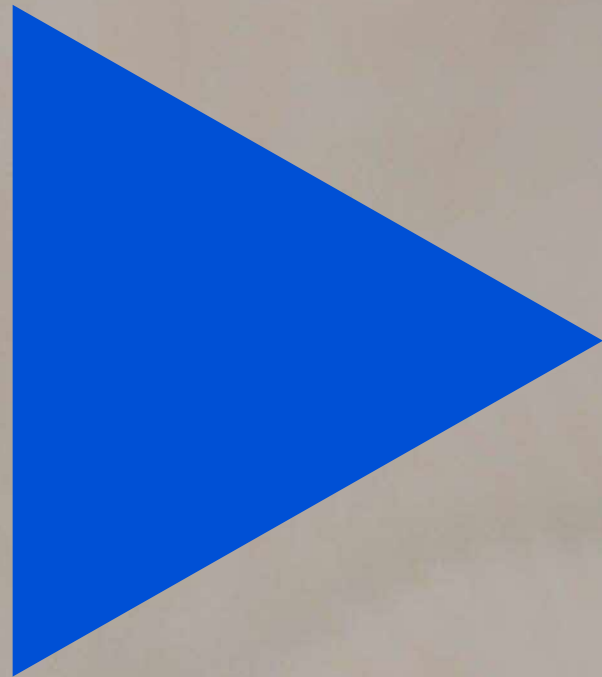




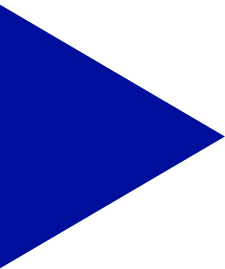
SCANNING...



Comment protéger votre activité en ligne



Un guide complet pour protéger
votre entreprise contre 3 risques
majeurs



Contenu

00 - Introduction	3
01 - Protégez votre marque et votre réputation à mesure que votre identité numérique se développe	4
La réputation est un atout précieux	5
Concevoir une stratégie de nom de domaine	6
Protégez votre marque grâce à l'enregistrement de domaine	7
Préservez la confiance de la marque avec la continuité d'activité	8
02 - Renforcez la stabilité financière pour résister aux marchés fluctuants	10
L'argent est roi	11
Intégrez l'infrastructure numérique dans votre planification financière	12
Choisissez un hébergeur avec des abonnements granulaires	14
Optez pour des outils de sécurité faciles à utiliser	15
03 - Lutte contre les cybermenaces	16
Prenez en main votre sécurité	17
Respectez les bonnes pratiques en matière de cybersécurité	18
Privilégiez la sécurité face aux attaques DDoS, une cybermenace croissante	20
Améliorez la sécurité de votre messagerie	21
Bâissez un avenir sûr pour votre entreprise	22

Introduction

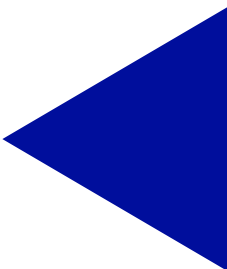
LA CROISSANCE DES ENTREPRISES S'ACCOMPAGNE D'UN PLUS GRAND NOMBRE D'OPPORTUNITÉS ET DE RISQUES

À mesure que le paysage numérique se développe et évolue rapidement, les risques auxquels les petites et moyennes entreprises (PME) sont confrontées évoluent également.

Il est aujourd'hui primordial de renforcer votre présence en ligne pour réussir sur le marché concurrentiel actuel. Pour tirer pleinement parti des avantages de la numérisation, comme l'évolutivité, une plus grande productivité, une meilleure expérience client et une exposition à un public mondial, il est essentiel d'élaborer un plan pour construire une infrastructure numérique forte.

Il existe cependant trois principaux types de risques (réputation, finances et cybersécurité) auxquels vous devez vous préparer à faire face lorsque vous développez en ligne. Heureusement, cette tâche s'avère moins complexe qu'auparavant. Les solutions essentielles pour protéger votre entreprise (ex. hébergement web, sécurité du domaine, sauvegarde des données) ont progressé à un point où il n'est plus nécessaire d'avoir recours à des spécialistes techniques à temps plein ou de collaborer avec plusieurs fournisseurs coûteux pour atteindre vos objectifs.

Voici comment vous pouvez prendre des mesures pratiques et adopter une technologie intuitive visant à protéger votre entreprise et à vous démarquer de la concurrence grâce à une stratégie numérique gagnante.

