CROWDSTRIKE

CONÇUE POUR ARRÊTER LES INTRUSIONS

Protection des endpoints basée sur le cloud

CROWDSTRIKE FALCON : LA NORME EN MATIÈRE DE PROTECTION DES ENDPOINTS

SÉCURITÉ DES ENDPOINTS BASÉE SUR UNE APPROCHE SIMPLE ET SOLIDE

L'agent Crowdstrike Falcon, par ailleurs très léger, fonctionne en harmonie avec sa plateforme cloud puissante. Ensemble, ceux-ci assurent protection et visibilité en temps réel — **même quand l'agent n'est pas connecté à Internet.** CrowdStrike Falcon assure une prévention solide contre les menaces, couplant des techniques relevant de l'Intelligence Artificielle ou encore du «Machine Learning» avec une stratégie de détection et de réponse sophistiquée, ainsi qu'un système intégré de cyber renseignements – le tout dans une console de gestion à l'utilisation intuitive.

CROWDSTRIKE FALCON POURQUOI ?

UNE PROTECTION COMPLÈTE
Prévention et détection immédiates et efficaces contre tout type d'attaques – avec ou sans logiciels malveillants – que vous soyez connecté ou offline.

UNE VISIBILITÉ SANS ÉQUIVALENT
Comme un système de surveillance vidéo pour vos endpoints – rien ne passe inaperçu. Explorez et examinez l'historique de l'activité d'un endpoint en quelques secondes.

UNE UTILISATION INCROYABLEMENT SIMPLE
Une plateforme cloud facile à déployer, configurer et entretenir – le tout avec un seul agent léger.

CROWDSTRIKE FALCON : RENDRE POSSIBLE L'IMPOSSIBLE

C'était une idée reçue qu'il était impossible de fournir une protection des endpoints complète en utilisant un agent léger n'ayant aucun impact sur la performance des utilisateurs. Nous avons prouvé le contraire. Grâce à la visibilité, la protection et l'intervention en temps réel de CrowdStrike Falcon, **vous pouvez maintenant :**

➤ Empêcher les attaques de commodité et les attaques sophistiquées — que vos assaillants utilisent des logiciels malveillants ou non, ou que vos terminaux soient en ligne ou non.

➤ Gagner en visibilité de vos endpoints, visibilité en temps réel - et avoir une vue d'ensemble sur les applications et processus en cours d'exécution dans votre environnement, afin de garantir les réponses nécessaires, sans omission.

➤ Rechercher activement les éventuelles menaces sophistiquées — plus rapidement et plus efficacement que jamais.

➤ Protéger les endpoints sur la totalité des plateformes les plus utilisées comme Windows, OS X et Linux, les serveurs de centres de données, les machines virtuelles et les plateformes cloud comme AWS, Azure et Google.

➤ Retirer votre antivirus existant et déployer une solution de nouvelle génération, testée indépendamment et certifiée comme étant un antivirus de remplacement efficace.

CrowdStrike – **Vue d'Ensemble**

FALCON DISCOVER

Hygiène Informatique

Falcon Discover identifie les applications et les systèmes non autorisés où qu'ils se trouvent dans votre environnement, en temps réel, permettant une intervention plus rapide qui pourra améliorer votre niveau de sécurité.

FALCON PREVENT

Antivirus nouvelle génération (AVNG)

Falcon Prevent protège contre les attaques réalisées avec ou sans logiciels malveillants. Il a été testé et certifié par des organismes tiers, ce qui permet aux entreprises de l'utiliser en remplacement de leur ancien antivirus.

FALCON INSIGHT

Détection et intervention sur terminaux (DIT)

Falcon Insight offre une visibilité totale et permanente des endpoints avec une couverture élargie de détection, d'intervention et d'analyse qui vous assure que rien n'est oublié et que les failles potentielles sont colmatées.

FALCON OVERWATCH

Recherche Active et Gérée des Menaces (Managed Threat Hunting)

L'équipe Falcon OverWatch 24/7 travaille en arrière-plan 7 jours sur 7 et 24 heures sur 24 pour améliorer la sécurité de votre entreprise et repérer les activités malveillantes le plus vite possible, stoppant net vos adversaires.

FALCON INTELLIGENCE

Cyber Renseignements (Threat Intelligence)

Falcon Intelligence traque les activités hostiles à travers le monde entier, fournissant des rapports personnalisés et des analyses menant à des prises d'action pour améliorer votre stratégie de sécurité.

