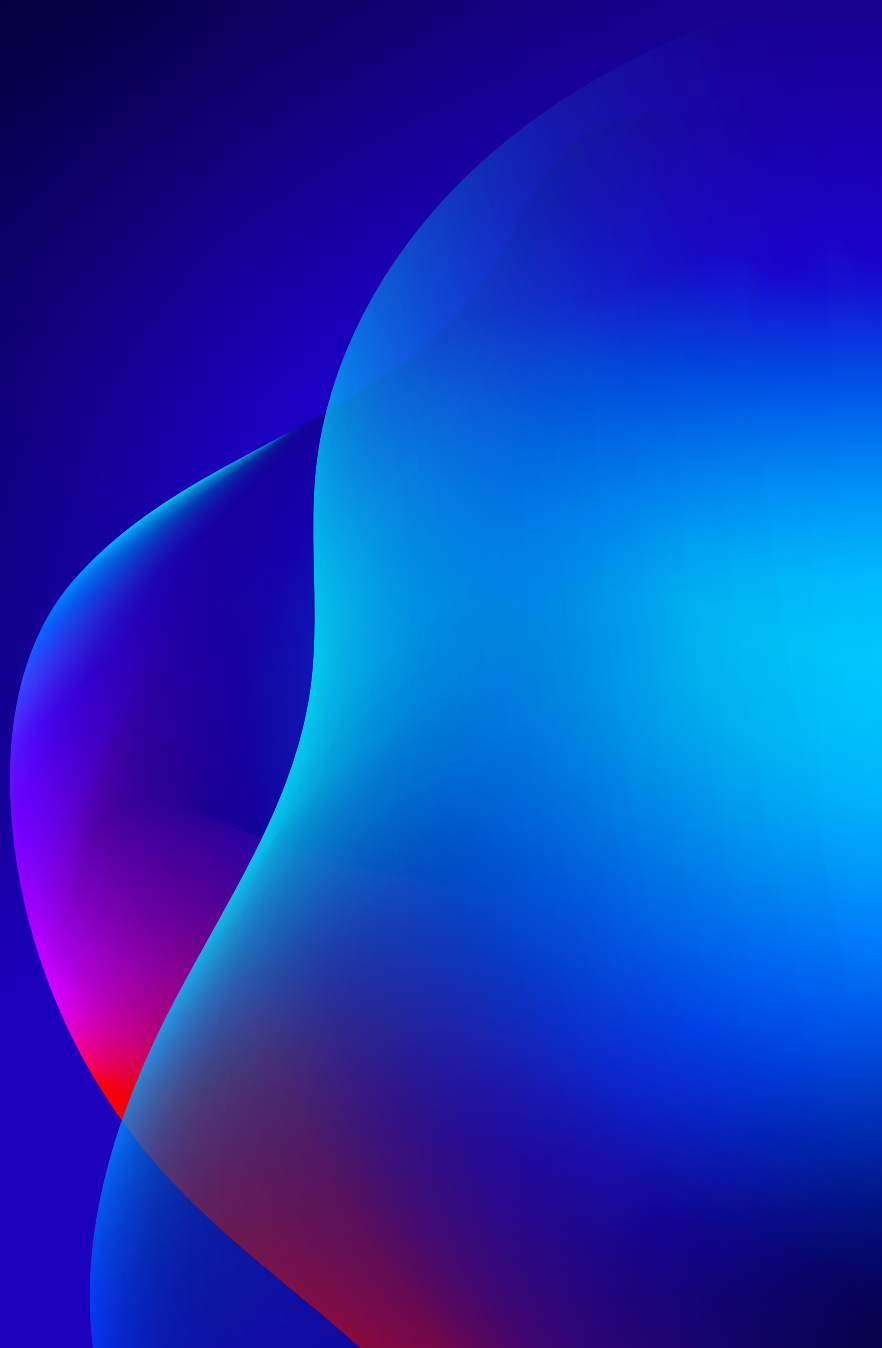


# 6 bonnes pratiques pour **renforcer la sécurité** **de votre site Web**



# Introduction

En 2024, le coût moyen d'une violation de données s'élevait à 4,88 millions de dollars, en raison des pertes commerciales, des réparations et des frais juridiques, soit une augmentation de 10 % par rapport à 2023.<sup>1</sup> Et comme la fréquence et la sophistication des cyberattaques continuent d'augmenter, il devient impératif pour les entreprises de sécuriser efficacement leurs sites Web afin de protéger leurs données et d'assurer la continuité de leurs activités.

