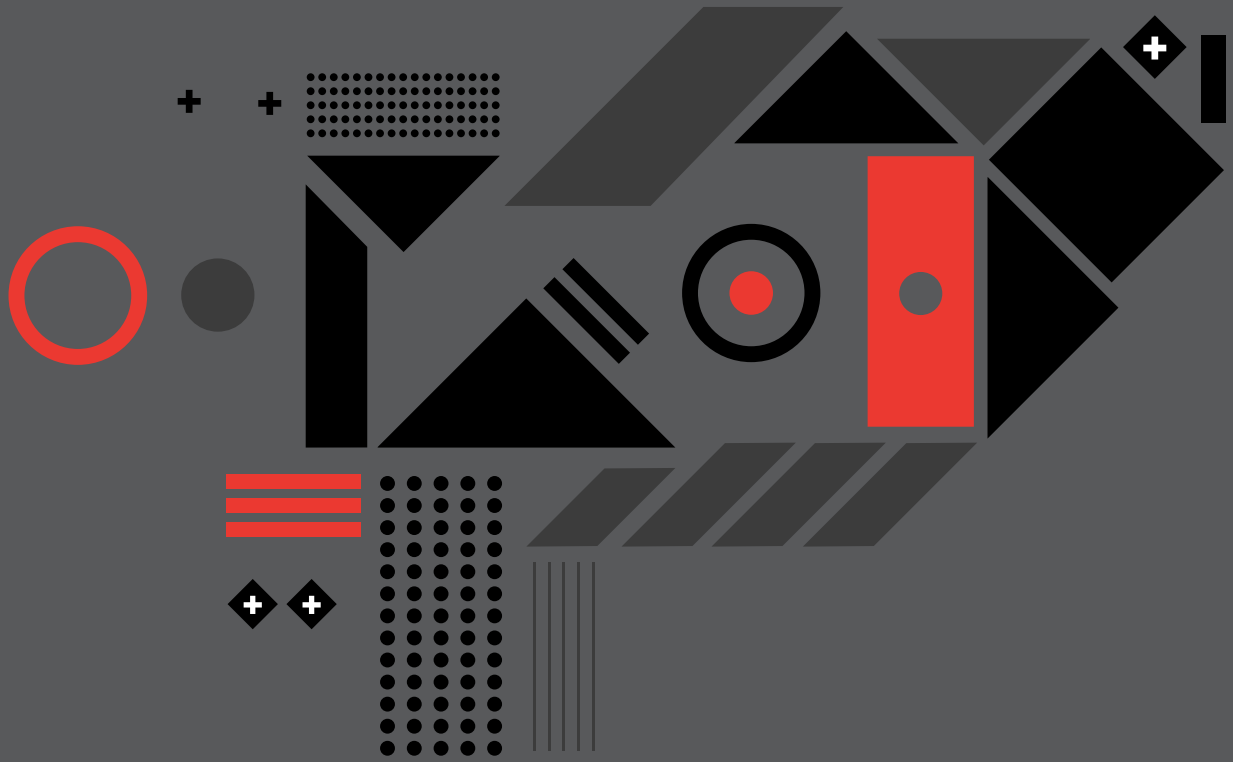
eBook

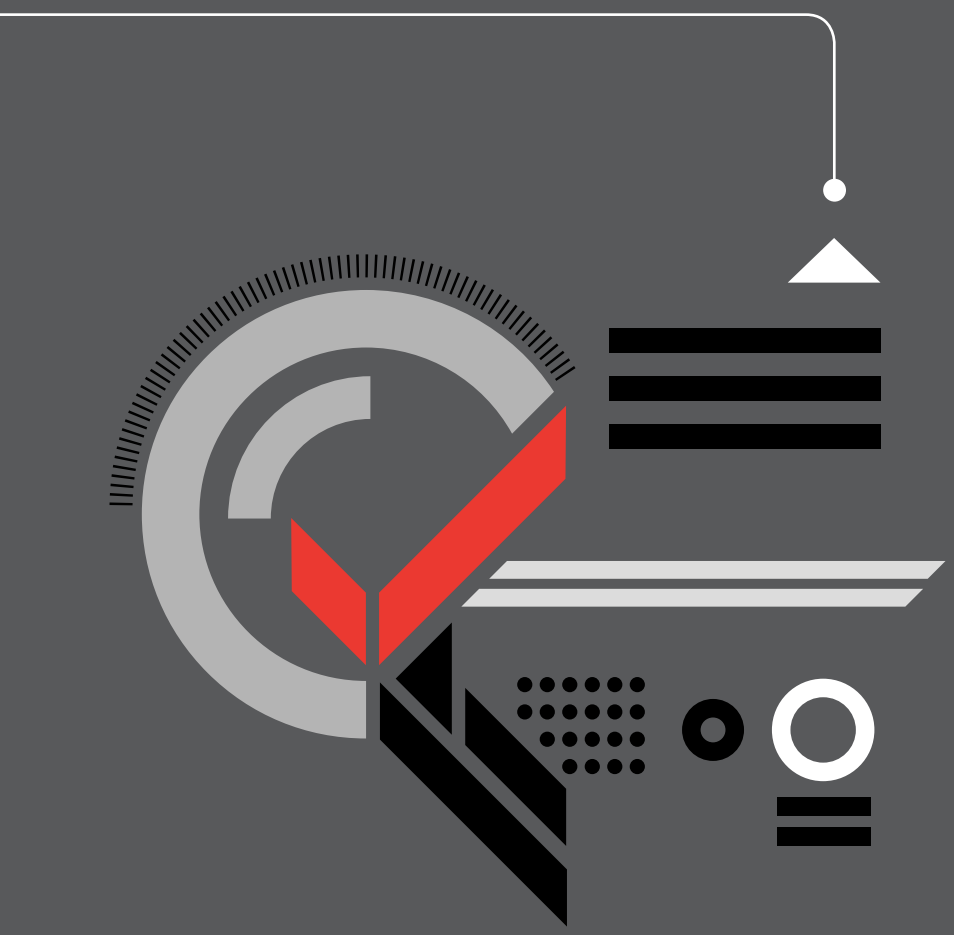


LE TÉLÉTRAVAIL EN TOUTE SÉCURITÉ

PROTÉGEZ VOS EFFECTIFS HYBRIDES, SÉCURISEZ VOS DONNÉES ET RENFORCEZ VOTRE RÉSILIENCE GRÂCE À LA PLATEFORME CROWDSTRIKE FALCON SUR AMAZON WORKSPACES

CROWDSTRIKE | aws

SOMMAIRE



LE TÉLÉTRAVAIL CRÉE DE NOUVELLES SURFACES D'ATTAQUE
page 3

PROTÉGER LES EFFECTIFS HYBRIDES AVEC CROWDSTRIKE FALCON ET AMAZON WORKSPACES
page 4

L'APPROCHE DE SÉCURITÉ DE CROWDSTRIKE VOUS PROTÈGE DES COMPROMISSIONS
page 5

SE DÉFENDRE CONTRE LES CYBERADVERSAIRES LES PLUS DÉTERMINÉS
page 6

BONNES PRATIQUES DE CYBERSÉCURITÉ POUR UN MONDE HYBRIDE
page 7

LA SÉCURITÉ COMMENCE PAR LA GESTION DES COÛTS