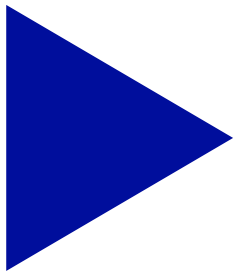




01

**Protégez votre
marque et votre
réputation à
mesure que
votre identité
numérique se
développe**

La réputation est un atout précieux



90% des acheteurs en ligne refusent de consommer auprès d'une entreprise en raison de sa mauvaise réputation.¹

La gestion de la marque et de la réputation devient de plus en plus importante à mesure que votre entreprise étend sa présence numérique. En vous ouvrant à de multiples plateformes en ligne, comme votre site web, les médias sociaux et le marketing par e-mail, vous pouvez interagir avec un plus grand nombre de prospects. Un public plus large, en retour, ouvre des possibilités supplémentaires de vente et de croissance.

Une réputation de marque fiable permet non seulement d'attirer une nouvelle clientèle, mais aussi de maintenir la fidélité des clientes et clients actuels. Les recherches menées par Trustpilot¹ ont révélé qu'une « bonne réputation en ligne » constitue le facteur numéro un permettant d'augmenter la confiance client. Plus de 95 % des consommateurs estiment que la réputation fait une différence tangible dans leur volonté d'acheter auprès d'une marque.

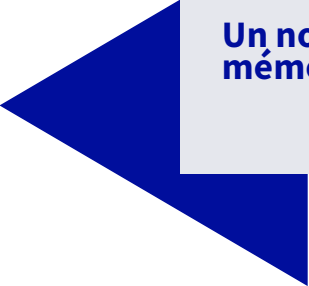
Cependant, cette voie est à double sens : au fur et à mesure que votre présence en ligne augmente, la perception et les opinions de votre clientèle sont également amplifiées via des posts sur les réseaux sociaux, des blogs, des avis et plus encore. Une seule mauvaise expérience peut être partagée à un large public, ce qui peut nuire à votre réputation et inciter les acheteurs à aller ailleurs.

Voici trois étapes à suivre pour aider votre marque à maintenir une excellente réputation afin qu'elle soit perçue comme digne de confiance en ligne.

¹[Rapport Trustpilot - La valeur d'une réputation de marque fiable](#)

CONCEVOIR UNE STRATÉGIE DE NOM DE DOMAINE

Choisir et préserver un nom de domaine adéquat est essentiel pour faire bonne impression sur Internet. Un nom de domaine est une adresse unique utilisée pour accéder à votre site web (ex. ovhcloud.com). Il n'est pas exagéré de dire qu'il s'agit d'une partie intégrante de l'identité de votre entreprise.



Un nom de domaine efficace doit être court, facile à mémoriser et pertinent pour votre marque.

Lors de l'acquisition d'un domaine, vous devez concevoir une stratégie pour protéger votre entreprise contre les risques pouvant menacer votre réputation. Le cybersquatting, entre autres, constitue une tactique courante. Cette méthode consiste à se faire passer pour une marque afin de tromper les utilisatrices et utilisateurs et obtenir des informations sensibles. Pour ce faire, les cybercriminels enregistrent des noms de domaine similaires au vôtre, contenant une extension de domaine légèrement différente (ex. .co au lieu de .com) ou une extension trompeuse liée à l'objectif de votre site web (ex. ovh.cloud au lieu d'ovhcloud.com).

Pour atténuer les risques liés au cybersquatting, il est fortement conseillé d'enregistrer plusieurs noms de domaine. OVHcloud vous facilite la tâche en vous proposant [automatiquement des options](#) parmi notre catalogue de plus de [900 extensions](#) couramment utilisées sur le marché (ex. .com, .net, .org), en fonction de votre emplacement géographique (ex. .fr, .eu, .uk) et de votre secteur d'activité (ex. .fashion, .health, .tech). Vous pouvez même utiliser OVHcloud pour enregistrer des fautes d'orthographe courantes dans votre domaine ou des noms similaires visuellement (ex. utiliser un 0 à la place d'un o).

Il est également essentiel que vous conserviez la propriété de vos noms de domaine aussi longtemps que possible. Sa perte peut en effet nuire à votre réputation, créant la confusion au sein de votre clientèle lorsque cette dernière arrive sur un site différent. De plus, un tel scénario peut entraîner des coûts exorbitants pour récupérer le nom auprès des [cybersquatteurs](#) qui n'hésiteront pas à exploiter cette erreur à leur profit. C'est pourquoi OVHcloud renouvelle automatiquement les noms de domaine par défaut afin de réduire le risque qu'une autre personne prenne votre nom.

