01. Cisco Advance Malware Protection

La visibilité et le contrôle dont vous avez besoin pour contrer les attaques avancées

Profitez d'une Threat Intelligence à l'échelle mondiale, de fonctions de sandboxing avancées et d'un blocage des malwares en temps réel pour prévenir les failles grâce à Cisco AMP (Advanced Malware Protection). Mais comme la prévention ne fait pas tout, Cisco AMP analyse également en permanence l'activité des fichiers sur tout votre réseau afin de détecter, de contenir et de supprimer rapidement les malwares avancés.

o Une Threat Intelligence à l'échelle mondiale

Les experts Cisco Talos analysent des millions d'échantillons de malwares et des téraoctets de données chaque jour, puis transmettent ces informations à Cisco AMP. Cisco AMP compare les fichiers, leur comportement et les données de télémétrie à cette base de connaissances contextuelle pour assurer une défense proactive contre les menaces connues et les nouveaux types d'attaques.

o Un sandboxing avancé

Les fonctionnalités de sandboxing avancées permettent de comparer automatiquement, et de manière dynamique et statique, les fichiers avec plus de 700 indicateurs comportementaux. Ces analyses permettent de détecter les menaces furtives et d'aider votre équipe chargée de la sécurité à identifier, à hiérarchiser et à bloquer les attaques les plus sophistiquées.

o La détection et le blocage ponctuels des malwares

Bloquez en temps réel les malwares qui tentent d'infiltrer votre réseau. Grâce à des moteurs de détection antivirus, à la mise en correspondance biunivoque des signatures, à l'apprentissage automatique et à la recherche d'empreintes partielles, Cisco AMP analyse les fichiers au niveau de leur point d'entrée afin de détecter les malwares connus et inconnus. Le résultat ? Des délais de détection plus courts et une protection automatisée.

o Des fonctions d'analyse continue et de sécurité rétrospective

Lorsqu'un fichier, quel qu'il soit, entre sur votre réseau, Cisco AMP continue d'observer, d'analyser et d'enregistrer son activité. Si un comportement suspect est détecté ultérieurement, Cisco AMP envoie une alerte rétrospective à votre équipe chargée de la sécurité pour lui indiquer la provenance du malware, ses déplacements et ses activités. En quelques clics, vous pouvez le contenir et l'éradiquer.

Besoin d'infos ou d'un devis ?

CONTACT

Protégez vos terminaux

Grâce à la solution Cisco de protection des terminaux, vous pouvez bloquer les malwares au point d'entrée, avoir une visibilité sur l'activité au niveau des fichiers et des exécutables, et éliminer les malwares de vos PC, Mac, systèmes Linux et terminaux mobiles.

Cisco AMP pour terminaux >

Protégez votre réseau

Bénéficiez d'une visibilité avancée sur l'activité des menaces, au coeur ou à la périphérie du réseau et bloquez les malwares les plus avancés.

AMP for Networks >
Pare-Feu >
Plate-Forme de gestion unifiée des risques Meraki MX >
Le routeur d'une succursale (ISR) >

Protégez votre messagerie et le trafic web

Ajoutez des fonctionnalités Cisco AMP à vos appliances de sécurisation du web et de la messagerie ou lors de vos déploiements de solutions cloud de sécurisation du web et de la messagerie.

La messagerie >
Le web >
Les passerelles Internet sécurisées (Cisco Umbrella) >

Pourquoi travailler avec DistriWan ?

- **Offre de services >** Un catalogue de prestations sur-mesure et adaptées à vos besoins
- **Expertise >** Une équipe avant-vente spécialisée par architecture
- **Accompagnement >** Une équipe commerciale à votre écoute pour répondre à toutes vos demandes de projets
- **Réactivité et flexibilité >** Une forte adaptabilité pour répondre à toutes vos exigences