Protégez vos terminaux avec les solutions Cisco AMP pour Endpoints et Cisco Umbrella

Les défis liés à la protection des terminaux

Près de 70 % des attaques passent par les terminaux : ordinateurs portables, postes de travail, serveurs et terminaux mobiles[1]. Pourquoi les terminaux sont-ils toujours le principal point d'entrée des attaques ?

Une protection insuffisante

Quand les utilisateurs et les terminaux se situent hors du réseau, les outils de prévention comme les antivirus sont souvent les seuls systèmes de protection disponibles. Mais cette protection n'est pas suffisante face aux menaces avancées d'aujourd'hui.

65 %

des entreprises déclarent avoir subi des attaques non détectées par leurs outils de sécurité préventive[2]

Une visibilité insuffisante

Souvent, les entreprises ne voient pas les attaques de malwares et ne connaissent pas leur portée. Elles ne disposent que d'une visibilité limitée sur les activités des utilisateurs et des terminaux, et ne possèdent pas assez d'informations contextuelles pour détecter les malwares (leur provenance, leurs déplacements et leurs activités). Elles ne peuvent pas détecter ce qu'elles ne voient pas.

55 %

des entreprises ne sont pas en mesure de déterminer la cause d'une faille[3]

100 JOURS

de délai moyen de détection[4]

Des erreurs humaines

Un cybercriminel envoie un e-mail de phishing accompagné d'une pièce jointe ou d'un lien malveillant. Malgré les formations et les innombrables mises en garde, certains utilisateurs ouvrent quand même ce type de fichiers ou cliquent sur certains liens alors qu'ils ne devraient pas.

48 %

des cybercriminels contournent les défenses des terminaux suite à une erreur humaine[5]

Les besoins des entreprises

Les entreprises ont besoin d'une visibilité plus poussée sur les activités des fichiers et des utilisateurs sur le terminal. Elles doivent aussi déterminer où le terminal essaie de se connecter à Internet. De plus, elles ont besoin du niveau de contrôle nécessaire pour mettre un terme aux éventuels comportements malveillants.

Une protection efficace pour les terminaux

Les solutions de sécurité Cisco AMP pour Endpoints et Cisco Umbrella travaillent de concert pour offrir la visibilité, les informations contextuelles et le contrôle nécessaires pour éviter, détecter et éliminer les attaques qui ciblent les terminaux, avant qu'elles causent des dégâts.

PRÉVENIR

AMP pour Endpoints

- Bloque les malwares connus lors de l'inspection initiale
- Utilise une sandbox (basée sur Threat Grid) pour analyser les fichiers inconnus

Umbrella

- Bloque les requêtes Internet malveillantes (domaine, URL et IP), quel que soit le mécanisme d'envoi (e-mail, attaque web « drive-by », etc.)

DÉTECTER

AMP pour Endpoints

- Analyse en permanence toutes les activités des fichiers sur les terminaux pour détecter rapidement les comportements malveillants et alerter rétrospectivement les équipes de sécurité

Umbrella

- Bloque les instructions de type commande-contrôle vers les serveurs du hacker pour stopper l'exfiltration des données et les fonctions de chiffrement des ransomwares

RÉAGIR

AMP pour Endpoints

- Affiche l'historique et le contexte complets de chaque compromission
- Peut stopper les attaques grâce aux fonctions de contrôle des incidents et de mise en quarantaine des fichiers

Umbrella Investigate

- Fournit des données récentes sur les menaces et des informations contextuelles historiques sur les domaines, les adresses IP et les hashs de fichiers pour effectuer des recherches plus rapidement

AMP pour Endpoints

AMP pour Endpoints est une solution de protection des terminaux gérée dans le cloud qui empêche les cyberattaques et détecte, isole et élimine rapidement les fichiers malveillants sur les terminaux.

