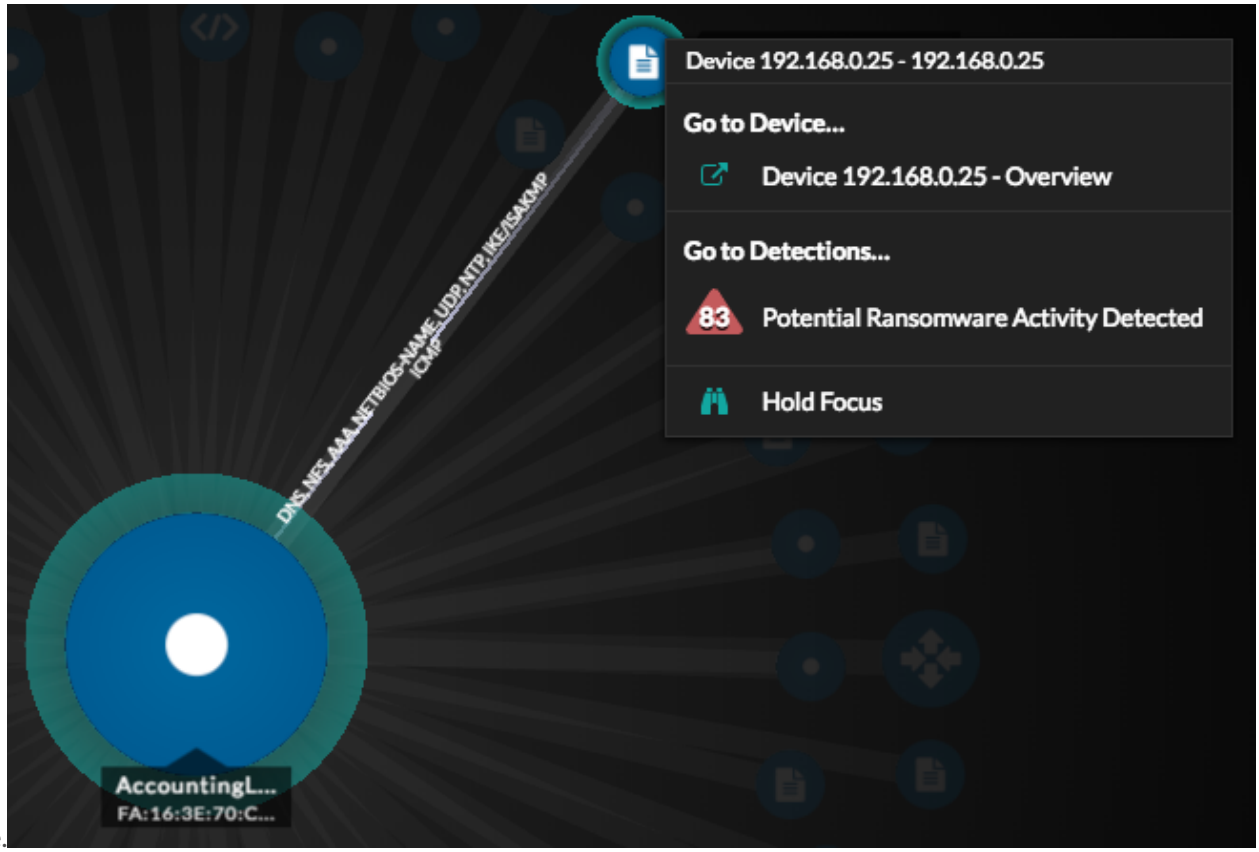
Cliquez sur un cercle ou une ligne pour accéder à un menu déroulant, comme illustré dans la figure suivante.

Sélectionnez le nom de l'équipement dans le menu pour afficher la page de présentation de l'appareil. Dans le volet de gauche, cliquez sur le nom d'un protocole pour afficher la page de protocole, qui contient un résumé des mesures de protocole importantes observées et associées à l'équipement. Sur une page de protocole, vous pouvez trouver des indicateurs connexes tels que les erreurs, les demandes, les réponses et le temps de traitement du serveur. Vous pouvez également accéder à une métrique depuis une page de protocole pour afficher les détails de la métrique, tels que l'adresse IP du serveur, l'adresse IP du client, les codes d'état, les méthodes et les URI.

Accédez aux détections identifiées sur l'équipement

Les appareils d'une carte dactivitiés associés à des détections sont affichés sous forme d'impulsions animées autour de l'étiquette circulaire. Cliquez sur un cercle avec ce

marqueur de détection pour accéder à un menu déroulant, comme illustré dans la figure suivante.



Sélectionnez un nom de détection dans le menu pour accéder à la page détaillée de cette détection. La page détaillée contient des informations sur le type de détection qui s'est produit et ce que cela signifie, ainsi que sur le moment où la détection s'est produite et la durée du problème. Pour plus d' informations, voir Page détaillée de la détection.

Rechercher des enregistrements de transactions associés à une connexion (nécessite un espace de stockage des enregistrements configuré)

Cliquez sur un cercle ou une ligne pour accéder au menu déroulant. Cliquez **Enregistrements**. Une page de requête d'enregistrements s'ouvre et affiche tous les enregistrements de chaque équipement connecté, y compris tous les types d'enregistrements associés aux protocoles de connexion de l'équipement.