LIVRE ÉLECTRONIQUE

Une sécurité simple et efficace pour la transformation de votre réseau

cisco

Dans ce livre électronique :

Voici ce que disent les statistiques :

82 %

Dans une proportion de 82 %, les travailleurs mobiles admettent qu'ils n'utilisent pas toujours un RPV lorsqu'ils travaillent[2].

60 %

Dans 60 % des cas, quelques minutes ont suffi pour pénétrer dans les systèmes d'une organisation et en compromettre la sécurité, alors que la détection de tels méfaits prend plusieurs jours[3].

Plus de 475

Une entreprise utilise en moyenne plus de 475 applications de tierces parties[4].

Plus de 50

Certaines entreprises ont recours à plus de 50 fournisseurs pour leurs besoins en matière de sécurité[5].

Le nouveau champ de bataille de la sécurité : mobilité, logiciel-service (SaaS) et transformation des bureaux régionaux

Auparavant, la sécurité des données et des ordinateurs était gérée sur le réseau, car toute l'activité des utilisateurs y était regroupée. Aujourd'hui, les choses sont différentes. L'explosion du recours aux appareils mobiles, au nuage, à la tendance BYOD (apportez votre propre appareil) et à l'Internet des objets (IDO) présente des défis sur tous les fronts :

1. **Mobilité.** Aujourd'hui, les utilisateurs travaillent partout. S'ils ne sont pas sur le réseau ou n'utilisent pas le RPV, leurs appareils sont vulnérables aux maliciels.

2. **Bureaux régionaux.** Plutôt que d'assurer l'acheminement du trafic sur le réseau d'entreprise, environ 70 % des bureaux régionaux se connectent directement à Internet. Les appareils et les données sont ainsi vulnérables en raison d'une sécurité insuffisante sur place[1]. Comme les entreprises adoptent des réseaux étendus reposant sur des logiciels (SD-WAN) pour réduire les coûts associés à la commutation multiprotocole par étiquette (MPLS) et améliorer les performances, la sécurité dans le nuage devient un élément plus important que jamais.

3. **Applications dans le nuage.** En misant sur des services dans le nuage pour en tirer un avantage concurrentiel, les organisations permettent que des données d'entreprise gravitent en dehors de leur écosystème. Or, impossible de protéger ce qui n'est pas visible.

4. **Nouvelles menaces.** Aujourd'hui, les menaces sont plus complexes, plus nombreuses et plus dangereuses que jamais, surtout pour les équipes de sécurité informatique disposant de ressources limitées.

5. **BYOD (apportez votre propre appareil).** Lorsque des visiteurs et des employés utilisent leurs appareils personnels pour se connecter à votre réseau Wi-Fi, ce dernier est exposé à la présence d'éventuels fichiers malveillants.

6. **Internet des objets (IDO).** Les appareils intelligents et les dispositifs d'extrémité continuent de se multiplier, et les menaces prolifèrent en parallèle.