Protégez votre marque grâce à l'enregistrement de domaine

En plus d'une stratégie de nom de domaine solide, il existe d'autres mesures que vous devez prendre pour protéger votre domaine contre les cybermenaces. Les acteurs malveillants peuvent tenter d'utiliser des techniques telles que le « domain slamming » (demandes de transfert illégitimes) et le [cache poisoning](#) (ou empoisonnement du cache) pour rediriger les utilisatrices et utilisateurs vers un autre site web, qu'ils pourraient utiliser pour des attaques de phishing, la distribution de spams ou l'hébergement de contenu malveillant. Cela peut nuire gravement à votre réputation et détériorer la confiance de la clientèle.



Nous vous suggérons de suivre toutes ces étapes et d'adopter une approche multicouche pour une sécurité optimale de votre nom de domaine. Ainsi, si une cybermenace contourne un type de mesure de sécurité, une autre couche est mise en place pour contrer l'attaque.

Pour vous défendre contre ces types sophistiqués d'attaques, OVHcloud propose une approche simple, en 1 clic. Celle-ci vous permet :

► 1

d'activer le protocole [Domain Name System Security Extensions \(DNSSEC\)](#) pour vous protéger contre le cache poisoning, une tactique cybercriminelle utilisée pour détourner le trafic vers des sites web malveillants ;

► 2

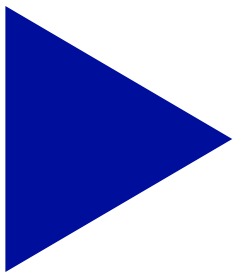
de déclencher un mécanisme pour [empêcher votre domaine de recevoir de faux avis de renouvellement ou d'autres demandes de transfert frauduleuses](#) ;

► 3

d'adopter des mécanismes de sécurité pour vos sites web et vos e-mails, comme les certificats SSL (Secure Sockets Layer) et TLS (Transport Layer Security).

Préservez la confiance de la marque avec la continuité d'activité

Bien sûr, il est impossible d'éliminer tous les risques numériques avec une totale certitude. C'est pourquoi il est important de mettre en place des mesures en cas d'incident (ex. cyberattaque ou pic de trafic) qui menacerait le bon fonctionnement de votre site web. Les temps d'arrêt des sites internet peuvent générer de la frustration au sein de la clientèle, nuire aux revenus et entacher de manière durable la réputation de l'entreprise.



Les temps d'arrêt peuvent coûter jusqu'à 427 \$ par minute aux petites entreprises.²

Un plan de continuité d'activité vous permet de maintenir votre site web en fonctionnement avec peu ou pas de temps d'arrêt en cas d'incident. Il fait partie intégrante de votre stratégie visant à protéger votre réputation et assure la stabilité de votre présence en ligne. Un plan de continuité d'activité doit comprendre les étapes suivantes :

- identifier les applications et les données les plus précieuses nécessaires à la continuité de l'activité;

- Eveiller à ce que seuls les membres formés et disposant d'une expertise informatique suffisante aient accès à la modification des services critiques susceptibles de mettre le système hors service;

- sauvegarder régulièrement [les données et systèmes](#) critiques (fichiers, contenus, bases de données, etc.) afin de restaurer rapidement le site web en cas de besoin;

- choisir un fournisseur réputé capable d'assurer un [temps de disponibilité optimal](#) pour les fonctions essentielles du site web, tout en fournissant des options de reprise après sinistre si nécessaire.

Pour les clientes et clients bénéficiant d'un hébergement web, OVHcloud surveille le réseau pour détecter les tentatives de piratage, comme un nombre anormal de requêtes sur le serveur, et émet une alerte afin que vous puissiez prendre des mesures immédiates pour résoudre le problème.

² [Pingdom, Average Cost of Downtime Per Industry](#)



L'hébergement web OVHcloud inclut également des sauvegardes automatiques pour préserver l'intégrité des données et favoriser une récupération rapide (ex. en cas de mauvaise gestion d'un site web), ce qui permet à votre entreprise de minimiser les temps d'arrêt et de conserver une réputation positive. Nous suggérons également aux clientes et clients d'effectuer une stratégie de sauvegarde « 3, 2, 1 » :

► 3

créez **trois** copies de vos données (c.-à-d. l'original et deux copies de sauvegarde) ;

► 2

stockez-les sur **deux** supports différents (ex. disque sur un site distant, stockage cloud, etc.).

► 1

conservez **une** copie hors ligne sur une solution de stockage déconnectée du reste du réseau ou sur un support de stockage amovible. removable storage medium.

Travailler avec plusieurs fournisseurs pour acquérir la technologie nécessaire au respect de ces meilleures pratiques peut s'avérer coûteux et difficile à gérer. OVHcloud, quant à lui, est un partenaire de site web unique et économique qui fournit des outils contribuant à préserver votre domaine et votre réputation.