Que vous soyez une ville affichant des informations à vos administrés, une banque accordant des prêts à vos clients ou un fabricant vendant des pièces détachées, la sécurité doit être au cœur de toute stratégie Web. Mais comment vous assurer que vos sites Web sont sécurisés et offrent une protection adéquate à votre entreprise et à vos utilisateurs ?

Outre les mesures de base, telles que le chiffrement du trafic Web, vous devez mettre en œuvre les six meilleures pratiques suivantes pour renforcer la sécurité de vos sites Web :

1. Empêcher les utilisateurs indésirables d'accéder à vos sites
2. Appliquer des autorisations basées sur les rôles
3. Se protéger contre les cyberattaques
4. Gérer efficacement les vulnérabilités
5. Mettre en œuvre une stratégie de reprise après sinistre
6. Mettre en place une équipe SOC (Security Operations Center) dédiée

## 1. Empêcher les utilisateurs indésirables d'accéder à vos site

Votre site Web permet à de nombreuses personnes de découvrir votre entreprise, de s'informer sur vos activités et d'acheter vos produits ou services. Mais tout le monde n'est pas bien intentionné. Vous devez gérer avec soin les personnes qui ont accès à votre site Web afin d'empêcher les personnes malveillantes de voler des données privées, de mettre votre site hors service ou même de le prendre en otage.

---

<sup>1</sup> Rapport sur le coût des violations de données 2024 | IBM

Une bonne pratique consiste à vous assurer que votre site Web peut appliquer plusieurs méthodes permettant aux éditeurs de prouver leur identité lorsqu'ils se connectent. Cela comprend :

- **L'authentification multifactorielle**, qui renforce la combinaison nom d'utilisateur/mot de passe par un facteur supplémentaire. Les facteurs courants incluent l'OTP par défaut, l'adresse IP configurée ou les appareils compatibles FIDO2.
- **L'authentification fédérée**, qui permet aux utilisateurs d'accéder à plusieurs services à l'aide d'un seul ensemble d'identifiants de connexion. Rationalisez la connexion grâce à l'Authentification Unique (SSO) en échangeant des données en toute sécurité avec des fournisseurs autorisés.

En outre, réfléchissez aux couches de sécurité dont votre site Web a besoin pour se protéger. Voici quelques couches de sécurité à ajouter :

- **Une couche d'autorisation IP** pour garantir que l'adresse IP à partir de laquelle une demande d'appel de service Web est émise figure sur la liste blanche. Toute tentative d'appel de service Web provenant d'une adresse IP non répertoriée dans la liste blanche échouera automatiquement.
- **Une couche de vérification d'authentification** pour valider les identifiants fournis qui prennent en charge différentes technologies d'autorisation.
- **Une couche de politique d'accès aux services** pour mettre sur liste blanche les points de terminaison des services Web accessibles aux clients distants. Cette couche permet aux services publics de ne pas exiger d'authentification et de restreindre les points de terminaison accessibles aux clients en s'appuyant sur le mot de passe de l'utilisateur, OAuth 2.0 et d'autres informations d'identification prises en charge.
- **Une couche d'autorisation utilisateur** pour effectuer des contrôles d'autorisation des données. Cette couche permet de s'assurer que l'utilisateur qui effectue une action dispose des autorisations appropriées pour manipuler les entités et les données correspondantes.

Ensemble, ces couches de protection permettent de renforcer les défenses de sécurité afin d'empêcher les acteurs malveillants d'accéder à votre site et de le mettre hors service.

## 2. Appliquer des autorisations asées sur les rôles

Bien que l'authentification empêche les utilisateurs indésirables d'accéder à votre site, il est tout aussi important de gérer ce à quoi les utilisateurs légitimes peuvent accéder après s'être connectés afin d'éviter les erreurs humaines et les fuites de données

potentielles. Ce n'est pas parce que l'identité d'un utilisateur a été vérifiée qu'il doit avoir le contrôle sur tout ce qui se trouve sur votre site.

