CYBERSECURITE

Livre blanc 2021

CYBERSÉCURITÉ

La cybersécurité renvoie à la protection des ressources disponibles sur le web, notamment le matériel, les logiciels et les données, contre la cyber menace. Les consommateurs et les entreprises adoptent cette méthode pour empêcher l'accès illégal aux centres d'information et autres systèmes numériques.

Un riche programme de cybersécurité peut garantir une véritable sécurité contre les attaques hostiles visant à accéder aux systèmes d'une entreprise ou d'un client, à les modifier, à les supprimer, à les détruire ou à extorquer des données essentielles. La cybersécurité est également essentielle pour répondre aux attaques qui visent à neutraliser ou à perturber les fonctionnalités d'un système ou d'un appareil.

Elle désigne le processus de protection des postes de travail, des serveurs, des dispositifs portables, des dispositifs de communication, des réseaux et des contenus contre les intrusions. Elle est également appelée sécurité de l'information électronique ou sécurité des technologies de l'information.

IMPORTANCE DE LA CYBERSÉCURITÉ

Le besoin de cybersécurité ne cesse de croître à mesure que le nombre de personnes, de dispositifs et de programmes dans l'entreprise moderne augmente, de même que le flot croissant de données, dont la plupart sont confidentielles ou privées. Le problème est intensifié par le nombre et la complexité accrus de cybercriminels et de stratégies d'attaque.

La cybersécurité est essentielle dans la mesure où elle protège tous les types de données contre le vol ou la perte. Les informations sensibles, les informations personnelles (IIP), les renseignements personnels sur la santé (RPS), les données privées, les droits d'auteur, les statistiques et la sécurité des informations gouvernementales et industrielles entrent tous dans cette catégorie.

Sans plan de sécurité, votre entreprise est incapable de se protéger contre toute opération de piratage, ce qui en fait une cible facile pour les pirates.

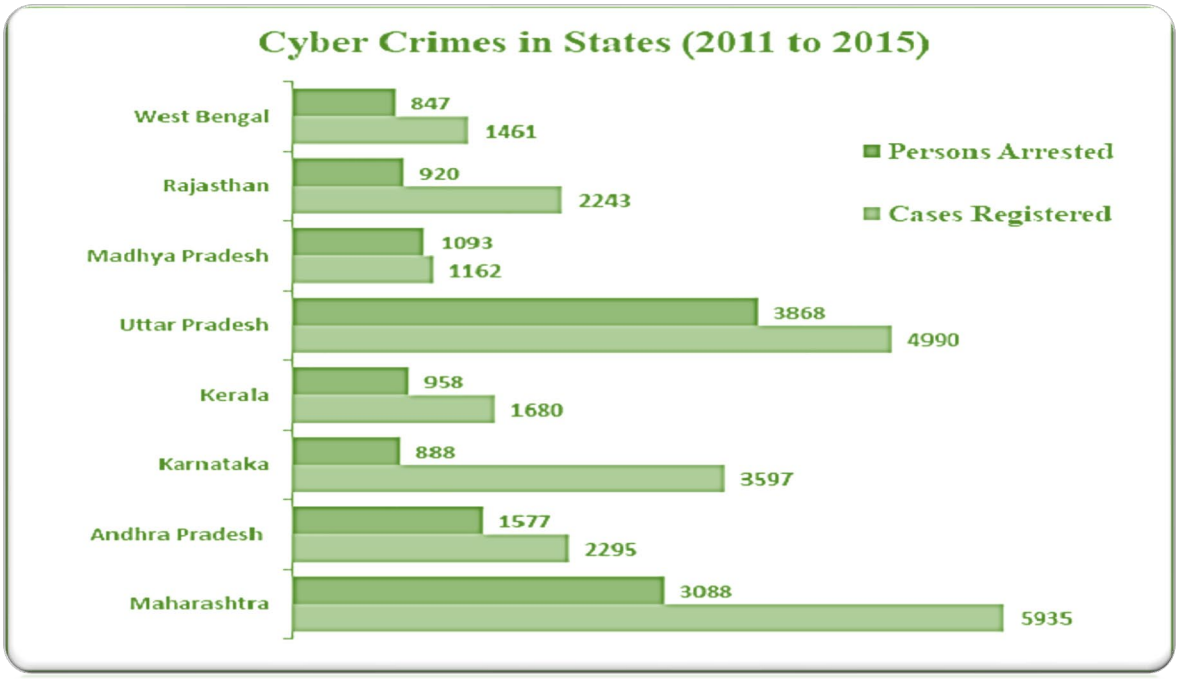
La mondialisation et l'utilisation du cloud computing, comme Amazon Web Services, pour stocker des données personnelles essentielles, font peser une menace à la fois innée et résiduelle. De plus, en raison de la conception souvent inappropriée des services cloud et de l'intelligence croissante des pirates informatiques, le risque que votre entreprise soit victime d'une cyberattaque à grande échelle est en augmentation.

