Akamai

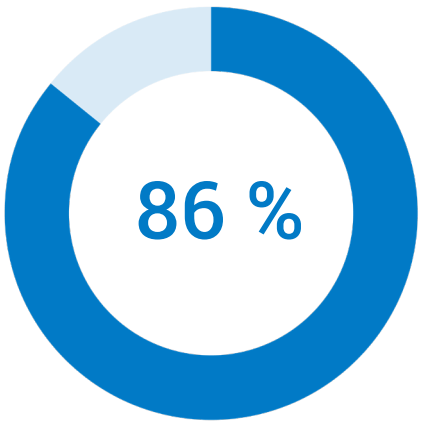
LIVRE BLANC

# 6 thèmes motivant l'investissement informatique dans les sciences de la vie dans la zone EMEA

L'innovation promet d'accélérer la R&D et les essais, mais nécessite de renforcer la cybersécurité et la protection des données

# Synthèse

- Ce livre blanc présente six domaines thématiques clés qui stimulent l'investissement informatique des entreprises du secteur des sciences de la vie en Europe, au Moyen-Orient et en Afrique (EMEA).
- Les avancées dans le domaine du digital offrent des opportunités importantes aux entreprises du secteur des sciences de la vie, mais l'augmentation de la surface de risque digital a coûté cher : 86 % des attaques par déni de service distribué (DDoS) de couche 7 observées sur la plateforme d'Akamai entre le 1er janvier 2023 et le 31 mars 2024 visaient des entreprises pharmaceutiques dans la zone EMEA.
- Les entreprises du secteur des sciences de la vie investissent davantage dans l'informatique, ce qui fait de la transformation digitale une priorité à l'échelle mondiale. Cependant, de nombreuses entreprises tardent à adopter des pratiques pour prévenir les cybermenaces.
- Les 6 thèmes motivant l'investissement informatique dans les sciences de la vie sont les suivants :
  1. Hébergement cloud, Big Data et analytique
  2. Intelligence artificielle et apprentissage automatique
  3. Soins virtuels
  4. Fusions et acquisitions
  5. Blockchain et bases de données distribuées
  6. Cybersécurité : sécurité, conformité et réputation
- Chacun des six thèmes nécessite une mise en œuvre sécurisée, des essais de qualité et des tests d'acceptation des clients, en plus de respecter certaines réglementations afin de promouvoir une protection rigoureuse.




**86 % des attaques DDoS de couche 7 sur la plateforme d'Akamai ont ciblé des entreprises pharmaceutiques de la zone EMEA**

# Gérer les sous-investissements dans un environnement à haut risque

Les investissements informatiques dans les secteurs pharmaceutiques et des sciences de la vie augmentent. En 2024, 72 % des entreprises pharmaceutiques ont renforcé leurs budgets informatiques, augmentant d'environ 58 % les opportunités de revenus pour le secteur des technologies de l'information et des communications dans le domaine des sciences de la vie d'ici 2028. Ces investissements sont motivés par les tendances et les réglementations, notamment la médecine de précision et la législation qui considère les entreprises des sciences de la vie comme des infrastructures critiques. Bien que ces facteurs soient divers, une priorité essentielle les unit : l'importance d'investir dans des mesures préventives en matière de cybersécurité. Selon une étude de KPMG, 75 % des PDG d'entreprises du secteur des sciences de la vie prévoient que la cybercriminalité et l'insécurité informatique auront probablement un impact négatif sur leur organisation au cours des trois prochaines années.

Cependant, malgré cette préoccupation imminente, les besoins en cybersécurité sont souvent négligés ou identifiés trop tard. Les stratégies de transformation digitale qui ne prévoient pas d'investissements dans la cybersécurité entraînent souvent une augmentation des contraintes budgétaires, car les entreprises sont confrontées à des risques accrus et à des cyberattaques coûteuses.