Votre site Web doit disposer de rôles et d'autorisations afin de personnaliser davantage l'accès aux services, aux données et au contenu. En attribuant des rôles et des autorisations spécifiques, vous pouvez vous assurer que les utilisateurs n'ont accès qu'aux informations qui les concernent, ce qui les empêche d'accéder accidentellement à des données sensibles ou de supprimer des données.

Évaluez le niveau de granularité des rôles et des autorisations sur votre site Web et leur portée. Bien que de nombreux créateurs de sites Web incluent des rôles « invité » ou « éditeur » de base, ceux-ci peuvent ne pas être suffisants pour répondre aux besoins spécifiques de votre entreprise, car ils offrent un accès très limité ou complet, sans aucune flexibilité pour répondre à des besoins plus complexes.

Par exemple, un fabricant travaillant avec un réseau de revendeurs peut attribuer à chaque revendeur un rôle spécial « revendeur ». Cela permet à chaque revendeur de gérer sa propre page sur le site Web du fabricant, en précisant son emplacement, ses offres de produits et ses prix, sans pouvoir accéder aux informations des autres revendeurs.

### 3. Se protéger contre les cyberattaques

Selon Microsoft, plus de 600 millions de cyberattaques sont perpétrées chaque jour dans le monde, et ce phénomène ne semble pas près de ralentir.<sup>2</sup> Il est donc extrêmement important que les entreprises soient en mesure de protéger leurs sites Web contre les cyberattaques courantes, notamment :

- **Les attaques DDoS.** Une attaque par déni de service distribué (DDoS) est une tentative malveillante visant à saturer l'infrastructure de la cible avec un flux de trafic. Les tensions géopolitiques accrues ont entraîné une augmentation du volume et de la durée des attaques DDoS. Chaque attaque peut coûter en moyenne 6 000 dollars par minute d'indisponibilité du site aux entreprises.<sup>3</sup> Recherchez des moyens de vous protéger contre ces attaques, par exemple en tirant parti d'une protection DDoS basée sur l'IA/ML pour identifier les modèles de trafic et bloquer le trafic excessif avant qu'il ne mette votre site Web hors service. D'autres fonctionnalités permettent également de prévenir ces attaques, notamment la limitation du débit, la liste blanche et les informations sur les menaces pour bloquer les adresses IP des attaquants connus.

<sup>2</sup> Rapport Microsoft Digital Defense : 600 millions de cyberattaques par jour dans le monde | Centre d'actualités multi-pays CEE

<sup>3</sup> Selon les dernières données de Zayo, le coût moyen d'une attaque DDoS s'élèvera à près d'un demi-million de dollars pour les entreprises en 2023

- **Malware.** Un malware, ou logiciel malveillant, est un programme ou un code créé dans le but de nuire. Les malwares, qui constituent l'une des formes les plus courantes de cyberattaques, comprennent les ransomwares, les logiciels espions, les bots, le cryptojacking, etc. Pour protéger votre site Web contre les malwares, veillez à ce que vos systèmes soient à jour afin que les pirates ne puissent pas exploiter les failles de sécurité. En outre, vous pouvez mettre en place un pare-feu pour applications Web (WAF) afin d'empêcher les attaquants d'accéder à votre site. Un WAF peut évaluer le trafic en fonction de sa provenance, de son comportement et des informations qu'il demande. Grâce à ces informations, un WAF peut déterminer quel trafic est « légitime » et bloquer le trafic « malveillant ». Enfin, analysez régulièrement votre site Web à la recherche de logiciels malveillants ou d'autres codes nuisibles.
- **Attaques par injection de code.** Ces attaques consistent pour un pirate à injecter un code malveillant qui lui permet d'exécuter des commandes non autorisées, d'accéder à des données sensibles ou de manipuler le fonctionnement du système. Parmi les exemples d'attaques par injection de code, on peut citer l'injection SQL, l'injection de commande, les attaques XSS ou l'injection XML. Les principales stratégies de défense contre ce type d'attaques consistent à nettoyer régulièrement les entrées de code et à adopter des normes de codage sécurisées.

