Cisco Umbrella

EN BREF

Présentation de Cisco Umbrella.

Auparavant, les postes de travail, les applications professionnelles et l'infrastructure critique se trouvaient tous derrière le pare-feu. Aujourd'hui, de plus en plus de choses se passent hors du réseau. Il y a plus d'utilisateurs en déplacement. Plus d'ordinateurs portables de l'entreprise accédant à Internet depuis d'autres réseaux. Plus d'applications cloud permettant aux utilisateurs de travailler hors du réseau de l'entreprise. Et plus de sites distants se connectant directement à Internet.

D'ici 2021, Gartner prédit qu'en moyenne 25 % du trafic des informations d'une entreprise s'effectuera en dehors du périmètre de son réseau. Lorsqu'un utilisateur est hors du réseau, il est plus vulnérable et l'entreprise manque de visibilité et de moyens de protection. Si vous assurez uniquement la sécurité de votre périmètre réseau, vous n'êtes pas entièrement protégé. Ces vulnérabilités ouvrent la porte aux malwares, ransomwares et autres attaques.

La première ligne de défense

En tant que passerelle Internet sécurisée, Cisco Umbrella constitue la première ligne de défense contre les menaces qui circulent sur Internet, où que se trouvent les utilisateurs. Umbrella offre une visibilité complète sur l'activité Internet de tous les sites, appareils et utilisateurs, et bloque les menaces avant même qu'elles atteignent votre réseau ou vos terminaux. Umbrella est une plate-forme cloud ouverte qui s'intègre facilement dans votre infrastructure de sécurité et fournit des informations de Threat Intelligence en temps réel sur les menaces actuelles et émergentes.

Umbrella analyse les modèles d'activité sur Internet et apprend à identifier automatiquement l'infrastructure utilisée par les hackers pour les attaques pour bloquer de manière proactive les requêtes vers les destinations malveillantes avant qu'une connexion soit établie, sans augmenter la latence pour les utilisateurs.

Avec Umbrella, vous pouvez arrêter le phishing et les infections par logiciels malveillants plus tôt, identifier plus rapidement les appareils déjà infectés et empêcher l'exfiltration de données.

Une protection intégrée avec l'accès Internet

Le système DNS est un composant essentiel d'Internet qui permet d'établir une correspondance entre les noms de domaine et les adresses IP. Lorsque vous cliquez sur un lien ou que vous saisissez une URL, une requête DNS se charge de connecter l'appareil à Internet. Umbrella utilise le système DNS comme l'un des principaux mécanismes pour diriger le trafic vers notre plate-forme cloud et pour ensuite assurer la sécurité.

Lorsqu'une requête DNS est reçue, Umbrella utilise ses flux d'informations afin de déterminer si la requête est sûre, malveillante ou encore risquée, c'est-à-dire si le domaine contient à la fois du contenu malveillant et du contenu légitime. Les requêtes sûres ou malveillantes sont respectivement acheminées comme d'habitude ou bloquées. Les requêtes risquées sont envoyées vers notre proxy dans le cloud pour une inspection approfondie. Le proxy Umbrella utilise le système de réputation web Cisco Talos et d'autres flux d'informations tiers afin de déterminer si une URL est malveillante. Il inspecte également les fichiers que les utilisateurs ont tenté de télécharger depuis ces sites à risque à l'aide de moteurs antivirus et de Cisco AMP (Advanced Malware Protection). Selon les résultats de cette inspection, la connexion est autorisée ou bloquée.