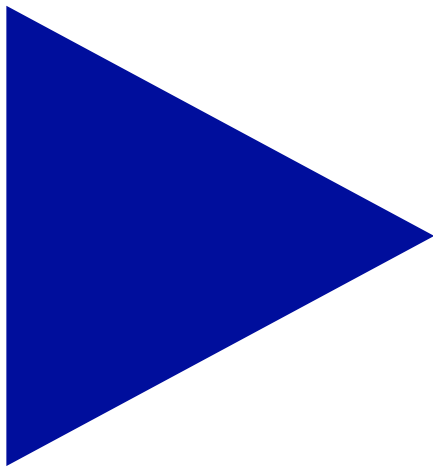
02

**Renforcez
la stabilité
financière
pour résister
aux marchés
fluctuants**



L'ARGENT EST ROI

La trésorerie est devenue un atout clé pour chaque entreprise, quelle que soit sa taille. Mais les PME, en particulier, se remettent encore des effets financiers dévastateurs de la pandémie. Cela signifie qu'elles ont souvent des flux de trésorerie limités et très peu de tolérance aux coûts imprévus.



« Ne perdez jamais de vue les flux de trésorerie, car ils sont essentiels aux affaires. » – Sir Richard Branson

Il est important d'assurer la stabilité et la prédictibilité de votre situation de trésorerie. Cependant, il est bon de garder à l'esprit que bon nombre des produits et services que vous envisagez d'utiliser pour renforcer votre présence en ligne s'accompagnent de frais supplémentaires, de frais de renouvellement, ainsi que d'autres coûts cachés. Toutes ces dépenses peuvent également vous enfermer dans une situation de vendor lock-in (ou enfermement propriétaire).

Par exemple, certaines solutions d'hébergement web semblent initialement attrayantes, car intuitives (en raison d'une personnalisation limitée). Cependant, ces solutions au premier abord peu coûteuses peuvent devenir prohibitives dans le cas où vous changeriez de fournisseur. Vous devrez en effet tout recommencer à zéro.

Voici trois étapes à suivre pour limiter les risques financiers lors du lancement et de la maintenance du site web de votre entreprise.

INTÉGREZ L'INFRASTRUCTURE NUMÉRIQUE DANS VOTRE PLANIFICATION FINANCIÈRE

Une chose est sûre, l'expansion en ligne devrait stimuler la rentabilité de votre entreprise et non l'entraver. Si vous investissez pour la première fois dans une ou plusieurs de ces ressources numériques, il est essentiel que vous planifiiez et que vous posiez les bonnes questions pour contrôler les coûts, éviter la pression financière et favoriser l'évolutivité à long terme

Les principales étapes à prendre en compte dans la planification financière de votre infrastructure en ligne sont les suivantes :

évaluer les dépenses courantes.

Examinez vos coûts numériques (ex. licences logicielles, outils de médias sociaux, services de courriel, etc.) et confirmez que chaque dépense génère de la valeur en matière de revenus, d'économie de temps, d'équité de marque ou de satisfaction de la clientèle.

élaborer un budget pour les services supplémentaires.

Votre site web s'accompagnant naturellement d'exigences en matière d'hébergement et de sécurité, veillez à réserver une section de votre budget mensuel/annuel à allouer à ces services ;

définir les besoins en matière d'hébergement.

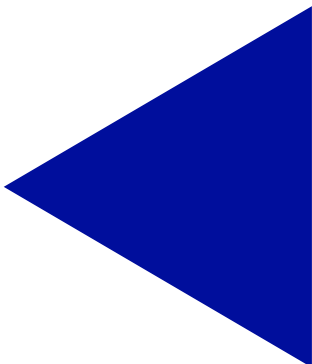
Comparez les fournisseurs d'hébergement sur la base de facteurs tels que la tarification, les fonctionnalités, le support client et le temps de disponibilité optimal, en accordant la priorité à ceux qui ont une [tarification transparente et des coûts sans surprise](#) ;