## 4. Gérer efficacement les vulnérabilités

Le moyen le plus simple pour les cybercriminels d'attaquer vos sites Web est d'exploiter les faiblesses des logiciels et des outils obsolètes ou vulnérables que vous utilisez pour créer, exploiter et maintenir vos sites Web.

La première stratégie, qui est aussi la plus importante, consiste à mettre à jour régulièrement vos logiciels et vos plug-ins afin de vous assurer qu'ils disposent des derniers correctifs et patches de sécurité.

Mais comment améliorer la gestion des vulnérabilités afin de prévenir les menaces de cybersécurité ? Recherchez des outils capables de :

- **Analyser et signaler régulièrement les vulnérabilités connues** dans votre code et vos outils. Il existe de nombreux outils d'analyse des vulnérabilités qui peuvent vous aider à identifier les faiblesses de votre infrastructure, les technologies obsolètes ou les terminaux exposés.
- **Assurer une surveillance en temps réel** du trafic et des performances de votre site Web, y compris la surveillance des journaux afin d'examiner les journaux du serveur à la recherche d'activités inhabituelles ou d'autres modèles suspects.

- **Effectuer des tests d'intrusion**, ou pentesting, pour imiter des attaques réelles et identifier les vulnérabilités potentielles. Les outils et services de pentesting utilisent soit des scanners de vulnérabilité, soit des tests pour analyser les réseaux et les systèmes afin de détecter toute faille logicielle. Les vulnérabilités identifiées sont ensuite exploitées pour obtenir un accès non autorisé aux systèmes ou aux données afin de mieux comprendre l'impact d'une attaque spécifique. Vous pouvez ensuite consulter un rapport de test détaillé et complet qui décrit les vulnérabilités découvertes et fournit des recommandations.

En adoptant une approche proactive pour surveiller et traiter les risques de sécurité, vous pouvez identifier les points faibles avant qu'ils ne deviennent des opportunités pour les pirates informatiques ou les utilisateurs malavisés de compromettre vos sites Web.

## 5. Mettre en œuvre une stratégie de reprise après sinistre

Bien que les meilleures pratiques précédentes devraient vous aider à empêcher votre site Web d'être mis hors service par un pirate informatique, que devez-vous faire si une attaque se produit ?

Il est important de mettre en place une stratégie de reprise après sinistre afin de minimiser les temps d'arrêt et de remettre votre site Web en service dès que possible. Plus votre site est indisponible longtemps, plus vous avez à perdre : les données sont compromises, la confiance est rompue et les ventes chutent. Cela vaut également au-delà des pirates informatiques et des cyberattaques ; par exemple, une catastrophe naturelle peut mettre votre serveur hors service, rendant votre site Web indisponible.

Pour éviter les interruptions et restaurer votre site Web le plus rapidement possible, élaborer une stratégie de reprise solide qui comprend :

- **Des sauvegardes régulières.** La sauvegarde régulière de votre site Web vous garantit de disposer d'une version récente de votre site Web qui peut être restaurée en cas de sinistre. Sauvegardez régulièrement votre site Web à plusieurs emplacements, dans le Cloud et dans un emplacement On-premise sécurisé.
- **Un plan d'intervention en cas d'incident.** Si une attaque se produit, votre équipe doit déjà avoir défini les étapes à suivre pour remettre votre site en état de fonctionnement. Ce plan doit définir votre équipe d'intervention en cas d'incident et les responsabilités de chaque membre de l'équipe. En cas d'attaque, ces membres doivent être formés et préparés à contenir l'attaque, à identifier la cause et à éliminer la menace, qu'il s'agisse de supprimer un code malveillant, de bloquer des robots ou de corriger des failles de sécurité.

## Seul 1 professionnel de l'informatique sur 4

respecte la règle 3-2-1 : trois copies des données, deux types de supports, une copie hors site et cryptée.<sup>4</sup>

## 6. Mettre en place une équipe SOC dédiée

Si les meilleures pratiques mentionnées ci-dessus constituent les boucliers et les armes utilisés pour protéger vos sites Web, alors une équipe SOC (Security Operations Center) est le super-héros qui manie ces outils.