page 8

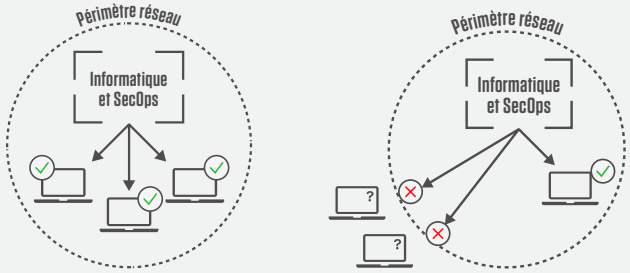
IL EST TEMPS DE SÉCURISER VOTRE ENVIRONNEMENT DE TÉLÉTRAVAIL
page 9

LE TÉLÉTRAVAIL CRÉE DE NOUVELLES SURFACES D'ATTAQUE

Le télétravail est appelé à perdurer. L'approche suscitant le plus d'intérêt est un modèle hybride, dans le cadre duquel certains collaborateurs sont exclusivement en télétravail, d'autres retournent au bureau et d'autres encore combinent les deux en se rendant au bureau certains jours de la semaine. À l'ère du télétravail, il est de plus en plus difficile de maintenir la sécurité et d'assurer la résilience à un moment où la plupart des entreprises peinent toujours à en faire plus avec moins.