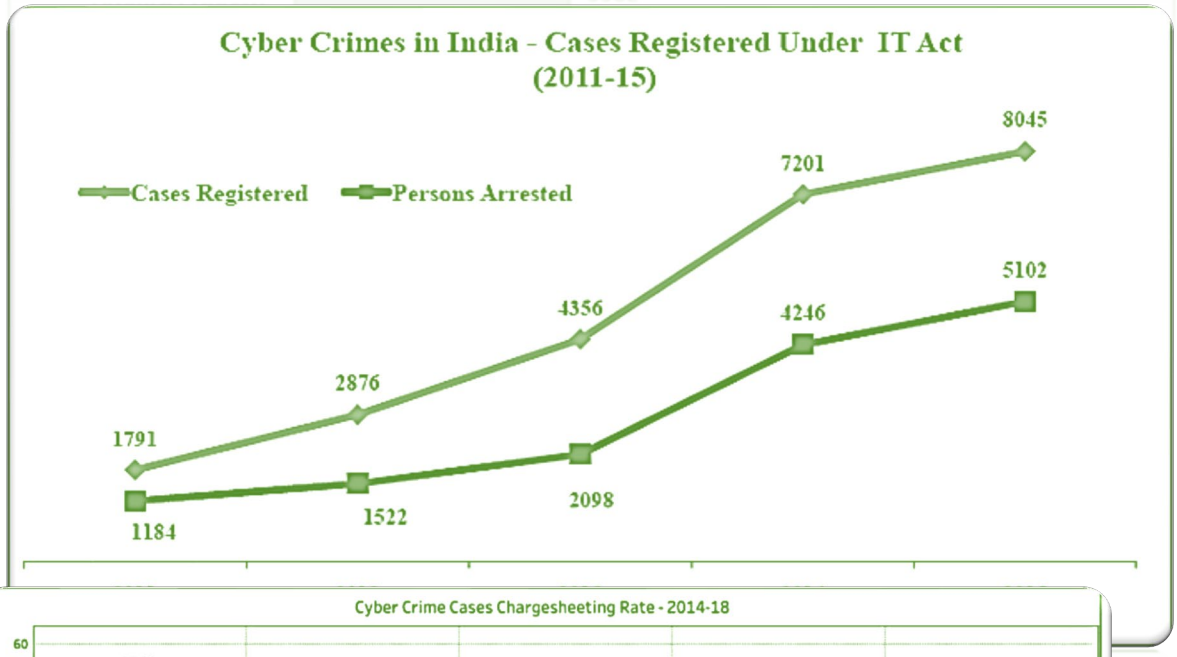
Les cybercriminels sont plus malins et leurs techniques sont beaucoup plus résistantes à la cyberdéfense traditionnelle. Les entreprises ne peuvent donc plus se contenter de solutions de cybersécurité prêtes à l'emploi tels les antivirus et les passerelles.

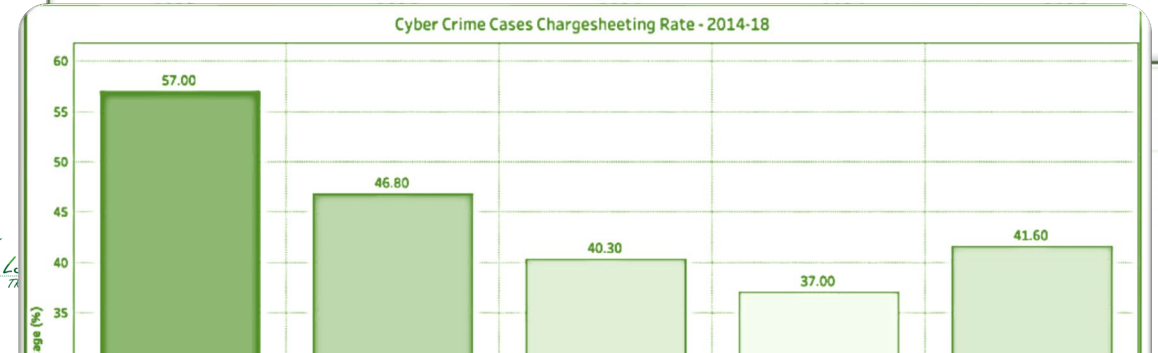
L'importance de la cybersécurité va croissante. Notre culture est plus que jamais dépendante de la technique, et cette tendance ne montre aucun signe de ralentissement. Aujourd'hui, les atteintes à la protection des données susceptibles d'entraîner une usurpation d'identité sont ouvertement diffusées sur les réseaux sociaux. Les numéros de compte, les informations relatives aux cartes de crédit et les informations bancaires sont désormais sauvegardés dans des services de stockage en ligne tels que Dropbox ou Google Drive.