Une équipe SOC peut être une équipe interne ou externe composée de professionnels de la sécurité informatique qui se consacrent à la détection, à l'analyse et à la réponse aux incidents de sécurité en temps réel. Les équipes SOC sélectionnent, exploitent et maintiennent également les technologies de cybersécurité de l'organisation et analysent en permanence les données relatives aux menaces afin de trouver des moyens d'améliorer la posture de sécurité.

Quelques éléments à prendre en compte lors de la constitution de votre équipe SOC :

- **Recherchez des experts.** Bien qu'il existe de nombreux outils et solutions pour renforcer votre équipe, ce sont les experts qui font la force de l'équipe. Réfléchissez donc aux types de personnel de sécurité, tels que des ingénieurs, des analystes ou des architectes, dont vous avez besoin pour constituer une équipe SOC solide
- **Renforcez vos équipes grâce à l'automatisation et au Machine Learning.** Tirez parti d'outils tels que l'automatisation et l'apprentissage automatique pour renforcer et compléter votre équipe SOC. De plus, l'IA avancée peut aider à traiter rapidement d'énormes quantités de données afin de détecter tout comportement suspect.
- **Sensibilisez l'ensemble de l'organisation.** L'équipe SOC sera votre première ligne de défense, mais la sécurité est renforcée lorsque tous les membres de votre organisation sont sensibilisés et formés aux principes de base de la cybersécurité, notamment à la manière d'identifier les tentatives d'hameçonnage ou d'autres attaques, aux meilleures pratiques générales en matière de sécurité et aux politiques générales de sécurité de l'organisation.

En effet, 68 % des violations de sécurité sont le résultat d'une erreur humaine.<sup>5</sup>

<sup>4</sup> Apricorn constate que 75 % des organisations exposent inutilement leurs données à des risques en raison de pratiques de protection incohérentes et de politiques de sauvegarde négligentes

<sup>5</sup> Rapport 2024 sur les enquêtes relatives aux violations de données | Verizon

Cependant, grâce à une meilleure formation et à une meilleure éducation, ce chiffre pourrait être considérablement réduit et permettre à l'ensemble de l'organisation de s'unir pour protéger vos sites Web.

## Renforcer la sécurité de votre site Web

Bien que nous ayons inclus ces meilleures pratiques à suivre, la sécurité des sites Web est un combat en constante évolution. À mesure que les attaques deviennent plus sophistiquées, ces tactiques devront évoluer en conséquence afin de rester à la pointe.

Cela peut sembler un défi pour votre équipe, surtout si vous ne disposez pas d'une équipe SOC dédiée ou des ressources nécessaires pour investir dans la sécurité. Mais pensez à tirer parti d'une plateforme sécurisée avec des fonctionnalités de sécurité intégrées pour créer vos sites Web, comme une Plateforme d'Expérience Digitale (DXP).

Une DXP est une plateforme complète et intégrée qui combine des capacités de création d'expériences digitales et une architecture extensible, le tout sur une base hautement sécurisée. Non seulement les DXP les plus puissantes sont sécurisées, mais elles offrent également de nombreuses fonctionnalités de sécurité pour aider à protéger les sites Web qui les utilisent.

**Comment une DXP peut-elle vous aider à créer des sites Web sécurisés ? En :**

### A. Protégeant vos utilisateurs et vos données

La protection de vos utilisateurs et de leurs données commence par le choix de la plateforme sur laquelle vous construisez vos sites Web. Les DXP les plus sécurisées doivent disposer des certifications de sécurité pertinentes délivrées par des organismes tiers qui valident la robustesse des contrôles de sécurité, de confidentialité et de conformité du fournisseur. Ces certifications indiquent que cette plateforme constitue une base sécurisée sur laquelle vous pouvez vous appuyer, afin que vous puissiez vous concentrer sur les besoins spécifiques de votre site Web en matière de sécurité et non sur la compensation des vulnérabilités ou des faiblesses de la plateforme.