L'adoption du cloud s'accélère et les effectifs hybrides augmentent

Avec la généralisation du télétravail, nombre d'entreprises ont été contraintes d'accélérer leur adoption des technologies cloud pour tenir la cadence, et notamment de faire évoluer leurs modèles de cybersécurité en abandonnant les solutions sur site au profit de plateformes cloud. Maintenant que le travail hybride est devenu la norme, ces entreprises constatent que les approches qu'elles ont adoptées dans la précipitation et sous la pression opérationnelle ne sont pas suffisantes pour protéger leurs effectifs hybrides et leurs données à long terme.



C'est la raison pour laquelle les entreprises novatrices adoptent une approche cloud native de la cybersécurité basée sur un cadre qui protège tous les utilisateurs, où qu'ils se trouvent.

Protection en temps réel

Prévenez les menaces, détectez les activités suspectes et répondez aux incidents en temps réel, quel que soit l'endroit où se trouvent vos utilisateurs et leurs terminaux.

Basé sur le cloud

Éliminez la complexité, simplifiez votre infrastructure de sécurité et exécutez vos déploiements en un temps record. Activez instantanément la gestion des vulnérabilités et l'hygiène IT avec Falcon Spotlight™ et Falcon Discover™.

Prise en charge de tous les terminaux

L'agent léger unique Falcon fonctionne dans tous les environnements, y compris les workloads cloud et les datacenters, pour protéger les utilisateurs sur leurs terminaux d'entreprise et personnels.

Six facteurs clés pouvant contribuer à assurer la cybersécurité des télétravailleurs

1. Vérifiez que vous disposez de règles de cybersécurité à jour qui couvrent le télétravail.
2. Prévoyez la connexion de terminaux BYOD au réseau de votre entreprise.
3. Ayez conscience que des données sensibles peuvent être consultées via des réseaux Wi-Fi non sécurisés.
4. La visibilité et l'hygiène de cybersécurité sont essentielles.
5. Une sensibilisation continue des utilisateurs finaux et une communication permanente sont extrêmement importantes, et il convient de s'assurer que les télétravailleurs peuvent contacter rapidement les services informatiques pour obtenir des conseils.
6. Les plans de gestion de crise et d'intervention sur incident doivent pouvoir être exécutés par des utilisateurs distants.

PROTÉGER LES EFFECTIFS HYBRIDES AVEC CROWDSTRIKE FALCON ET AMAZON WORKSPACES

Protéger les identités de vos collaborateurs et vos données

Avec Amazon WorkSpaces, les télétravailleurs disposent d'une solution DaaS (Desktop-as-a-Service) sécurisée leur permettant d'accéder à leurs bureaux où qu'ils se trouvent. L'installation de l'agent CrowdStrike Falcon dans un environnement Amazon WorkSpaces renforce davantage votre niveau de sécurité afin de réduire les risques de cybermenaces.

Amazon WorkSpaces propose une solution DaaS pour les effectifs hybrides

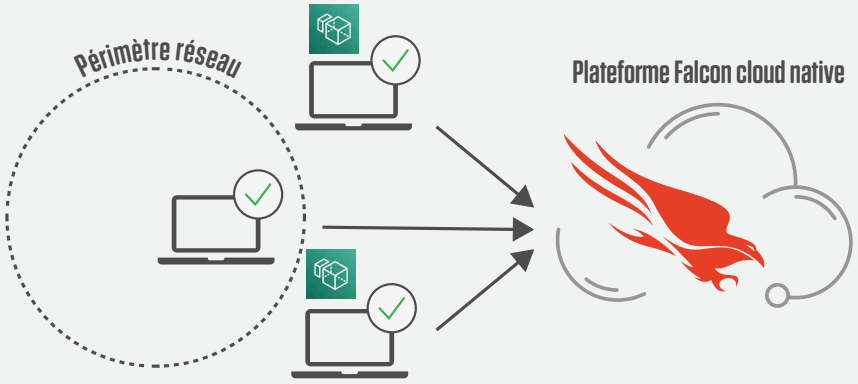
- Proposez à vos collaborateurs un bureau cloud accessible partout avec une simple connexion Internet.
- Exécutez-le directement sur un large éventail de terminaux, y compris des PC, des Mac et des iPad.
- Éliminez les tâches administratives telles que la mise en service, le déploiement et le maintien à jour des ordinateurs de bureau.