Pour quantifier la menace, les entreprises pharmaceutiques de la zone EMEA ont représenté 86 % des attaques DDoS de couche 7 sur la plateforme d'Akamai entre le 1er janvier 2023 et le 31 mars 2024. Les attaques DDoS, ou d'autres méthodes qui provoquent des interruptions ou des arrêts opérationnels, sont extrêmement coûteuses pour les entreprises pharmaceutiques, car elles peuvent entraîner des retards dans les essais, modifier ou altérer des médicaments et engendrer de surcroît une perte de revenus.

## Les impacts économiques potentiels des cyberattaques

Bien qu'un investissement dans la cybersécurité ne semble pas être une préoccupation immédiate, il peut permettre aux entreprises d'économiser des millions en termes de résolution des cyberincidents, de gestion des interruptions et de restauration de l'image de marque (Tableau 1).

| Conséquences des cyberattaques | Impact économique |
|---|---|
| Arrêts opérationnels | • Perte de revenus<br>• Retards dans les essais/recherches |
| Violations de données | • Atteinte à la réputation de la marque<br>• Perte de confiance des patients et des participants à l'essai<br>• Perte de propriété intellectuelle |
| Ransomwares | • Coûts liés aux rançons<br>• Interruptions opérationnelles |
| Informations dégradées | • Données d'essais cliniques incertaines ou peu fiables, pouvant entraîner des soins inappropriés et retarder l'approbation de l'Agence européenne des médicaments (EMA)<br>• Perte de revenus due à une protection réduite des brevets<br>• Perte de confiance des fournisseurs et des patients quant aux produits commerciaux |
| Reconstruction des systèmes après attaque | • Coûts de reconstruction et perte de revenus en raison des arrêts opérationnels pendant le processus (si nécessaire) |

**Tableau 1 :** Les impacts économiques potentiels des conséquences des cyberattaques

Le meilleur moyen de protéger les populations de patients contre les cyberattaques consiste à prioriser les exigences en matière de cybersécurité et les décisions d'investissement technique.

# Les six thèmes motivant l'investissement informatique dans les sciences de la vie

Vous trouverez ci-dessous les six thèmes qui motivent l'investissement informatique dans les secteurs pharmaceutiques et des sciences de la vie, ainsi que les bonnes pratiques que peuvent suivre les entreprises pharmaceutiques pour optimiser leur protection contre les cyberattaques.

## Thème n° 1

### Hébergement cloud, Big Data et analytique

Le Big Data et l'analytique impliquent le déploiement d'un système de Cloud Computing évolutif avec un puissant logiciel d'analyse pour identifier les modèles de données et extraire des informations exploitables. Cela implique la migration des technologies et de l'infrastructure de base depuis le site vers le cloud, et l'utilisation d'outils et d'algorithmes avancés pour exécuter des modèles afin d'analyser les ensembles de données et d'obtenir des informations utiles.

Les avantages de l'hébergement cloud, du Big Data et de l'analytique pour les entreprises du secteur des sciences de la vie sont les suivants :

- Transformer les dépenses d'investissement importantes en dépenses d'exploitation plus prévisibles et évolutives de manière dynamique en profitant de la tarification basée sur la consommation
- Rapprocher les charges de travail des utilisateurs finaux via des réseaux en bordure de l'Internet distribués, pour améliorer les performances en réduisant la latence et les dépenses liées au cloud
- Accroître la flexibilité avec des infrastructures multicloud et de cloud hybride, ce qui permet aux entreprises de conserver les avantages des configurations existantes tout en bénéficiant de nouvelles fonctionnalités
- Améliorer l'observabilité des journaux grâce à l'utilisation d'outils plus performants et plus économiques qui conservent les données à chaud tout en réduisant les coûts de stockage
- Automatiser et améliorer l'évolutivité du système en utilisant des outils pour provisionner automatiquement les ressources en fonction des pics de trafic
- Raccourcir les cycles d'exploration, pour accélérer la découverte et la distribution de nouveaux médicaments plus efficaces
- Améliorer les capacités de gestion des données, en particulier lors du partage de données avec des tiers et des collaborateurs
- Développer et généraliser la médecine personnalisée (de précision), comme l'étude génomique