Que vous soyez un particulier, une entreprise locale ou une grande société, vous dépendez au quotidien des réseaux internet. Si vous y ajoutez la croissance des services cloud, des services cloud non sécurisés, des téléphones portables et de l'Internet des objets (IoT), vous obtenez une multitude de dangers de cybersécurité qui n'existaient même pas quelques décennies auparavant. Même si les compétences et les connaissances sont de plus en plus similaires, nous devons faire la distinction entre cybersécurité et sécurité des données.

Les raisons de la montée de la cybercriminalité







Le piratage d'informations personnelles est de loin le type de cybercriminalité le plus coûteux et le plus rapide. La disponibilité accrue des informations d'identification des utilisateurs sur l'Internet via les services cloud est à l'origine de cette tendance.

Toutefois, ce n'est pas la seule raison. Les centrales électriques et autres installations peuvent être démolies si les contrôles de l'entreprise sont endommagés ou détruits. Les cyberattaques.

Les cybercriminels deviennent de plus en plus avertis et changent de cible, d'impact sur les entreprises et de tactique d'attaque pour les différents systèmes de sécurité. Ils peuvent également tenter de porter atteinte à l'intégrité des données (supprimer ou modifier des données) pour susciter la méfiance à l'égard d'une organisation ou d'un gouvernement.

L'ingénierie sociale reste le type de cyberattaque le plus courant, suivi des logiciels malveillants, du piratage et des logiciels espions. Un autre outil d'administration de premier plan est constitué par les fournisseurs tiers et quatrième partie qui gèrent vos informations et dont les procédures de cybersécurité sont faibles, ce qui rend encore plus critique la gestion des risques par les fournisseurs et l'évaluation des risques par les tiers.

D'autres facteurs contribuent à la montée de la cybercriminalité, notamment :

- La structure dispersée d'Internet ;
- Étant donné que les cybercriminels peuvent mener des attaques en dehors de leur territoire, la réglementation devient extrêmement compliquée ;
- La promotion et la simplicité du commerce ;
- L'Internet des objets et la montée en puissance des appareils numériques.

CARACTÉRISTIQUES D'UNE POLITIQUE EFFICACE EN MATIÈRE DE CYBERSÉCURITÉ

Elle fonctionne

Le plus important dans toute politique est qu'elle fonctionne. Bien que cela puisse sembler évident, vous serez surpris de voir combien de stratégies de cybersécurité d'entreprise apparemment efficaces entravent les résultats au lieu de les améliorer. Une politique de cybersécurité utile est une politique qui est suffisamment efficace pour empêcher les envahisseurs de réseau indésirables d'entrer tout en permettant à vos clients et partenaires commerciaux d'accéder rapidement aux données dont ils ont besoin.

Une stratégie de cybersécurité pratique doit être simple à comprendre. Cela garantit que tous les membres de l'entreprise, du PDG au stagiaire du help desk, sont parfaitement au courant des problèmes traités et de la manière dont ils peuvent aider. Les règles de cybersécurité ne peuvent être utiles que si chacun au sein de l'entreprise est responsable de leur maintien en sécurité. Un système n'est efficace que comme son maillon le plus faible, et vous devez donc vous attendre à ce que les cybercriminels découvrent cette faiblesse flagrante tôt ou tard.

Elle évolue avec le temps

Ce qui a permis de sécuriser des informations sensibles en 2014 ne le fera pas en 2015, et ce qui fonctionne en 2015 ne sera peut-être pas suffisant pour répondre aux exigences de sécurité les plus pressantes en 2016. En raison d'un tel manque d'adaptation de la culture de sécurité de l'information des entreprises, des entreprises criminelles entières se sont constituées suite à l'évolution du comportement des cybercriminels au fil du temps. En effet, les malfaiteurs pouvant réagir à de nouvelles situations plus rapidement et plus efficacement que jamais, la seule façon de contrer leurs menaces est d'être aussi adaptable qu'eux.