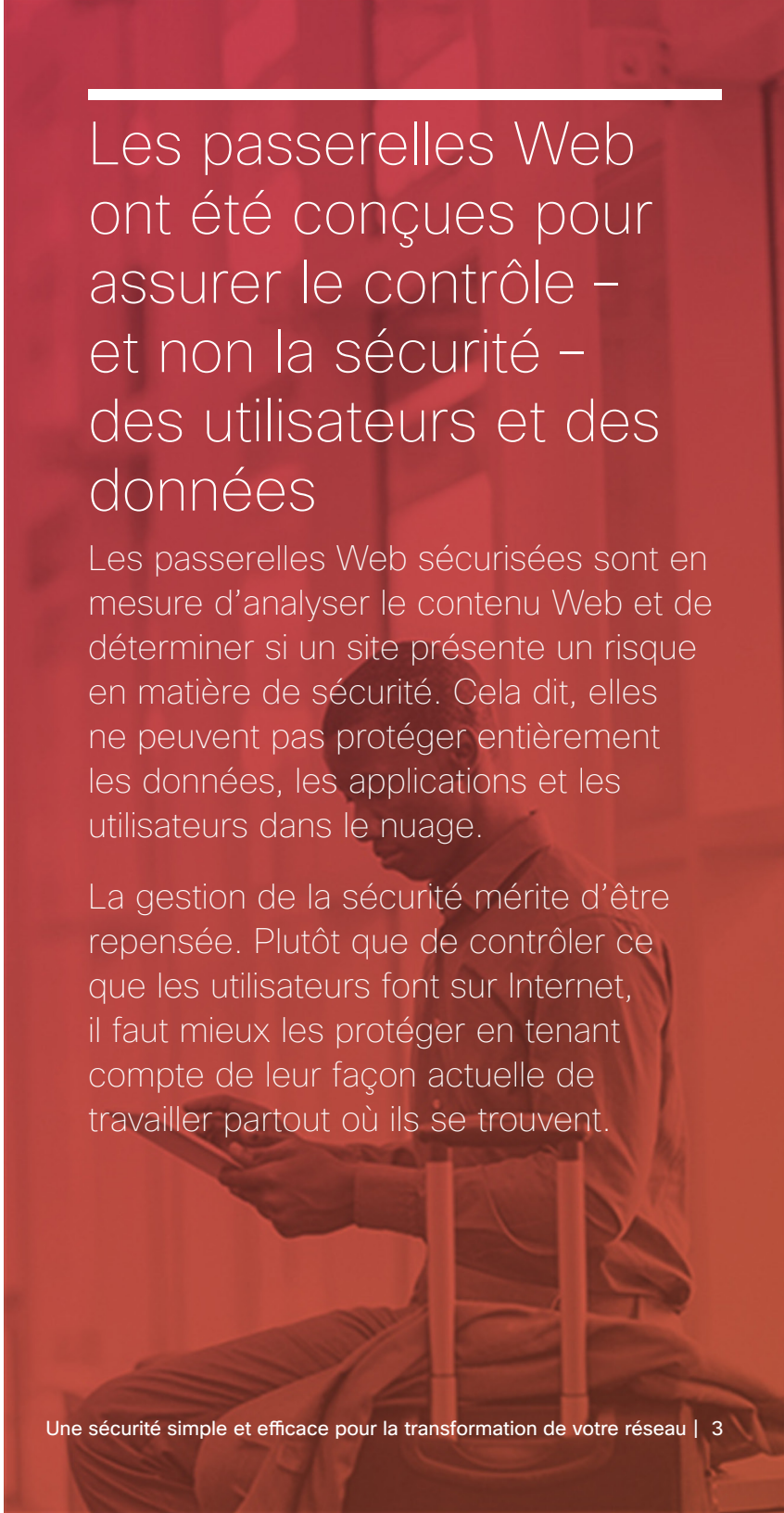
La sécurité traditionnelle est dépassée

Si vous comptez uniquement sur une sécurité traditionnelle, vous êtes vulnérable à de nombreux égards. Lorsque les utilisateurs quittent le réseau, ils créent des zones d'ombre pour lesquelles il est impossible d'assurer la sécurité. Les passerelles Web sécurisées protègent uniquement les ports Web 80/443, alors que 15 % des procédures de rappel malveillantes de type commande et contrôle utilisent des ports autres que le port 80/443 pour exfiltrer des données[6].

Mais ce n'est pas tout. Il faut aussi conserver une longueur d'avance. Dans la sécurité traditionnelle, la vigie des menaces repose sur des notes établies après la détection de ces menaces. Les nouvelles menaces et celles en gestation ne sont pas détectées. De plus, si vous comptez uniquement sur des éléments matériels, votre capacité d'action se trouve limitée par la puissance de traitement de vos appareils.

Les solutions traditionnelles limitent également l'intégration. Comme c'est un usage répandu, votre entreprise utilise probablement plusieurs produits de sécurité provenant de différents fournisseurs[5], et ces derniers travaillent généralement en silo. Il vous incombe alors d'établir des rapprochements, de faire des synthèses et d'établir les priorités en fonction des alertes, sans disposer d'une vue d'ensemble cohérente de votre environnement.

Enfin, les logiciels-service (SaaS) qui sont si efficaces d'un point de vue de la productivité n'offrent que peu de visibilité sur les activités de l'utilisateur. Les données sensibles de l'entreprise, des employés et des clients peuvent ainsi être versées dans le nuage et partagées à l'insu de l'équipe informatique et sans le moindre contrôle.



Les passerelles Web ont été conçues pour assurer le contrôle – et non la sécurité – des utilisateurs et des données

Les passerelles Web sécurisées sont en mesure d'analyser le contenu Web et de déterminer si un site présente un risque en matière de sécurité. Cela dit, elles ne peuvent pas protéger entièrement les données, les applications et les utilisateurs dans le nuage.

La gestion de la sécurité mérite d'être repensée. Plutôt que de contrôler ce que les utilisateurs font sur Internet, il faut mieux les protéger en tenant compte de leur façon actuelle de travailler partout où ils se trouvent.