## Thème n° 2

### Intelligence artificielle et apprentissage automatique

L'intelligence artificielle (IA) est la capacité générale des ordinateurs à imiter la pensée humaine et à effectuer des tâches dans des environnements réels, tandis que l'apprentissage automatique (ML) fait référence aux technologies et algorithmes qui permettent aux systèmes d'identifier des modèles, de prendre des décisions et de s'améliorer grâce à l'expérience et aux données.

Ces outils permettent aux ordinateurs de développer des capacités de réflexion et de réalisation de tâches autrefois confiées à des agents humains, sans intervention de ces derniers. Cependant, l'IA et le ML dépendent fortement des ensembles de données, souvent sensibles (cliniques, financières) ou propriétaires. À mesure que les entreprises investissent dans des capacités d'IA/ML, elles doivent procéder à un examen de sécurité en parallèle pour garantir une résilience continue. Enfin, ces mises en œuvre nécessitent une bordure de l'Internet sécurisée afin d'empêcher le vol ou l'utilisation abusive de l'investissement.

Les avantages de l'intelligence artificielle et de l'apprentissage automatique pour les entreprises pharmaceutiques sont les suivants :

- Possibilité de simuler les interactions médicamenteuses et d'interventions avec des patients synthétiques, réduisant ainsi les pertes liées à la recherche et au développement
- Amélioration du profilage, de la découverte et de la correspondance des participants, accélérant ainsi le recrutement pour les essais cliniques
- Évaluation de bout en bout des données relatives à la chaîne logistique et à la fabrication, pour établir des performances de base et identifier des opportunités de rationalisation des opérations de fabrication, d'expédition et de livraison
- Des expériences conversationnelles améliorées via des agents IA et des modèles de chat, qui réduisent les coûts administratifs tout en offrant aux patients ou aux participants à l'essai un accès 24 h/24 et 7 j/7

**Les investissements dans l'IA, le cloud et les soins virtuels doivent aller de pair avec des cadres de cybersécurité robustes pour être véritablement porteurs de changement.**

## Thème n° 3

### Soins virtuels

Ce thème inclut les essais cliniques décentralisés conçus pour être exécutés là où les patients se trouvent grâce à l'association de la surveillance à distance des patients et de la télésanté. Il comprend également les accessoires connectés et les dispositifs de surveillance à distance des patients, qui sont des outils portés par les patients qui collectent et transmettent des informations clés. Comme pour d'autres domaines clés d'investissement, la décentralisation des soins s'accompagne de risques potentiels en raison de la visibilité « physique » réduite des patients, des utilisateurs et des émetteurs de données. Les entreprises du secteur des sciences de la vie qui utilisent les soins virtuels et distribués doivent également envisager de mettre en œuvre des éléments Zero Trust, tels que l'authentification multifactorielle, pour sécuriser l'accès à leurs systèmes par des utilisateurs authentifiés et autorisés.

Les avantages des soins virtuels pour les entreprises pharmaceutiques sont les suivants :

- Réduction des coûts de recrutement et de rétention des participants aux essais cliniques et diminution des retards dans les essais cliniques en raison de problèmes de recrutement
- Population de participants aux essais plus diversifiée grâce à un accès plus facile aux essais
- Réduction des coûts de réalisation des essais cliniques grâce à la télésanté
- Davantage de communication en temps réel et de collecte de données auprès des patients utilisant des produits commerciaux, ce qui réduit les délais d'intervention des praticiens. Les patients prennent ainsi le contrôle de leur parcours médical et augmentent l'efficacité potentielle des médicaments

## Thème n° 4

### Fusions et acquisitions

Ce thème concerne les entreprises qui fusionnent ou acquièrent d'autres organisations pour étendre leur présence sur le marché, élargir leur gamme de produits et/ou réaliser des économies d'échelle. Pour une intégration réussie, les entreprises doivent consolider et rapprocher les technologies, les utilisateurs et les processus. Ces efforts sont très vulnérables aux risques et expositions imprévus en raison des empreintes techniques complexes créées après l'acquisition ou la fusion.