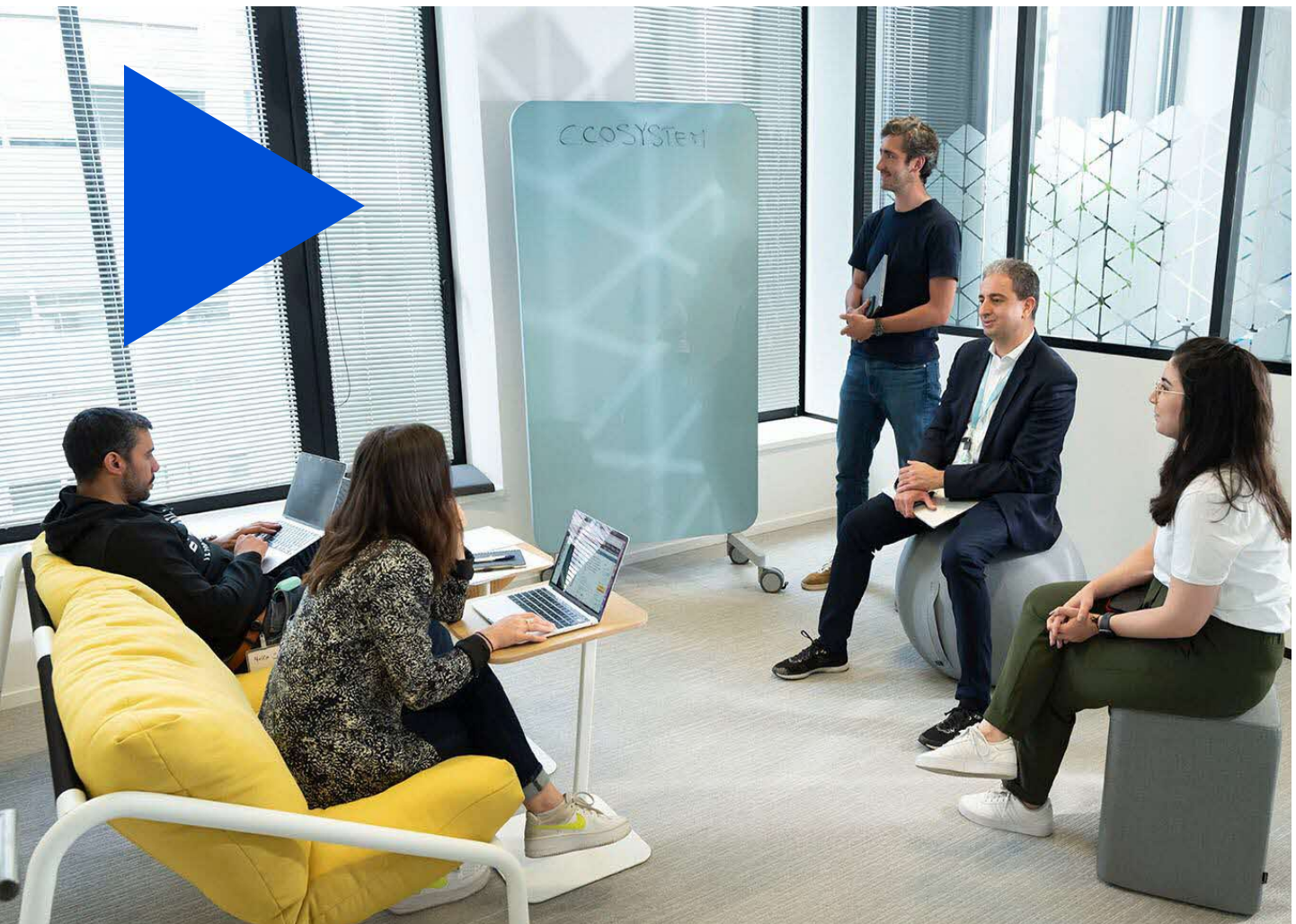
éviter le vendor lock-in.

Certaines entreprises rendent très difficile le changement de fournisseur et d'infrastructure sans coûts extrêmement élevés. Pour éviter cela, renseignez-vous sur la réversibilité des offres proposées par le fournisseur ainsi que les mesures mises en place pour empêcher le vendor lock-in ;

envisager l'évolutivité.

Optez pour un fournisseur offrant une évolutivité verticale (ex. [mises à niveau d'hébergement](#)) et horizontale (ex. [services supplémentaires](#)) afin que votre plan d'hébergement puisse évoluer en fonction des besoins de votre entreprise.