Présentation de la passerelle Internet sécurisée

Une passerelle Internet sécurisée est une plateforme assurant la sécurité de l'ensemble d'un écosystème : nuage, logiciels-service (SaaS), bureaux régionaux et dispositifs d'extrémité. Elle touche tant l'accès que l'utilisation des différentes composantes, partout où vos utilisateurs les utilisent, sur le réseau ou non. Comment? En offrant une voie d'accès sécurisée à Internet dotée des capacités essentielles ci-dessous.

Caractéristiques	Avantages
Protection contre les menaces sur tous les ports et tous les protocoles, sur le réseau d'entreprise et en dehors de ce dernier	Obtenir une visibilité et un levier d'action partout, même lorsque les utilisateurs sont en dehors du RPV, sans latence supplémentaire
Inspection des domaines risqués reposant sur un serveur mandataire (proxy), y compris une inspection des URL et des fichiers par des moteurs antivirus et une protection avancée contre les maliciels	Bloquer davantage de menaces grâce à des inspections approfondies du trafic présentant un risque, sans impact pour les utilisateurs
Plateforme ouverte et API bidirectionnel s'intégrant à votre pile de sécurité existante (y compris les appareils de sécurité, les plateformes et les flux de renseignements, les fournisseurs de services infonuagiques, etc.)	Tirer une plus grande valeur des investissements existants, étendre la protection partout et activer facilement la sécurité pour la transformation des réseaux grâce à l'adoption de réseaux étendus reposant sur des logiciels (SD-WAN)
Vigie des menaces dynamique compilée à partir de requêtes mondiales traitées en temps réel	Protéger les utilisateurs contre les menaces émergentes avant le lancement des attaques
Découverte et contrôle des logiciels-service (SaaS)	Assurer la sécurité des utilisateurs, des données et des applications, peu importe où ils résident

Cisco Umbrella : la passerelle Internet sécurisée de l'avenir est maintenant accessible

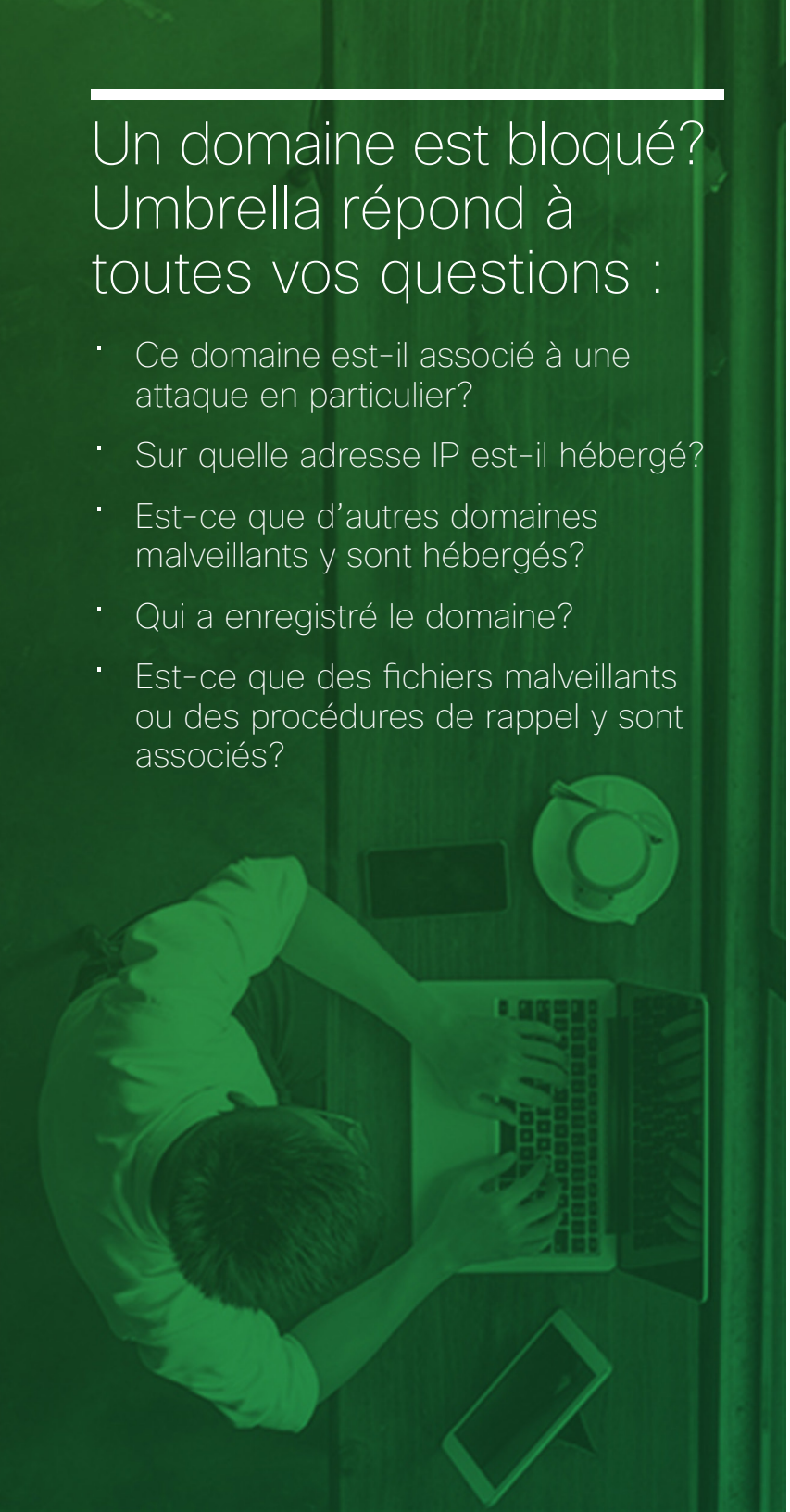
Cisco Umbrella est votre première ligne de défense contre les menaces. Peu importe quand et où vos utilisateurs accèdent à Internet, le trafic passe d'abord par Umbrella. Umbrella bloque les connexions aux sites qui hébergent des maliciels ou des campagnes d'hameçonnage et bloque les menaces avant qu'elles atteignent les points d'extrémité. Si des périphériques infectés se joignent à votre réseau, Umbrella retient les procédures de rappel de type commande et contrôle pour arrêter l'exfiltration de données. Umbrella fournit les éléments suivants :