**Les certifications clés à rechercher sont les suivantes :**

- Sécurité générale : ISO/IEC 27001, SOC 2 (Type 1 et 2)
- Sécurité du Cloud : ISO/IEC 27017, CSA STAR (niveaux 1 et 2)
- Confidentialité des données : ISO/IEC 27018, HIPAA (pour les soins de santé)



Et comme les lois sur la protection des données varient d'une région à l'autre, les DXP doivent offrir des fonctionnalités permettant de se conformer aux réglementations locales. Par exemple, le RGPD exige des entreprises qu'elles garantissent la portabilité des données et le droit à l'oubli. Les DXP conçues dans le respect de la confidentialité des données intègrent ces fonctionnalités.

## B. Protégeant votre site

Les DXPs offrent en natif des fonctionnalités garantissant que seuls les utilisateurs autorisés peuvent accéder à votre site et le modifier. Une fois connectés, ces utilisateurs ne doivent avoir accès qu'aux informations qui les concernent.

### Empêchez les visiteurs indésirables d'accéder aux sites

Recherchez des DXP qui peuvent fournir à la fois une authentification multifactorielle et une authentification fédérée. Les DXP les plus flexibles doivent également être capables de synchroniser et de vérifier les utilisateurs via LDAP, SCIM, SAML 2.0 ou OpenID Connect, fournis par les principaux fournisseurs d'identité tels que MS Active Directory, Google Identity Platform et autres.

En outre, les DXPs les plus sécurisées doivent fournir plusieurs couches de sécurité des services Web afin de protéger davantage vos sites Web.

### Appliquez des autorisations basées sur les rôles

Les DXPs robustes doivent être capables de prendre en compte des rôles et des autorisations plus complexes. Créez des rôles et des autorisations personnalisés pour les niveaux d'accès dont votre organisation a besoin.

## C. Vous protégeant via le Cloud

La plupart des fournisseurs DXP proposent leurs logiciels sous forme d'abonnement PaaS (Platform as a Service) ou SaaS (Software as a Service) et, ce faisant, tirent parti d'une technologie Cloud sophistiquée pour renforcer la sécurité des sites Web. RapidScale affirme que 94 % des entreprises ont constaté une amélioration de leur sécurité après être passées au Cloud, et 91 % ont déclaré que le Cloud leur permettait de se conformer plus facilement aux exigences réglementaires.<sup>6</sup>

6 Conformité dans le Cloud - Récapitulatif du Webinar de juin | RapidScale

En tirant parti des offres SaaS ou PaaS des fournisseurs, vous pouvez bénéficier de fonctionnalités de sécurité spécifiques au Cloud pour :

### **Protégez vous contre les cyberattaques**

Les options d'abonnement SaaS et PaaS peuvent inclure :

- **Des systèmes de détection d'intrusion**, qui permettent une surveillance constante et une identification précoce des failles de sécurité potentielles grâce à l'IA.
- **Une technologie DDoS** améliorée avec WAF et ML pour protéger contre le trafic malveillant connu et inconnu. Mais avec le Cloud, le trafic malveillant ne s'approchera pas du serveur.
- **Une technologie anti-malware** qui stocke les informations sur les logiciels malveillants dans le Cloud afin de vous protéger contre les menaces.

### **Mettez en œuvre une stratégie de reprise après sinistre**

En cas d'attaque, la plupart des options d'abonnement SaaS et PaaS sont en mesure de vous aider à rétablir le fonctionnement de vos sites Web grâce à :

- **Sauvegardes**, effectuées par le fournisseur pour les déploiements SaaS. Les déploiements PaaS offrent des fonctionnalités de sauvegarde contrôlées par le client, planifiées ou automatiques. Pour les deux options, des routines de sauvegarde incrémentielles peuvent être exécutées régulièrement, et les sauvegardes peuvent être répliquées dans différentes régions, chiffrées au repos, puis conservées de manière permanente.
- **Une reprise après sinistre** pour remettre l'ensemble de l'infrastructure en ligne dès que possible.
- **Une disponibilité accrue**. Aujourd'hui, la plupart des fournisseurs de Cloud d'entreprise spécifient dans leurs SLA une disponibilité de 99,5 % ou plus, garantie par plusieurs niveaux de redondance dans des centres de données répartis dans le monde entier. Certains fournisseurs peuvent fournir une mise à l'échelle automatique pour répondre à une demande accrue, par exemple lors d'une campagne marketing saisonnière ou du lancement d'un nouveau produit ou service.