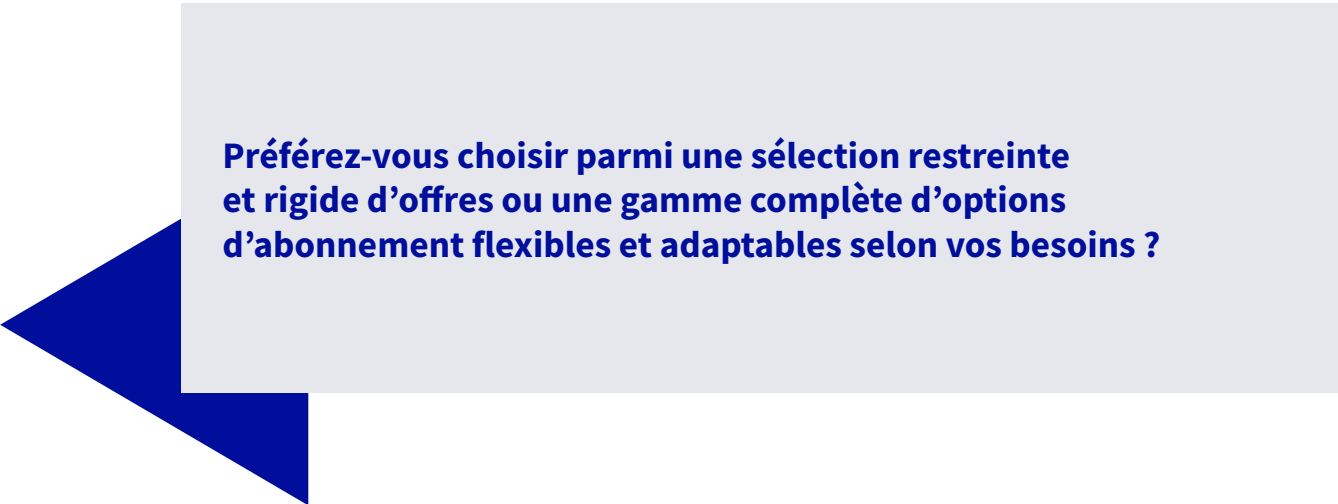


OVHcloud a pour objectif de rendre votre planification financière aussi facile que possible grâce à la transparence des prix. Nous proposons également des serveurs privés virtuels (VPS) et des serveurs dédiés. Ces derniers constituent une solution idéale si vous souhaitez bénéficier d'un contrôle accru de vos serveurs pour créer des applications web, des sites internet plus complexes et des infrastructures numériques.

Besoin d'aide pour votre planification financière ? L'OVHcloud Marketplace dispose d'une gamme d'applications, comme iPaidThat, pour vous aider à gérer la comptabilité et les opérations de trésorerie de votre entreprise.

CHOISISSEZ UN HÉBERGEUR AVEC DES ABONNEMENTS GRANULAIRES

Il est important de vous associer à un fournisseur d'hébergement web qui vous permet d'ajuster un abonnement incluant uniquement les fonctionnalités et les avantages qui vous seront précieux. Vous ne souhaitez payer que les fonctionnalités et services que vous utiliserez, avec la possibilité de modifier votre abonnement en fonction de l'évolution de vos besoins professionnels.



Préférez-vous choisir parmi une sélection restreinte et rigide d'offres ou une gamme complète d'options d'abonnement flexibles et adaptables selon vos besoins ?

OVHcloud propose des options d'abonnement, ce qui signifie que vous bénéficiez du prix idéal pour les fonctionnalités requises pour votre site web. Nous avons toujours pour objectif d'offrir le rapport performance-prix optimal pour tous nos services.

Avec OVHcloud, les coûts sont prédictibles, permettant une planification financière et des prévisions en toute sérénité. Nous savons que la politique de la « taille unique » n'est pas ce que vous cherchez. C'est pourquoi nous élaborons des plans tarifaires granulaires afin de proposer ce dont vous avez réellement besoin à chaque étape de votre projet.

Optez pour des outils de sécurité faciles à utiliser

La sécurité des PME est un aspect souvent négligé de la stabilité financière. Un hébergement web solide vise à protéger les données sensibles, à maintenir la confiance de la clientèle et à atténuer les pertes financières qui peuvent résulter d'une violation ou d'une activité frauduleuse. Il s'agit d'une menace croissante dans le paysage numérique actuel. Une étude mondiale de Mastercard³ indique que les entreprises européennes sont confrontées à un risque élevé de fraude.

Deux revendeurs en ligne sur trois en Allemagne ont remarqué une augmentation de la fraude en ligne.³

Si vous gérez ou traitez des informations financières, nous vous conseillons d'utiliser des outils et des plugins fiables et à jour (ex. PayPal, Stripe, etc.) qui peuvent facilement s'intégrer à votre système de gestion de contenu (CMS). Les CMS et les sociétés de traitement des paiements mettent fréquemment à jour leurs logiciels en fonction de l'évolution des menaces. Il est donc important de mettre à jour vos outils et vos plugins régulièrement.

Avec OVHcloud, vous avez l'assurance que l'infrastructure d'hébergement de votre site web bénéficie d'une protection optimale. Et ce, afin que vous puissiez vous concentrer sur l'identification des données critiques ou sensibles et sur le développement d'un plan pour protéger ces informations.

