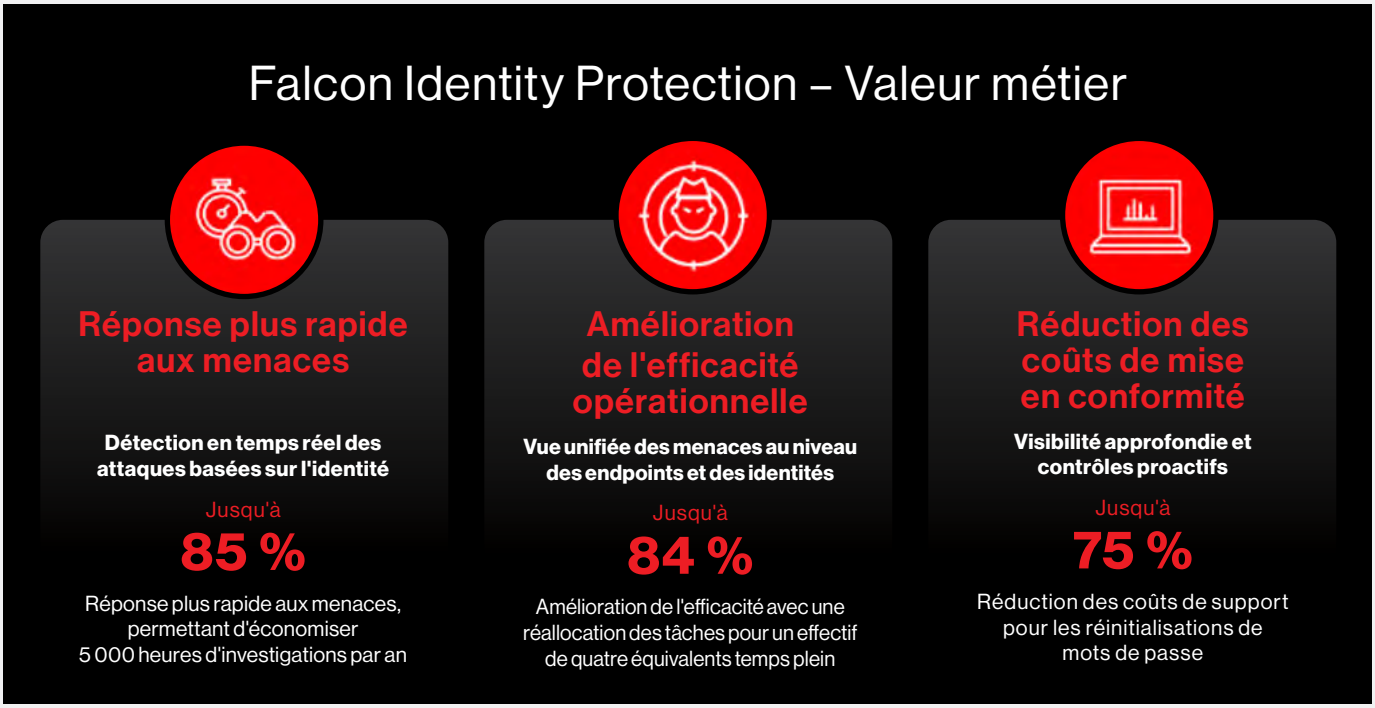
CROWDSTRIKE

Principales raisons d'ajouter Falcon Identity Threat Protection à votre cyberdéfense sans attendre

Les attaques basées sur l'identité sont la principale cybermenace à laquelle les entreprises font face à l'heure actuelle. En effet, plus de 80 % des cyberincidents reposent sur l'utilisation abusive d'identifiants valides pour accéder au réseau d'une entreprise.

CrowdStrike Falcon® Identity Threat Protection, composant de la plateforme CrowdStrike Falcon®, détecte et bloque en temps réel les compromissions liées à l'identité dans un paysage de l'identité hybride et complexe, au moyen d'un seul agent et d'une interface unifiée avec mise en corrélation des attaques au niveau des endpoints, des workloads, des identités et des données. Voici cinq avantages que vous pouvez attendre de l'intégration de la protection des identités à votre stratégie de cybersécurité*.



1. Réponse aux menaces jusqu'à 85 % plus rapide

Les solutions traditionnelles limitées aux endpoints passent à côté des menaces liées à l'identité, et l'approche actuelle consistant à mettre manuellement en corrélation les menaces au niveau des endpoints et des identités avec plusieurs outils autonomes (outils d'hygiène d'AD, logs d'événements Windows, PAM, UEBA, SIEM et plus encore) ralentit l'intervention de l'équipe SOC. Grâce à la plateforme unifiée CrowdStrike Falcon, les clients Falcon Identity Threat Protection peuvent visualiser tous les vecteurs d'attaque et mettre en corrélation les menaces au sein d'une console unique. Cela peut se traduire par une **réponse aux menaces jusqu'à 85 % plus rapide** et par une protection en temps réel, ce qui permet d'économiser des milliers d'heures d'investigations post-compromission chaque année.