La plateforme CrowdStrike Falcon bloque les compromissions grâce à une sécurité fluide et à une protection cloud native des endpoints

- Installez-la rapidement à partir du cloud grâce à une solution SaaS assurant la protection de l'ensemble des terminaux, quel que soit l'endroit où ils se trouvent.
- Sécurisez tous les modèles de travail potentiels sans nuire aux performances.
- Réduisez la complexité grâce à une solution SaaS hébergée dans le cloud qui ne nécessite aucun matériel et qui contribue à réduire les coûts opérationnels.

L'APPROCHE DE SÉCURITÉ DE CROWDSTRIKE VOUS PROTÈGE DES COMPROMISSIONS

L'agent léger Falcon peut être installé facilement dans l'environnement WorkSpaces d'un utilisateur final, afin que celui-ci puisse télétravailler en toute sécurité. Ensemble, ces solutions cloud native permettent d'assurer la continuité des activités en bloquant les menaces émergentes, en proposant une solution hybride sécurisée et en réduisant les coûts grâce à une diminution de la charge administrative.



80 %
des compromissions impliquent des identifiants compromis

Barrez la route aux cyberadversaires

Compte tenu des nouvelles menaces qui ciblent les vulnérabilités des effectifs hybrides, la sécurité offerte par un cloud privé virtuel (VPC) Amazon et la protection des endpoints par Falcon sont essentielles. Protégez vos effectifs hybrides grâce à une solution de cybersécurité qui allie Machine Learning, intelligence artificielle et Threat Hunting proactif.

Assurez la réponse, la reprise et la correction à distance

Falcon offre une protection à distance pour assurer la sécurité des données, des workloads et des terminaux de vos collaborateurs, où qu'ils se trouvent. Corrigez rapidement les hôtes à distance grâce à une solution cloud native performante.

Compensez les coûts pour renforcer votre résilience

Le DaaS via WorkSpaces et l'architecture cloud native de Falcon réduisent considérablement le matériel requis et la nécessité de mettre en service des terminaux et des logiciels. Adoptez une approche entièrement managée pour réduire votre charge administrative et renforcer votre résilience.

SE DÉFENDRE CONTRE LES CYBERADVERSAIRES LES PLUS DÉTERMINÉS

Derrière chaque attaque se cache un cyberadversaire en chair et en os. Ces cyberattaquants évoluent en permanence et profitent d'événements pertinents pour dissimuler leurs attaques.

CrowdStrike surveille de près les menaces émergentes et a conçu l'agent Falcon pour offrir une visibilité étendue sur les vulnérabilités. En tant qu'agent intégré à Amazon WorkSpaces, Falcon vous aide à rester vigilant afin de protéger vos effectifs hybrides et vos données cloud.

Une protection jusqu'au cloud

Amazon WorkSpaces est déployé au sein de VPC Amazon, qui fournissent à chaque utilisateur un accès à des volumes de stockage persistants et chiffrés dans le cloud AWS, et peut être intégré à AWS Key Management Service. Aucune donnée utilisateur n'est stockée en local sur le terminal, ce qui renforce la sécurité des données des utilisateurs et réduit la surface d'attaque, même pour les effectifs hybrides.

Détection et prévention en temps réel

Optimisé par les renseignements de Threat Graph, Falcon assure la détection et la prévention en temps réel les plus efficaces qui soient des menaces connues et inconnues. Les endpoints sont protégés 24 heures sur 24 et 7 jours sur 7 des cyberadversaires.

Falcon ne se limite pas aux logiciels malveillants : il emploie une approche centrée sur les cyberadversaires qui identifie les indicateurs de compromission, mais aussi les indicateurs d'attaque.

BONNES PRATIQUES DE CYBERSÉCURITÉ POUR UN MONDE HYBRIDE

À l'ère du télétravail, la cybersécurité requiert une approche différente. Les systèmes qui protègent les utilisateurs au bureau exigent une analyse à large bande passante pour identifier les systèmes, évaluer les correctifs et visualiser les vulnérabilités. Dans un scénario de travail hybride, une telle configuration n'est plus possible. Les collaborateurs qui partagent leur temps entre le bureau et l'extérieur, et qui accèdent donc à vos données sur des terminaux managés et non managés, créent d'importantes zones d'ombre pour le personnel de sécurité informatique, introduisant ainsi des risques inconnus qui peuvent ralentir les efforts de neutralisation des menaces.