PROTECTION DES ENDPOINTS

BASÉE SUR LE CLOUD

HYGIÈNE INFORMATIQUE

Il vous faut être prêt à affronter tout type d'attaques — mais vous ne pouvez pas corriger ce qui vous est invisible. Les entreprises ont besoin d'une visibilité en temps réel à travers leur environnement afin d'identifier la totalité des endpoints, gérés ou non, et établir un inventaire des applications, ce qui leur permettra d'améliorer leur stratégie de sécurité.

BASÉE SUR LE

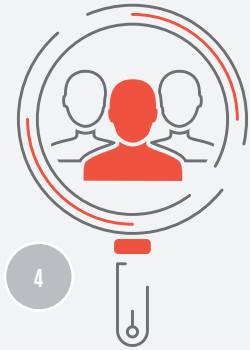
ANTIVIRUS DE NOUVELLE GÉNÉRATION (AVNG)

Afin de vous protéger contre les attaques provenant ou non de logiciels malveillants, il vous faut un antivirus de nouvelle génération complet et ayant fait ses preuves, qui combine plusieurs technologies de prévention comme le «Machine Learning», le blocage de failles de sécurité, et disposant d'un Indicateur d'Attaques Avancées (IAA) à analyse comportementale.

DÉTECTION ET INTERVENTION SUR TERMINAUX (DIT)

Une DIT permanente et complète, avec une capacité de recherche de 5 secondes, afin d'examiner et d'enquêter sur l'activité de vos endpoints passée et en cours, vous informera de ce qui se passe sur vos terminaux, vous assurant que rien n'est oublié et ne laissant aucun espace libre aux assaillants.

BASÉE SUR LE



RECHERCHE ACTIVE ET GÉRÉE DES MENACES (MANAGED THREAT HUNTING)

Déployer les technologies de défense les plus sophistiquées ne suffit plus. Pour vaincre des adversaires sophistiqués, il vous faudra une équipe dédiée travaillant 24 heures sur 24 et 7 jours sur 7 pour traquer proactivement les comportements suspects, tout en analysant les nouvelles tendances afin d'identifier les menaces émergentes.

CYBER RENSEIGNEMENTS (THREAT INTELLIGENCE)

Si vous ne connaissez pas la menace, il vous sera impossible de la protéger. Threat Intelligence vous permet de comprendre les motifs des assaillants, d'anticiper leurs techniques et d'implémenter des actions efficaces pour les empêcher de s'infiltrer dans votre organisation.

Services CrowdStrike

SERVICES D'INTERVENTION LORS D'INCIDENTS

Les services d'intervention pré et post incident (SI) sont disponibles 24 heures sur 24, 7 jours sur 7, pour vous aider avant, pendant ou après une intrusion. Ces équipes hautement qualifiées vous apportent les capacités nécessaires pour vous défendre et réagir contre les incidents de sécurité, traiter les failles de manière préventive et accélérer votre réactivité.

DES SERVICES PROACTIFS

Les équipes de service CrowdStrike travailleront avec vous afin d'anticiper les menaces, de préparer votre réseau pour contrer les intrusions et d'améliorer les compétences de vos équipes pour empêcher les dégâts consécutifs à des cyberattaques. Ces services proactifs prennent en charge les estimations de potentiel d'intrusions, effectuent des tests de penetration de nouvelle génération et proposent des exercices didactiques, en complément des programmes de développement SI et COS (centre des opérations de sécurité).

CROWDSTRIKE : TESTÉ ET APPROUVÉ

Avec CrowdStrike, vous aurez la certitude que votre organisation est enfin protégée contre les cyberattaques, connues ou pas, avec ou sans malware. Mais écoutez ceux qui en parlent le mieux : voici ce que disent les experts à propos de CrowdStrike Falcon:

«VISIONNAIRE»

— Gartner Magic Quadrant sur les plateformes de protection des endpoints – Janvier 2017

«EXCELLENTES PERFORMANCES»

— Forrester Wave : Sécurité des endpoints – Octobre 2016

«PRODUIT DE SÉCURITÉ APPROUVÉ POUR ENTREPRISE»

AV comparatives

— Comparatifs AV – Décembre 2016

SIÈGE SOCIAL

15440 Laguna Canyon Road, Suite 250 Irvine, California 92618, U.S.A. | +1 (888) 512-8906

info@crowdstrike.com | sales@crowdstrike.com | crowdstrike.com

Vous avez subi une faille de sécurité ? Contactez-nous au +1 (855) 276-9347 ou services@crowdstrike.com