2. Amélioration allant jusqu'à 84 % de l'efficacité opérationnelle

CrowdStrike Falcon est **une solution cloud native dotée d'un agent unique** qui peut être déployée n'importe où dans l'environnement client, simplifiant ainsi la collecte de données télémétriques (auprès des endpoints ou des identités). Un grand distributeur **a consolidé plus de cinq outils** (typiques de nombreuses entreprises) en un seul pour gérer les menaces liées à l'identité avec Falcon Identity Threat Protection. La consolidation du SOC avec une plateforme et un agent uniques élimine les outils et agents autonomes, ce qui permet de réduire les coûts opérationnels et associés aux outils. Par ailleurs, en évitant d'avoir à employer des outils d'ingestion de logs disparates, la détection en temps réel peut réduire les heures de maintenance et **accroître l'efficacité opérationnelle jusqu'à 84 %**, permettant de réallouer à d'autres tâches près de quatre équivalents temps plein.

3. Réduction allant jusqu'à 75 % des coûts de mise en conformité et de support

Une visibilité approfondie sur les mots de passe compromis, les comptes à privilèges excessifs et l'utilisation abusive de comptes de services permet aux clients de résoudre les problèmes d'hygiène d'Active Directory de façon précoce et de mettre en place des contrôles proactifs, réduisant ainsi les coûts de mise en conformité. Un CISO a notamment signalé une **baisse de 75 % des demandes de réinitialisation de mots de passe et des coûts associés,** une diminution de 8 % de la vulnérabilité au phishing et une réduction de 32 % des droits d'accès utilisateur superflus. Un important opérateur de télécommunications a affirmé avoir amélioré son niveau de conformité à la certification du modèle de maturité de la cybersécurité (CMMC) en utilisant Falcon Identity Threat Protection pour étendre l'authentification multifacteur (MFA) à l'ensemble de l'environnement, y compris les applications héritées.

4. Réduction allant jusqu'à 57 % du risque de vol d'identifiants menant à une compromission

Avec huit attaques sur 10 impliquant des identifiants volés ou compromis, la réduction du risque de vol d'identifiants a des conséquences directes sur l'amélioration du niveau de sécurité. La capacité de Falcon Identity Threat Protection à détecter les menaces liées à l'identité permet aux clients d'identifier les comptes à haut risque et les potentiels vecteurs d'attaque dans l'ensemble de leur environnement, réduisant ainsi la surface d'attaque. Récemment, le CISO d'une chaîne hôtelière a expliqué comment Falcon Identity Threat Protection a immédiatement identifié 250 000 vecteurs d'attaque potentiels dans l'environnement de l'entreprise et comment 93 % d'entre eux pouvaient être corrigés grâce à trois modifications spécifiques de la configuration. Les évaluations de la valeur métier de CrowdStrike ont mis en lumière une **réduction allant jusqu'à 57 % du risque de vol d'identifiants** menant à une compromission. Cela a également été démontré par la réussite des tests d'intrusion effectués par des clients pour lesquels ces mêmes tests s'étaient soldés par un échec avant le déploiement de Falcon Identity Threat Protection.

5. Amélioration de la cyberassurabilité et réduction des primes

Alors que les cyberadversaires continuent à exploiter les contrôles de sécurité faibles pour lancer des attaques, **les compagnies de cyberassurance mettent l'accent sur** la nécessité de renforcer les contrôles afin de réduire les cyberrisques. Les ransomwares étant l'un des principaux facteurs entrant en ligne de compte, les assureurs ont réaffirmé la nécessité pour les entreprises de renforcer la sécurité d'AD, d'appliquer le MFA à l'ensemble des applications (y compris héritées), de protéger les comptes à privilèges et de service, ainsi que de déployer une solution de détection et de réponse à incident (EDR) pour être éligibles à une cyberassurance. Les clients ayant déployé Falcon Identity Threat Protection affirment que la solution a eu un impact positif sur leur programme de cyberassurance et a permis de réduire les primes.

Témoignages des clients CrowdStrike

« Après avoir déployé Falcon Identity Threat Protection, nous avons effectué un autre test d'intrusion et avons immédiatement constaté les avantages de la visibilité accrue. »

Ryan Melle
SVP, CISO, Berkshire Bank
(**Lire l'étude de cas**)

« Depuis le déploiement de Falcon Identity Threat Protection, nous avons constaté une nette amélioration de notre visibilité sur les identifiants, les identités à privilèges, les différents vecteurs d'attaque et les moyens de les corriger. »

Steven Townsley
Head of Information Security, Mercedes-AMG Petronas F1 Team
(**Regarder la vidéo**)

« Dans les deux heures suivant le déploiement de Falcon Identity Threat Protection, nous avons identifié 10 comptes à privilèges avec des mots de passe compromis et avons immédiatement commencé à les réinitialiser. »

CISO d'un comté de la région de Washington, D.C.
(**Lire l'article de blog**)

« Nous avons constaté la valeur de Falcon Identity Threat Protection dès la première minute, lorsque la solution a identifié 250 000 vecteurs d'attaque potentiels, dont 93 % pouvaient être corrigés par seulement trois modifications de la configuration. »