³ [Mastercard, Ecommerce Fraud Trends and Statistics Merchants Need To Know in 2023](#)

03

Lutte contre les cybermenaces



Prenez en main votre sécurité

Les cybercriminels ne choisissent pas toujours leurs cibles en fonction de la taille ou du type d'entreprise. Ils peuvent également rechercher des ouvertures faciles à exploiter, comme un CMS obsolète ou une faible politique de sécurité. En plus du vol de données, les acteurs malveillants peuvent utiliser une faille pour manipuler vos services et votre marque ou pour usurper l'identité de votre entreprise afin de l'aider à mener de futures attaques.

Prendre des mesures pour atténuer les risques s'avère désormais une exigence primordiale dans le monde de l'entreprise. Mais de nombreuses organisations ne se sentent pas prêtes à faire face aux cybermenaces actuelles. Dans une enquête menée auprès des petites et moyennes entreprises de l'UE, 90 %⁴ ont déclaré que les problèmes de cybersécurité auraient un impact négatif grave dans la semaine suivant un incident.

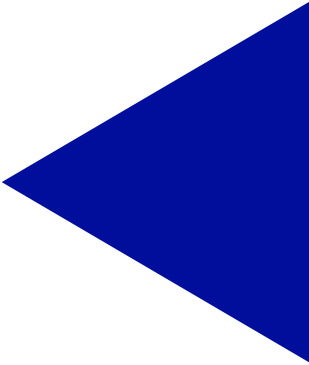
Plus de la moitié (57 %) des PME estiment qu'elles feraient probablement faillite ou fermentaient leurs portes après un incident de cybersécurité.⁴



Bien que la cybersécurité puisse sembler intimidante, il existe de nombreuses mesures simples mais efficaces que vous pouvez mettre en œuvre pour réduire considérablement les risques. Voici trois étapes à suivre pour améliorer la sécurité et la résilience de votre entreprise.

⁴ [Agence européenne pour la cybersécurité, rapport sur la cybersécurité des PME](#)

RESPECTEZ LES BONNES PRATIQUES EN MATIÈRE DE CYBERSÉCURITÉ



Les cybercriminels utilisent souvent des outils automatisés pour analyser des milliers, voire des millions d'entités commerciales afin d'identifier les vecteurs d'attaque à exploiter. Il est dans leur intérêt de trouver quelque chose dont ils peuvent rapidement tirer parti avec un minimum d'effort. Les recherches⁵ montrent que les vecteurs les plus courants comprennent les vols d'informations d'identification (ex. noms d'utilisateur, mots de passe), le phishing (envoi d'e-mails frauduleux en votre nom) et l'exploitation de vulnérabilités (ex. bug ou faille dans un système).

Il est essentiel que vous et vos équipes preniez toutes les précautions nécessaires pour atténuer le risque que ces attaques nuisent à votre entreprise. Selon un rapport du Forum⁶ économique mondial, 95 % de tous les problèmes de cybersécurité sont les conséquences d'erreurs humaines. Heureusement, vous n'avez pas besoin de partir de zéro pour réduire les cybermenaces. Il existe en effet des pratiques d'excellence éprouvées que vous pouvez utiliser pour protéger votre entreprise. Cela inclut :

la mise en œuvre de stratégies de mot de passe fort.

Appliquez l'utilisation de mots de passe complexes [et l'authentification multifacteur](#) pour bloquer les tentatives de bas niveau de contournement de la sécurité ;

d'effectuer régulièrement des mises à jour et des correctifs.

Maintenez tous les logiciels, y compris les systèmes d'exploitation, les applications et les plugins, à jour et corrigez les vulnérabilités connues ;

de chiffrer les données. Utilisez des protocoles de chiffrement pour sécuriser les données en transit et chiffrer les informations sensibles stockées sur les serveurs et dans les bases de données ;

d'installer des pare-feux. Mettez en œuvre des pare-feux pour surveiller et filtrer le trafic réseau, empêchant ainsi les accès non autorisés et détectant les activités suspectes ;

d'effectuer régulièrement des sauvegardes des données.

Sauvegardez les données critiques, en confirmant que les informations sont stockées en sécurité et peuvent être restaurées en cas d'incident informatique

;

de comprendre vos responsabilités. Reconnaissez l'importance du partage des responsabilités et du [devoir qui vous incombe](#) (ex. effectuer des mises à jour logicielles régulières) avec les outils qui vous sont fournis.

⁵ [Verizon, 2023 Data Breach Investigations Report](#)

⁶ [World Economic Forum, Global Risks Report 2022](#)



Il n'existe pas de solution parfaite et universelle pour une sécurité complète : une défense à plusieurs niveaux constitue la seule option viable.