Une mise à jour périodique, tous les six à douze mois, doit être intégrée à votre politique de cybersécurité. L'équipe de cybersécurité de votre entreprise se réunira alors pour traiter les problématiques qui sont ressorties à ce moment-là. Avant d'être appliquée, la politique doit être examinée, modifiée et approuvée.

Elle tient compte de l'erreur humaine

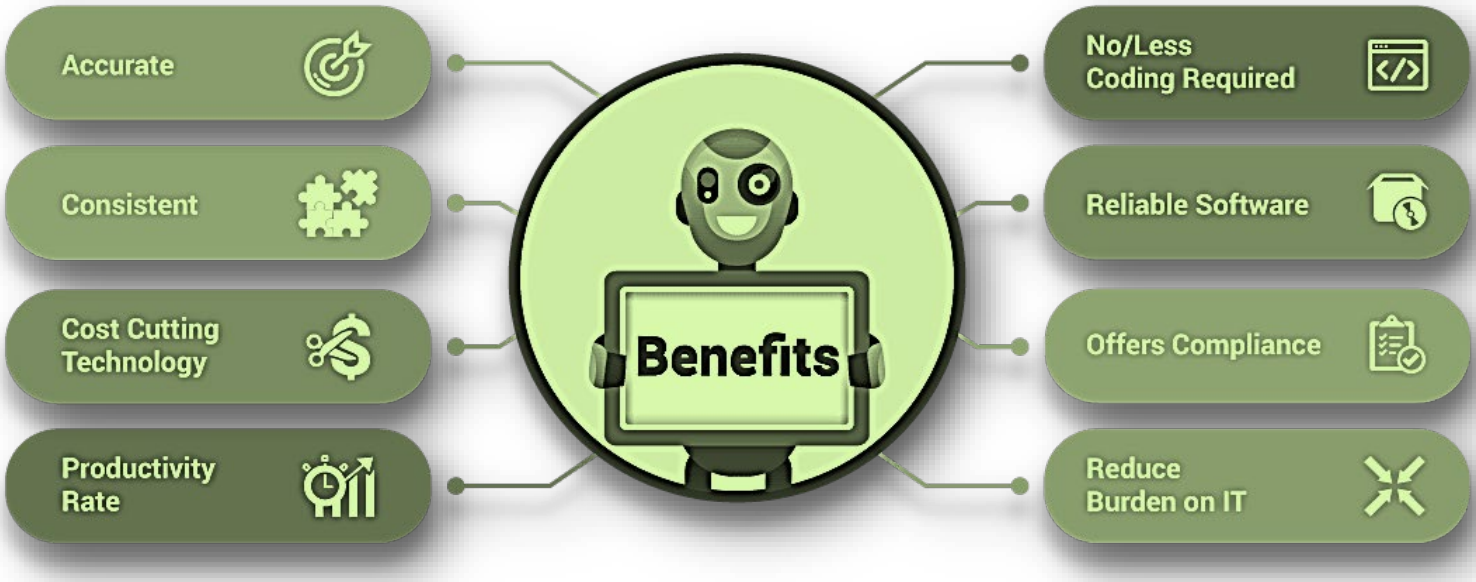
Nous sommes tous des humains, donc susceptibles de commettre des erreurs. Par conséquent, dans votre architecture de cybersécurité, le gros du travail doit être géré.