Pour relever les défis de cybersécurité de ce nouvel environnement de travail, les experts de CrowdStrike recommandent les bonnes pratiques suivantes :

Autonomisez les collaborateurs et tirez parti des technologies

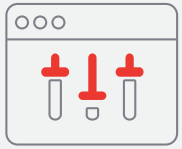
L'élaboration d'une stratégie de cybersécurité complète et efficace commence par l'examen des règles, processus et technologies de chaque fonction métier. Les stratégies de cybersécurité les plus efficaces combinent ressources humaines et solutions technologiques avancées, telles que l'intelligence artificielle, le Machine Learning et d'autres formes d'automatisation intelligente, afin d'améliorer la détection des activités anormales et de réduire le délai de réponse et de correction.

Choisissez votre cloud avec soin

Tous les clouds ne se valent pas lorsqu'il s'agit de tirer parti des avantages des technologies cloud sans compromettre la sécurité. Amazon Web Services (AWS) a été conçu pour répondre aux normes les plus strictes de sécurité des données. À cette fin, il offre des contrôles granulaires des identités et des accès pour une visibilité inégalée. Les fonctionnalités de prévention et de détection de pointe de CrowdStrike pour Amazon WorkSpaces prennent en charge vos collaborateurs en télétravail sans nuire à la continuité de vos activités.

Assurez la réponse, la reprise et la correction à distance

Les attaques et les intrusions ne sont pas près de s'arrêter. Vous devez donc vous assurer de disposer des ressources et des fonctionnalités nécessaires pour répondre aux incidents où qu'ils surviennent et protéger votre entreprise. L'architecture cloud d'Amazon WorkSpaces et de Falcon vous permet de protéger tous les workloads, où qu'ils se trouvent, y compris ceux à l'extérieur d'un pare-feu, pour une sécurité en temps réel.



Simplifiez la distribution des bureaux

Amazon WorkSpaces étant un service cloud, l'inventaire matériel à gérer est moins important. En outre, vous n'avez pas besoin de déployer des infrastructures de bureau virtuel complexes et non évolutives. Amazon WorkSpaces est disponible dans 13 régions AWS et offre un accès à des bureaux cloud hautes performances quel que soit l'endroit où travaillent vos équipes.

LA SÉCURITÉ COMMENCE PAR LA GESTION DES COÛTS

Les entreprises du monde entier sont confrontées au climat d'incertitude. Pressées de renforcer leur résilience, elles ont mis en pause leurs initiatives de croissance, verrouillé leurs budgets et commencé à accumuler des liquidités. Avec Amazon WorkSpaces et CrowdStrike Falcon, les entreprises disposent d'un moyen d'assurer la continuité de leurs activités en toute sécurité et de limiter les coûts.

Architecture cloud rentable

Les fonctionnalités de gestion centralisée d'Amazon WorkSpaces pour les télétravailleurs permettent de faire évoluer l'accès aux bureaux cloud. Ainsi, vous n'avez pas besoin de planifier, de préparer et de mettre en service du matériel et des logiciels pour continuer à prendre en charge vos effectifs hybrides, ce qui vous permet de gagner du temps et de l'argent. En outre, Amazon WorkSpaces élimine la nécessité d'acheter une grande quantité d'ordinateurs portables et de bureau en fournissant un accès à la demande aux bureaux cloud, qui incluent un large éventail de ressources de calcul, de mémoire et de stockage pour répondre aux besoins de vos effectifs hybrides en matière de performances.
La plateforme CrowdStrike Falcon analyse tous les endpoints pour assurer leur sécurité où qu'ils se trouvent et sans nuire aux performances.