Chez OVHcloud, nous proposons des solutions de sécurité packagées pour votre transition numérique. Par exemple, tous nos services de domaine incluent le [DNSSEC](#) pour la sécurité de votre nom de domaine. Nos services d'hébergement web incluent également des [certificats SSL](#) pour le chiffrement des données.

Privilégiez la sécurité face aux attaques DDoS, une cybermenace croissante

Les attaques par déni de service distribué (DDoS) sont une tactique malveillante de plus en plus fréquente, visant à bloquer l'accès à un site web. La barrière à l'entrée ici est très faible : presque n'importe qui peut mener une attaque DDoS avec un ensemble d'outils automatisés bon marché.

Ces attaques sont uniques dans la mesure où elles n'impliquent généralement pas de violation de la sécurité ou de vol de données. Le but est simplement de rendre votre site indisponible. Les auteurs de ces actes peuvent être des criminels qui tentent de demander une rançon pour rétablir des services, des concurrents malveillants qui veulent ternir votre réputation ou tout simplement des vandales numériques qui cherchent uniquement à causer des problèmes.

Les attaques DDoS sont en hausse de 200 % d'une année à l'autre.⁷

C'est pourquoi il est important de vous assurer que la prévention DDoS est bien comprise dans votre site afin de vous prémunir contre cette menace aujourd'hui très répandue. Bien que cela puisse être difficile à réaliser par vous-même, la bonne nouvelle est que les services d'hébergement OVHcloud sont livrés avec des mécanismes de sécurité, y compris un [Anti-DDoS](#). Parmi ceux-ci, on peut citer :

- une détection permanente des attaques et une mitigation rapide du trafic malveillant ;
- une utilisation illimitée, sans coûts supplémentaires, quel que soit le volume de l'attaque ;
- une protection qui dure toute la durée d'une attaque DDoS.

Notre technologie Anti-DDoS fonctionne de manière transparente en arrière-plan de votre site web. Quel que soit le nombre de fois où des hackers tentent de submerger vos serveurs, OVHcloud s'efforce de dévier les tentatives afin de minimiser votre perception de tout type de perturbation.

⁷ [Zayo Group, The Truth and Trends of DDoS Attacks](#)

Améliorez la sécurité de votre messagerie

La compromission des e-mails commerciaux (BEC) est un type d'attaque très courant qui consiste en l'envoi d'e-mails frauduleux, imitant souvent ceux d'une entreprise, pour voler des informations sensibles. En cas de succès, ces attaques peuvent être difficiles à détecter, car elles ne déclenchent souvent pas d'alerte de sécurité. Le fraudeur peut avoir accès à des renseignements ou à des systèmes essentiels pendant des mois.

L'identification et le confinement d'une violation de données résultant d'une compromission des e-mails professionnels prennent en moyenne **266 jours**.⁸

OVHcloud propose une authentification robuste, des mécanismes antispam, des protocoles [SPF](#), [DKIM](#) et [DMARC](#) installés automatiquement, qui réduisent considérablement votre risque d'incident lié aux e-mails. Ces méthodes d'authentification protègent votre entreprise contre les e-mails indésirables et les spams, empêchant ainsi la modification des données comme l'usurpation d'adresse e-mail (falsification de l'adresse expéditeur). Alors que de nombreux fournisseurs obligent leur clientèle à mettre en place ces fonctionnalités elle-même, nous configurons ces mesures de sécurité pour une efficacité optimale.

Lorsque vous choisissez OVHcloud pour vos [services de messagerie](#), vous bénéficiez également d'une résilience optimale, nos solutions fonctionnant dans trois datacenters différents. Cela signifie que vos services de communication continueront à fonctionner sans problème, même en cas de panne ou d'interruption de service sur l'un des sites.

⁸ [IBM Cost of a Data Breach Report](#)



BÂTISSEZ UN AVENIR SÛR POUR VOTRE ENTREPRISE

Votre marque, votre réputation, votre situation financière et votre sécurité sont étroitement liées. Veillez donc à ne pas omettre ou ignorer l'une des étapes ci-dessus afin de ne pas mettre en péril l'intégrité de l'ensemble de l'entreprise.

Heureusement, prendre les mesures nécessaires pour protéger votre entreprise est moins stressant et plus facile à gérer que jamais. Au lieu d'étudier et d'investir dans de nombreuses solutions ponctuelles et coûteuses, vous pouvez vous associer à OVHcloud : un point de contact unique et abordable pour vos besoins numériques.

[En savoir plus sur nos solutions d'hébergement web et de noms de domaine](#) : découvrez comment nous pouvons accompagner le succès de votre stratégie numérique