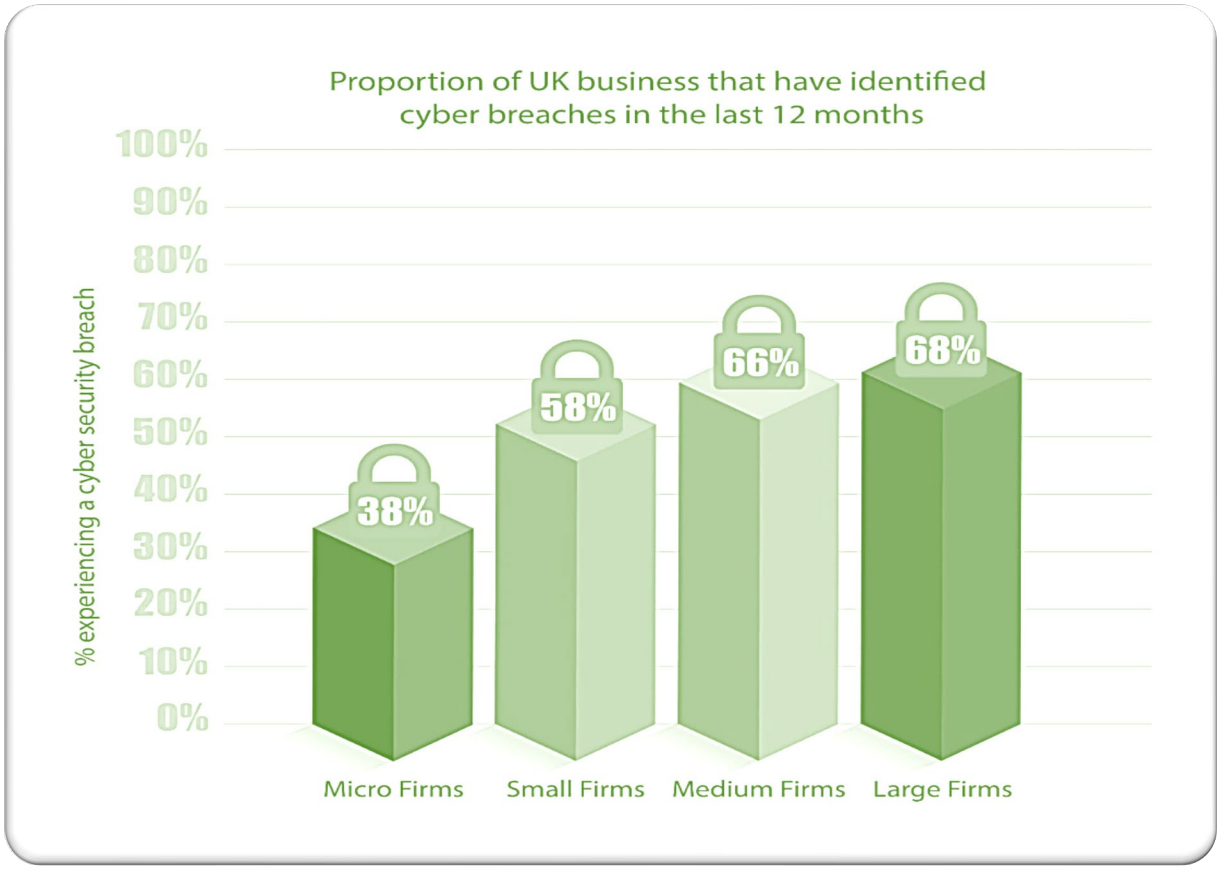
Le personnel, les sous-traitants, les fabricants et les grossistes auront moins de temps pour commettre des erreurs si vous automatisez au maximum. Même si des erreurs peuvent se produire dans cet environnement, une politique de cybersécurité dynamique et parfaitement adaptée donnera la structure nécessaire pour inverser ou isoler les erreurs selon les besoins.

Elle prévoie les exemptions

Dans le meilleur des mondes, il ne serait pas nécessaire de procéder à des changements et il n'y aurait pas d'exceptions. Cependant, nous ne vivons pas dans un environnement idéal, et les exceptions peuvent devenir la norme lorsqu'il s'agit d'un ensemble de règles régulièrement mises à jour, qui doivent être flexibles et adaptables. Lors de la rédaction de votre politique de cybersécurité, vos divisions commerciales n'ont peut-être pas exploré toutes les possibilités ni planifié les choses suffisamment en détail pour répondre à toutes leurs demandes. Cela implique que vous devez être prêt à mettre en place une procédure exceptionnelle normalisée, documentée, fiable et bien organisée.

Les avantages de la cybersécurité





- Protection de votre entreprise - les solutions de cybersécurité offrent une protection numérique à votre entreprise, garantissant que votre personnel est à l'abri de menaces telles que les adwares et les rançongiciels.
- Productivité renforcée - les bugs peuvent paralyser les machines, rendant le travail quasiment impossible. Une cybersécurité efficace réduit ce risque, permettant à votre entreprise d'atteindre son plein potentiel.
- Inspire la confiance des clients - si vous pouvez démontrer que votre entreprise est bien protégée contre tous les types de cyberattaques, vous pouvez donner à vos clients l'assurance que leurs informations personnelles ne seront pas exploitées.
- Sécurité pour vos consommateurs - garantir que votre entreprise est à l'abri des cyberattaques peut également contribuer à protéger vos clients, qui pourraient être vulnérables à une cyber-violation par le biais de proxys.
- Empêche la chute de votre site web - Si vous possédez un site web et que vous le gérez vous-même, une cyber-attaque peut être redoutable. Si votre réseau est attaqué, votre site Web peut être contraint de fermer, ce qui vous fait perdre de l'argent en raison des paiements perdus.