## Gérez efficacement les vulnérabilités

Les fournisseurs de Cloud surveillent et analysent de manière proactive vos solutions afin de détecter toute vulnérabilité grâce à :

- **Surveillance des performances.** Dans le cloud, vous pouvez obtenir une visibilité sur les performances et l'état de votre solution en surveillant son utilisation en temps réel et en recevant des alertes en cas de problème.
- **Des analyses DAST et SAST régulières** effectuées par un fournisseur SaaS pour tester et détecter toute vulnérabilité dans vos solutions.

## Bénéficiez d'une équipe SOC dédiée

Les fournisseurs DXP qui accordent la priorité à la sécurité disposent d'une équipe de sécurité interne qui s'engage à garantir la sécurité de leur plateforme.

De plus, les DXP pouvant être déployées via un modèle SaaS vous permettent de confier une grande partie des tâches de sécurité à une équipe d'experts, ce qui vous offre une tranquillité d'esprit et vous libère du temps et des ressources pour vous consacrer à d'autres tâches stratégiques. Par exemple, le fournisseur peut se charger de la surveillance des performances et des journaux, des analyses de sécurité, des mises à jour de sécurité et des correctifs.

Pour le PaaS, les fournisseurs fournissent les outils et l'accès aux équipes SOC des clients pour qu'elles puissent effectuer leurs propres surveillances, analyses et mises à jour, ou ils peuvent proposer des abonnements supplémentaires pour des services de sécurité plus robustes.

Certaines organisations ont déjà investi massivement dans des infrastructures Cloud ou sur site qui intègrent tout ou partie de ces bonnes pratiques. Dans ce cas, recherchez un fournisseur DXP qui propose une option d'hébergement de son logiciel dans l'infrastructure choisie par le client.

# Intégrer votre approche de la sécurité à une Plateforme d'Expérience Digitale

Parmi les fournisseurs DXP, Liferay DXP est une plateforme fiable qui vous aide à créer des sites Web sécurisés. Depuis plus de deux décennies, Liferay place la sécurité, la conformité et la protection des données au cœur de ses produits, de ses abonnements et de ses opérations. Grâce à notre expertise et à l'importance que nous accordons à la sécurité, nous fournissons des solutions fiables à des secteurs où la sécurité est primordiale, tels que la finance, le gouvernement et la santé.



En plus de sa base sécurisée, Liferay DXP offre également une protection accrue grâce à son partenariat avec Google Cloud pour Liferay PaaS et Liferay SaaS.

Pour en savoir plus sur la manière dont Liferay privilégie la sécurité, rendez-vous sur notre [Trust Center](#).

Mais la sécurité n'est pas le seul facteur à prendre en compte dans une plateforme de création et de conception de sites Web. En fonction des besoins spécifiques de votre entreprise, la création de sites Web efficaces nécessite souvent :



**D'offrir des expériences modernes**



**De garantir une image de marque cohérente**



**De créer et gérer plusieurs sites**



**ID'une agilité accrue pour répondre aux besoins changeants du marché**



**D'ajouter des fonctionnalités commerciales et de self-service à mesure que les besoins de votre entreprise évoluent**



**De se développer grâce à des solutions digitales supplémentaires**

Pour atteindre ces objectifs, vous aurez besoin de multiples fonctionnalités, notamment la gestion multisite, la personnalisation, le Low-Code, etc.



Liferay aide les organisations à construire leur avenir en leur permettant de créer, gérer et développer des solutions puissantes sur la Plateforme d'Expérience Digitale (DXP) la plus flexible au monde. Plus d'un millier d'entreprises dans le monde font confiance à Liferay. La DXP open-source de Liferay aide au développement de sites Web, de Portails clients, d'Intranets, et bien plus encore. Découvrez comment nous utilisons la technologie pour améliorer le monde ensemble sur [liferay.com](https://liferay.com).

© 2025 Liferay, Inc. Tous Droits Réservés.