Présentation vidéo | Démonstration vidéo

AMP pour Endpoints utilise :

- L'analyse continue des comportements des fichiers
- La détection rétrospective
- Un moteur d'inspection antivirus
- Des analyses statiques et dynamiques des fichiers (sandboxing via Threat Grid)
- L'apprentissage automatique
- La surveillance des vulnérabilités
- La protection des exploits et de la mémoire

Principales fonctionnalités :

- **Un blocage proactif** : AMP pour Endpoints utilise la réputation des fichiers, les indicateurs comportementaux, la technologie de sandboxing intégrée et la Threat Intelligence à l'échelle mondiale fournie par le groupe de recherche Talos pour analyser les fichiers inconnus et bloquer automatiquement les malwares qui tentent de s'infiltrer dans un terminal.

- **L'analyse en continu et la sécurité rétrospective** : les malwares avancés peuvent contourner les premières lignes de défense et s'infiltrer dans un terminal. AMP pour Endpoints vous protège. Il surveille et enregistre en permanence toute l'activité des fichiers sur les terminaux afin de détecter rapidement les comportements malveillants. Cisco AMP vous présente ensuite un historique complet du comportement du programme malveillant : sa provenance, ses déplacements et ses activités. Vous pouvez ainsi détecter et éliminer les menaces de manière rétrospective avant qu'elles causent des dégâts.

« Avec Cisco Advanced Malware Protection et Cisco Umbrella, nous avons éliminé totalement les incidents liés aux ransomwares au cours des 8 derniers mois. »

Freek Bosscha, Architecte informatique, Université NHL

« Nous faisons entièrement confiance aux solutions Cisco AMP et Cisco Umbrella pour sécuriser nos terminaux. Depuis que nous les avons implémentées il y a trois ans, nous n'avons déploré aucune infection par malware. »

Un ingénieur d'une entreprise de taille moyenne du secteur des services financiers

Umbrella

Umbrella est une plate-forme de sécurité cloud qui représente la première ligne de défense contre les menaces issues d'Internet, que les utilisateurs se connectent depuis le réseau de l'entreprise ou en dehors. Umbrella offre une visibilité totale sur l'activité en ligne de l'ensemble de vos sites et terminaux. La solution bloque de façon proactive les requêtes malveillantes avant qu'une connexion soit établie.

Présentation vidéo | Démonstration vidéo

Umbrella aide les entreprises à :

- bloquer les attaques plus tôt
- identifier plus rapidement les appareils infectés
- éviter l'exfiltration de données

Principales fonctionnalités :

- **La Threat Intelligence** : Umbrella repose sur un réseau mondial qui traite plus de 100 milliards de requêtes DNS (Domain Name System) tous les jours et transforme ces données en informations exploitables. En combinant l'apprentissage automatique et l'intelligence humaine, les données sont analysées afin de repérer les tendances, de détecter les anomalies et de créer des modèles statistiques pour identifier automatiquement les attaques en cours et l'infrastructure mise en place par le hacker pour les prochaines menaces.

- **Un proxy intelligent** : le proxy intelligent Umbrella fournit aux clients une protection plus granulaire. Si Umbrella reçoit une requête d'un domaine qui n'a pas encore été identifié comme étant bon ou mauvais, celle-ci est routée vers le proxy pour être analysée plus en détail. Umbrella s'appuie sur Cisco Talos, les systèmes de réputation web de Cisco et les flux d'informations de nos partenaires pour bloquer des millions d'URL malveillantes. La solution inspecte les fichiers en utilisant un moteur antivirus et Cisco AMP.

Plus d'infos :

Cisco AMP pour Endpoints

Cisco Umbrella

1. Effective Incident Detection and Investigation Saves Money (Détecter et étudier efficacement les incidents permet de réaliser des économies), IDC, 2016
2. A Year of Mega Breaches (L'année des grandes failles), Ponemon Institute, 2015
3. A Year of Mega Breaches (L'année des grandes failles), Ponemon Institute, 2015
4. Rapport annuel Cisco 2016 sur la sécurité, Cisco, 2016
5. Exploits at the Endpoint : SANS 2016 Threat Landscape Survey (Exploits visant les terminaux : enquête SANS 2016 sur les menaces d'aujourd'hui)