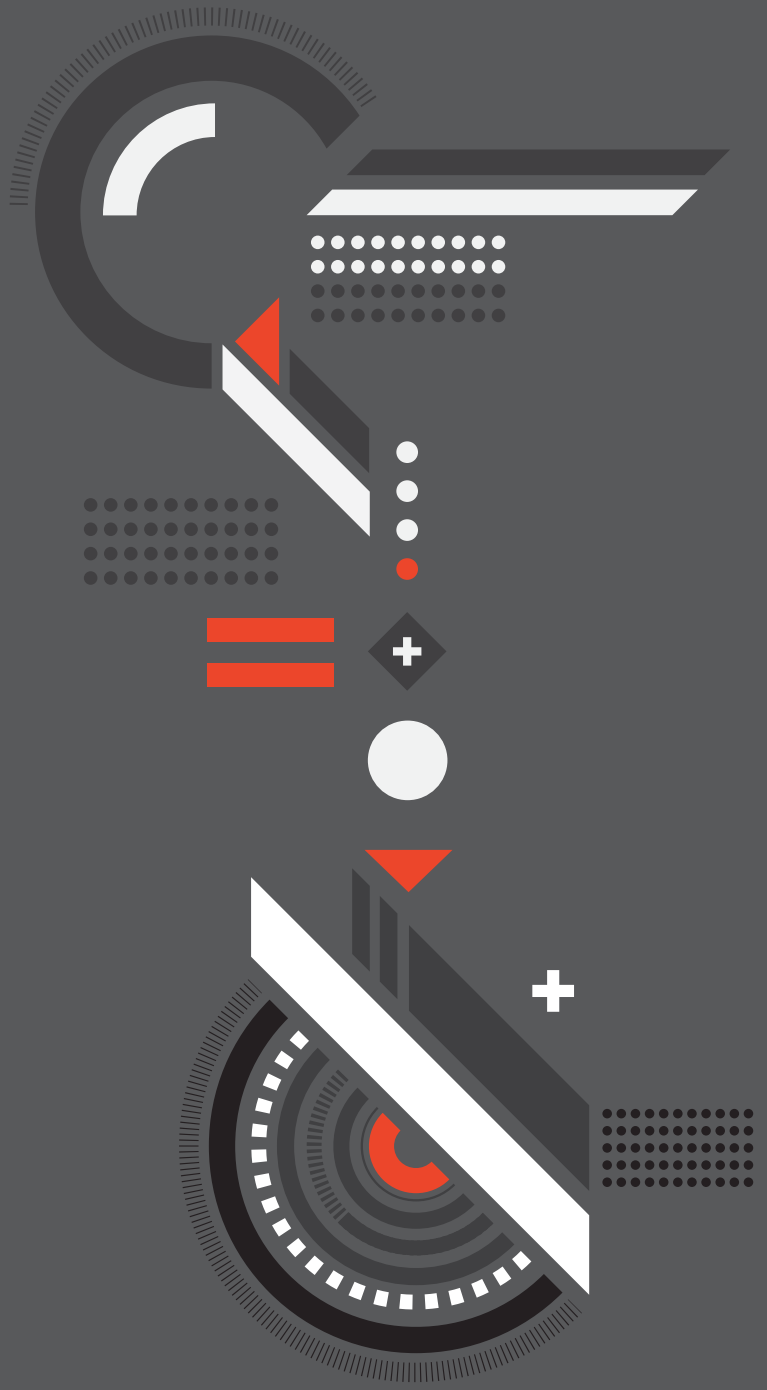
Service entièrement managé pour une charge administrative réduite

Les entreprises ont la possibilité de booster leurs efforts de cybersécurité en déployant la protection des endpoints Falcon en tant que service entièrement managé. Cette solution sans faille vous permet de confier l'implémentation et la gestion de la sécurité des endpoints, ainsi que la réponse à incident, à l'équipe d'experts en sécurité chevronnés de CrowdStrike. Vous bénéficiez ainsi instantanément d'un niveau de sécurité optimisé, sans devoir assumer la charge, la complexité et le coût de la gestion interne d'un programme complet de sécurité des endpoints.

IL EST TEMPS DE SÉCURISER VOTRE ENVIRONNEMENT DE TÉLÉTRAVAIL

CrowdStrike facilite la prise en main. Pour en savoir plus sur l'implémentation de la plateforme CrowdStrike Falcon et/ou Amazon WorkSpaces, **profitez de notre évaluation gratuite de 15 jours**.

Pour en savoir plus sur les solutions CrowdStrike et AWS, consultez le **site de CrowdStrike** ou **AWS Marketplace**.



aws marketplace