- **Visibilité et protection** permettant de voir tous les périphériques réseau, les emplacements réseau, les utilisateurs itinérants et les applications risquées ou inappropriées.
- **Intelligence** permettant de prévoir et d'arrêter les attaques avant qu'elles ne soient lancées, en tirant parti de plus de 125 milliards de requêtes Internet quotidiennes et de plus de 11 milliards d'événements historiques.
- **Couverture étendue** des destinations malveillantes et des fichiers malveillants. Umbrella utilise des modèles d'apprentissage automatique pour découvrir les menaces connues et émergentes et les bloquer au niveau des couches du système DNS et du protocole IP. Il inspecte les fichiers à l'aide de moteurs antivirus et de la protection avancée contre les logiciels malveillants de Cisco pour réaliser un blocage en ligne.
- **Plateforme ouverte** facile d'intégration, qui permet de programmer une extension de la protection au-delà de l'écosystème, afin d'assurer la sécurité des utilisateurs mobiles.
- **Découverte et contrôle** des données sensibles dans l'ensemble des logiciels-service (SaaS) lorsque vous jumelez Cisco Umbrella et Cisco Cloudlock.

Passerelle Internet sécurisée de Cisco

Un domaine est bloqué? Umbrella répond à toutes vos questions :

- Ce domaine est-il associé à une attaque en particulier?
- Sur quelle adresse IP est-il hébergé?
- Est-ce que d'autres domaines malveillants y sont hébergés?
- Qui a enregistré le domaine?
- Est-ce que des fichiers malveillants ou des procédures de rappel y sont associés?



Umbrella est différent. Voici comment.

Aucune autre passerelle Internet sécurisée sur le marché ne fournit une telle combinaison de vitesse, de fiabilité à 100 % et de visibilité complète.

1. **Une solution simple, extrêmement simple.** Comme le système DNS repose sur un protocole utilisé par tous les périphériques qui se connectent à Internet, vous n'avez qu'à faire pointer votre système DNS sur le réseau mondial d'Umbrella, et tous les appareils qui se joignent à votre réseau seront protégés.

2. **Un déploiement en quelques minutes, et non en plusieurs jours, voire plusieurs mois.** Il n'y a aucun matériel à déployer ni aucun logiciel à tenir à jour. De plus, vous pouvez tirer parti de votre empreinte Cisco existante pour atteindre des milliers de périphériques réseau et d'ordinateurs portables en quelques minutes. Aucun autre produit de sécurité ne peut être déployé plus rapidement ou mis à l'échelle avec aussi peu de perturbations.

3. **Disponibilité opérationnelle à 100 % à vitesse maximale.** Notre réseau mondial utilise le routage Anycast, qui vous relie à tout moment au centre de données le plus rapide au lieu de vous attacher à un seul centre de données. L'équilibrage de charge automatique permet de s'assurer de compter sur la vitesse la plus rapide possible. Vos utilisateurs constateront peut-être même une amélioration.