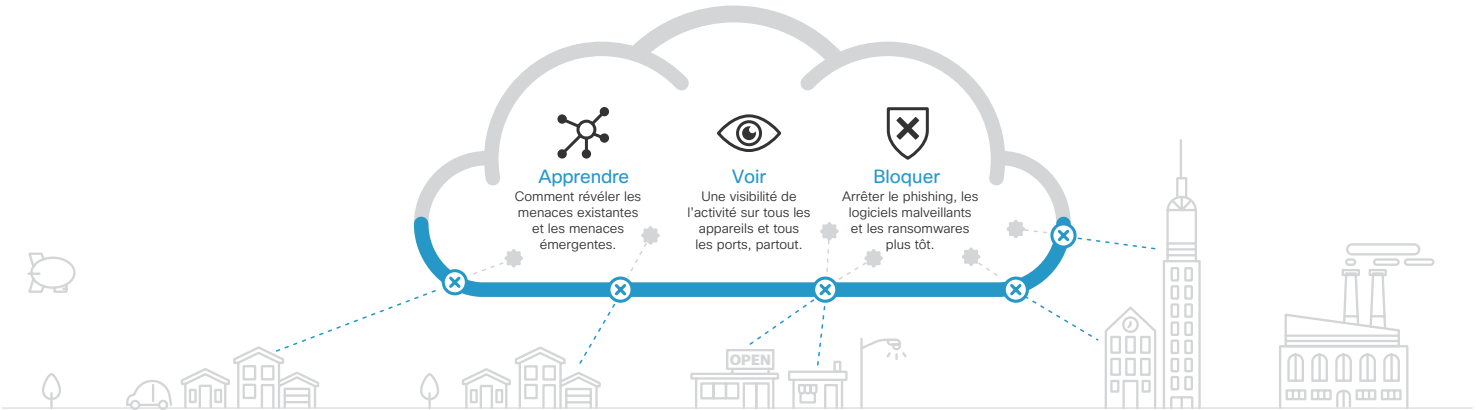
Les bénéfices

Réduisez les coûts de remise en état et les dommages dus aux failles : parce que Cisco Umbrella agit comme la première ligne de défense, les équipes en charge de la sécurité ont moins d'infections par malwares à éliminer et les menaces sont stoppées avant qu'elles ne causent des dégâts.

Réduisez le temps de détection et de contention des menaces : Cisco Umbrella bloque les instructions de type commande-contrôle quel que soit le port ou le protocole utilisé, et fournit des rapports en temps réel sur ce type d'activité.

Augmentez votre visibilité sur l'activité Internet de l'ensemble de vos sites et utilisateurs : Cisco Umbrella offre la visibilité dont vous avez besoin pour répondre aux incidents et vous assure de voir absolument toute l'activité.

Identifiez les applications cloud utilisées dans l'entreprise : Cisco Umbrella offre une visibilité sur les services cloud autorisés et non autorisés utilisés dans toute l'entreprise, afin de détecter les nouveaux services, de voir qui les utilise et d'identifier les risques potentiels.



Bloquer les menaces avant leur propagation grâce à la Threat Intelligence

Le réseau global d'Umbrella, qui est le réseau sur lequel repose notre service DNS récursif, résout chaque jour des milliards de requêtes Internet émanant de millions d'utilisateurs dans le monde. Nous analysons cette énorme quantité de données pour détecter des modèles récurrents et identifier l'infrastructure utilisée par les hackers.

Nous intégrons en temps réel toutes ces données sur l'activité Internet émanant de notre réseau mondial dans notre gigantesque base de données graphique. Nous exécutons ensuite en continu des modèles statistiques et d'apprentissage automatique sur cette base de données. Ces données sont également constamment analysés par les experts en sécurité Umbrella et complétés par les informations de Cisco Talos. Cette combinaison d'intelligence humaine et d'apprentissage automatique nous permet d'identifier les sites malveillants, qu'il s'agisse de domaines, d'adresses IP ou d'URL, sur l'ensemble d'Internet.

Une intégration facile avec d'autres produits

Umbrella s'intègre dans votre infrastructure de sécurité, y compris les appliances de sécurité, les plates-formes d'informations et les points de contrôle de courtage des services de sécurité pour l'accès au cloud (CASB). Umbrella peut envoyer les données des journaux relatifs à l'activité Internet à vos systèmes SIEM ou de gestion des événements. De plus, à l'aide de notre API, vous pouvez programmer l'envoi des domaines malveillants à Umbrella pour qu'ils soient bloqués. Cela vous permet d'optimiser vos investissements et d'étendre facilement la protection à tous les niveaux.

Un déploiement à l'échelle de l'entreprise en quelques minutes

Umbrella constitue le moyen le plus rapide et le plus simple de protéger tous vos utilisateurs en quelques minutes. Parce qu'Umbrella est basé dans le cloud, il n'y a aucun matériel à installer ni logiciel à mettre à jour manuellement. Vous pouvez provisionner tous les équipements sur le réseau en quelques minutes, y compris les appareils BYOD et IoT, et utiliser votre solution Cisco actuelle (AnyConnect, routeurs à services intégrés ISR 1000 et 4000, contrôleurs LAN sans fil 5520 et 8540) pour provisionner rapidement des milliers de sorties réseau et d'ordinateurs portables itinérants. En outre, grâce à l'application Cisco Security Connector, vous pouvez utiliser l'extension Umbrella pour protéger les terminaux iOS 11 supervisés.

Étapes suivantes

Contactez un conseiller commercial Cisco ou un partenaire pour savoir comment Cisco Umbrella peut aider à protéger votre entreprise mobile et connectée au cloud contre les menaces avancées. Rendez-vous sur signup.umbrella.com pour essayer gratuitement Umbrella pendant 14 jours. Si votre entreprise compte plus de 1 000 utilisateurs, vous pouvez bénéficier du rapport de sécurité Umbrella, qui fournit une analyse détaillée après l'essai.

Principales fonctionnalités

- Une visibilité et une protection à tous les niveaux
- Des fonctions de Threat Intelligence pour détecter les attaques plus rapidement
- Un déploiement et une gestion simples
- Une plate-forme ouverte pour l'intégration
- Une infrastructure cloud fiable et rapide

Chiffres clés

- 125 milliards de requêtes web par jour
- 90 millions d'utilisateurs
- 27 data centers dans le monde
- Plus de 7 millions de destinations malveillantes bloquées simultanément au niveau de la couche DNS

Cisco Umbrella