CISO d'une chaîne hôtelière internationale

« Il est plus simple de se référer à une seule interface pour la majorité de votre SOC que d'examiner 13 consoles et pages différentes pour analyser et surveiller quelque chose. »

CISO d'une entreprise agroalimentaire

La protection des identités n'est pas une option mais une nécessité

Le Global Threat Report 2023 de CrowdStrike montre que les attaques basées sur l'identité sont en hausse, avec une augmentation de **112 % des publicités pour des fournisseurs frauduleux d'accès réseau** sur le Dark Web en 2022. Microsoft Active Directory demeure une cible de choix pour les cyberadversaires, car il est utilisé par plus de 90 % des entreprises[1]. Une récente analyse des métadonnées de millions de comptes (humains, de service et à privilèges) réalisée par CrowdStrike a révélé que **50 % des entreprises possèdent des comptes à privilèges avec un mot de passe compromis**.

Pour ne rien arranger, les compromissions liées à l'identité sont connues pour être difficiles à détecter. Sans les bons outils, leur identification requiert en moyenne **250 jours**[2]. Pendant ce temps, les cyberadversaires peuvent se déplacer latéralement dans votre environnement en échappant à toute détection et lancer des attaques dévastatrices. Le temps de propagation moyen d'une attaque ayant été **réduit à 84 minutes en 2022**, selon le Global Threat Report 2023 de CrowdStrike, les entreprises ne peuvent pas se permettre d'attendre qu'une compromission grave se produise. Le cyberadversaire pourrait en effet déjà se trouver dans votre environnement sans que vous en ayez connaissance.

Négliger les menaces axées sur l'identité peut avoir de graves conséquences, comme la compromission totale du domaine de votre infrastructure AD, des attaques de ransomware paralysantes et des interruptions d'activité dévastatrices. D'après IBM et le Ponemon Institute, le **coût total moyen d'une compromission de données au niveau mondial s'élève à 4,35 millions de dollars (9,44 millions de dollars aux États-Unis)**[3]. Avec **huit attaques sur 10** impliquant des identifiants volés ou compromis, le déploiement de la protection des identités aura un impact immédiat, ce qui pourrait vous permettre d'économiser des millions de dollars et d'éviter que votre marque et votre réputation souffrent d'un préjudice irréversible.

N'oubliez pas : les cyberadversaires ne vont pas attendre que vous soyez prêt à riposter pour lancer leurs attaques. Protégez-vous dès aujourd'hui contre les compromissions avec Falcon Identity Threat Protection.

Contactez votre chargé de compte CrowdStrike ou demandez votre analyse gratuite des risques liés à Active Directory.

[1]Frost & Sullivan, « Active Directory Holds the Keys to your Kingdom, but is it Secure? »

[2]IBM et Ponemon Institute, « Cost of a Data Breach Report 2022 »

[3]IBM et Ponemon Institute, « Cost of a Data Breach Report 2022 »

* Les résultats attendus et réels ne sont pas garantis et peuvent varier selon le client. Les avantages attendus n° 1, 2 et 4 sont basés sur des moyennes agrégées calculées à partir de plus de 100 évaluations de la valeur métier et analyses de la valeur métier obtenue réalisées auprès d'entreprises clientes de CrowdStrike par l'équipe CrowdStrike dédiée à la valeur métier entre 2018 et décembre 2022. Les évaluations de la valeur métier sont des analyses du ROI prévisionnel basées sur la valeur de CrowdStrike par rapport à la solution existante des clients. Les analyses de la valeur métier obtenue sont des analyses du ROI obtenu pour les clients ayant déployé CrowdStrike depuis plus de six mois, basées sur les retours des clients et les données télémétriques collectées. L'avantage attendu n° 3 est basé sur des données partagées par un client avec CrowdStrike.

À propos de CrowdStrike

CrowdStrike (Nasdaq : CRWD), leader mondial de la cybersécurité, redéfinit la sécurité avec sa plateforme cloud native la plus avancée au monde, conçue pour protéger les ressources critiques des entreprises, à savoir les endpoints, les workloads cloud, les identités et les données.

Optimisée par l'architecture de sécurité cloud de CrowdStrike et une intelligence artificielle de pointe, la plateforme CrowdStrike Falcon® s'appuie sur des indicateurs d'attaque en temps réel, le renseignement sur les cybermenaces, l'évolution des techniques des cybercriminels et des données télémétriques enrichies récoltées à l'échelle de l'entreprise pour assurer une détection ultraprécise, une protection et une correction automatisées, un Threat Hunting de pointe et une observation priorisée des vulnérabilités.

Spécialement conçue dans le cloud au moyen d'une architecture à agent léger unique, la plateforme Falcon offre un déploiement rapide et évolutif, une protection et des performances de haut niveau, une complexité réduite et une rentabilité immédiate.

CrowdStrike : **We stop breaches.**

Suivez-nous : **Blog | Twitter | LinkedIn | Facebook | Instagram**

Démarrer une évaluation gratuite

Pour en savoir plus, consultez le site **www.crowdstrike.fr**