TOP 5 DES ENTREPRISES DE CYBERSÉCURITÉ

	Darktrace est une startup de cyberdéfense d'IA basée au Royaume-Uni. Elle a été créée en 2013.
	FireEye, basée en Californie, est une entreprise de cybersécurité cotée en bourse. Elle a participé à la découverte et à la limitation d'importantes attaques internet.
	Rapid7 Insight collecte les informations de l'ensemble de votre écosystème, ce qui simplifie la gestion des risques pour les employés, la vérification des comportements préjudiciables, l'analyse et la suppression des menaces, ainsi que l'automatisation des activités.
	Programmes et technologies physiques et logiques intégrés pour la sécurité informatique, notamment la sécurité de l'information, d'une entreprise mondiale.
	Advantaged Account Protection est assuré par CyberArk, une entreprise de sécurité des données cotée en bourse. Les technologies de l'entreprise sont largement utilisées dans les secteurs des produits financiers, de l'énergie, du commerce, de la médecine et du gouvernement.

LA SOLUTION CISCO POUR LA CYBERSÉCURITÉ :

Les pirates ne se soucient guère de la taille de votre entreprise en matière de cybercriminalité ; ils ne s'intéressent qu'à la faiblesse de votre protection. Ils sont plus enclins à s'en prendre aux entreprises dont la cybersécurité est la moins efficace, qu'elles soient grandes ou petites. Les menaces de type rançongiciels sont particulièrement dangereuses. La reprise suite à une attaque par rançongiciel coûte désormais plus de 85 000 dollars en moyenne. D'ici 2021, on s'attend à ce qu'une entreprise soit touchée par un rançongiciel toutes les 12-13 secondes. La cybercriminalité est un problème majeur, et les cybercrimes deviennent de plus en plus complexes. En fait, 85 % des dirigeants de petites entreprises estiment que la sécurité est un enjeu majeur et que la confidentialité et la protection des informations sont devenues des composants de leur environnement professionnel.

Caractéristiques distinctives

- Parce que la solution de sécurité de Cisco est basée sur le cloud et intégrée, elle garantira que vos employés peuvent opérer en toute sécurité à partir de n'importe quelle plateforme, à tout moment et de n'importe quel point, contrairement à tout autre fournisseur.
- Les personnes rejoignent votre plateforme de différentes manières. Ils peuvent y accéder à partir d'un poste de travail, d'un ordinateur personnel ou d'un smartphone si vous avez un personnel mobile ou à distance. Cisco Advanced Malware Protection for Endpoints (Protection avancée contre les logiciels malveillants pour les terminaux) est une solution de sécurité efficace qui identifie et bloque les virus et les menaces sur les systèmes d'exploitation du personnel. Si un logiciel malveillant est installé sur l'ordinateur d'une personne, il peut se propager dans tout votre

système. Tous vos ordinateurs et serveurs importants requièrent une sécurité complète contre les logiciels malveillants.

- Les petites entreprises bénéficient des mêmes technologies d'analyse de la sécurité et de la science des données que les entreprises les plus grandes et les plus complexes du monde, car Cisco a consacré des sommes considérables à la création de son logiciel de sécurité.
- L'analyse de la sécurité de Cisco System est assurée par les systèmes Talos avancés, qui identifient, analysent et protègent contre les attaques existantes et en cours de développement, ce qui permet de se démarquer de tout autre système de cybersécurité.
- Pour une petite entreprise, vous obtenez des fonctions de sécurité sans avoir à payer le prix d'une entreprise. Il n'y a pas d'équipement à installer ni de programme à mettre à jour en permanence car la protection est assurée par le cloud. Vous économisez du temps et de l'argent, puis vous assurez la sécurité de votre petite entreprise.
- Une fois introduit, le logiciel malveillant se reproduit dans tout votre système, chiffrant vos fichiers ou mettant hors service des systèmes essentiels. Le système de nom de domaine est utilisé pour transmettre des informations sur le Web et les réseaux, ainsi la majorité des rançongiciels ne fonctionnent pas sans lui. Cisco Umbrella est la première ligne de défense contre les cyberattaques, protégeant les clients où qu'ils soient grâce à une protection adaptée, rapide et puissante fournie par le cloud.