4. **Une vigie des menaces réellement utilisable.** Umbrella présente un portrait complet de l'infrastructure de l'attaquant et fournit des informations détaillées sur tout domaine bloqué.

Cisco : une gamme complète de solutions de sécurité

Obtenez une protection complète et unifiée d'un seul fournisseur pour tous vos dispositifs d'extrémité, tous vos bureaux régionaux et tous vos utilisateurs, applications et données dans le nuage. Protégez chaque emplacement et chaque appareil de manière uniforme, et outillez votre personnel restreint en informatique afin de le rendre plus efficace que jamais.

Protection des points d'extrémité

En combinant Umbrella avec la protection avancée contre les logiciels malveillants de Cisco pour les points d'extrémité, vous comptez sur la protection des points d'extrémité la plus complète. Umbrella fournit une première ligne de défense contre les menaces en bloquant les connexions aux sites malveillants au point le plus rapproché possible. Ensuite, la protection avancée contre les logiciels malveillants pour les points d'extrémité fournit la dernière ligne de défense en bloquant de façon proactive des fichiers malveillants avant leur exécution et en établissant une surveillance continue et des balayages de sécurité rétrospectifs pour contenir et supprimer les menaces qui auraient échappé aux défenses initiales.

Protection des bureaux régionaux

Que vous transformiez le réseau de vos bureaux régionaux en adoptant une technologie de réseaux étendus reposant sur des logiciels, tels que Cisco SD-WAN (Viptela) ou Meraki MX, ou que vous mettiez à la disposition de vos clients un réseau Wi-Fi d'invités, Umbrella représente un moyen simple et efficace d'ajouter la sécurité et de protéger les utilisateurs qui se connectent directement à Internet.

Protection du nuage

Cisco propose une gamme de produits pour assurer la transition et le déplacement des données, des applications et des infrastructures vers le nuage. Dans le cas d'Office 365, Umbrella peut être jumelé aux solutions Cisco Cloudlock et Cloud Email Security (sécurité de la messagerie en nuage) pour offrir une protection plus complète contre l'hameçonnage, les rançongiciels, la compromission des courriels d'entreprise et plus encore.

Profitez d'un essai gratuit de Cisco Umbrella et déployez-le dans votre plus grand point de sortie. Nous vous prouverons que nous sommes la protection la plus rapide et la plus efficace.

ESSAYEZ-LE DÈS AUJOURD'HUI

Sources :

1. « Securing Direct-To-Internet Branch Offices: Cloud-Based Security Offers Flexibility and Control ». Forrester, 2015.
2. « Your Users Have Left the Perimeter. Are You Ready? ». IDG, 2016
3. « 2015 Cost of Data Breach Study: Global Analysis ». Ponemon Institute, 2015
4. « Cloud Cybersecurity Report: The Extended Perimeter ». Cisco Cloudlock, 2015
5. Rapport annuel 2017 de Cisco sur la cybersécurité. Cisco, 2017.
6. « Visual Investigations of Command & Control Botnet Behavior ». Cisco (Lancope), 2013.

Le bilan est simple : une sécurité plus intelligente, plus rapide et plus complète

Cisco est reconnue comme l'un des fournisseurs de système DNS les plus rapides au monde. Et quand il est question d'intelligence et de renseignements, nous allons bien au-delà de l'apprentissage artificiel.

Nous avons réuni une équipe de recherche composée de scientifiques des données, de spécialistes en infrastructure et de chercheurs en menaces informatiques, et nous lui avons donné une vocation non conventionnelle. Plutôt que de procéder à une rétro-ingénierie des maliciels, l'équipe trouve de nouvelles façons d'appliquer des concepts mathématiques aux données de sécurité, en créant des systèmes d'apprentissage automatique qui classifient et notent automatiquement les domaines et les protocoles IP, afin de découvrir les menaces avant même le début des attaques. Les équipes de recherche de Cisco Umbrella et Talos représentent le plus grand groupe d'experts dans le marché de la sécurité.

Grâce à Umbrella, vous pouvez arrêter l'hameçonnage et les maliciels plus tôt, relever plus rapidement les périphériques déjà infectés et empêcher l'exfiltration de données. Et comme il est déployé dans le nuage, Umbrella représente une plateforme de sécurité efficace qui est ouverte, automatisée et simple à utiliser.

Aucune autre passerelle Internet sécurisée ne peut vous protéger avec la vitesse, l'intelligence et la fiabilité de Cisco Umbrella.