Les principaux domaines prioritaires doivent être une visibilité complète grâce à une solution telle que la microsegmentation (pour obtenir une visibilité et une résilience logicielles complètes et dynamiques), en plus d'une surveillance et d'une sécurité continues des API. À l'ère digitale, la fusion de deux entreprises entraîne souvent la détérioration ou l'obsolescence de produits et de services. Cependant, les API et les microservices associés doivent toujours être surveillés et sécurisés, au risque d'être également détériorés. Avec des équipes et des systèmes mixtes, la consolidation de la documentation interne peut ne pas suffire, et les solutions automatisées de segmentation et de sécurité des API réduisent le risque d'erreur humaine.

Les avantages des fusions et acquisitions pour les entreprises pharmaceutiques sont les suivants :

- Capacité à réaligner ou à étendre les portefeuilles en réponse aux changements stratégiques (y compris le réapprovisionnement de médicaments qui atteignent la phase du brevet)
- Capacité à acquérir des technologies innovantes qui complètent un portefeuille de produits existant ou une compétence de base
- Accès à de nouveaux marchés et/ou à des marchés différents
- Synergies de réduction des coûts, y compris l'expertise dans les solutions digitales

## Thème n° 5

### Blockchain et bases de données distribuées

Une blockchain est un registre public décentralisé et distribué digitalement qui existe sur un réseau d'entreprise. Dans le secteur de la santé, il est utilisé pour conserver et échanger les données des patients par le biais de divers systèmes et parties prenantes. La blockchain a également été utilisée pour fournir une visibilité sur la chaîne d'approvisionnement pour les matières premières et les API, ainsi que pour vérifier l'authenticité et suivre les expéditions de produits pharmaceutiques.

Bien que la blockchain soit une méthode de mise en œuvre de bases de données distribuées, il existe d'autres alternatives déployées dans le cloud et en bordure de l'Internet qui peuvent engendrer des avantages similaires. La santé est distribuée et les implémentations techniques doivent pouvoir gérer les performances et les fonctionnalités distribuées à grande échelle. En outre, il est important de s'assurer que la mise en œuvre est effectuée avec une infrastructure fournissant la vitesse nécessaire aux performances et la sécurité indispensable à la confiance.

Les avantages de la blockchain pour les entreprises pharmaceutiques sont les suivants :

- Sécuriser les chaînes d'approvisionnement grâce à une transparence accrue réduisant les médicaments non conformes et/ou obsolètes
- Réduire les médicaments contrefaits grâce à la traçabilité de la chaîne d'approvisionnement
- Améliorer la confidentialité des patients et la protection des données pendant les essais cliniques
- Prévoir et prévenir les pénuries de médicaments grâce à la visibilité sur les API et les matières premières

## Thème n° 6

### Cybersécurité : sécurité, conformité et réputation

Les entreprises du secteur des sciences de la vie sont confrontées à un environnement hautement réglementé dans lequel la non-conformité ou un investissement insuffisant dans l'infrastructure technique, la sécurité et la résilience organisationnelle peuvent s'avérer coûteux à bien des égards. Les interruptions de service ou de la chaîne d'approvisionnement dues à des cyberincidents peuvent avoir un impact sur la sécurité des patients en retardant l'accès aux médicaments prescrits ou aux informations. En outre, l'environnement réglementaire européen met l'accent sur la protection des données et la cybersécurité des infrastructures critiques. Le secteur des sciences de la vie est donc soumis à certaines des réglementations les plus strictes, tous secteurs confondus. Au-delà de la sécurité et de la conformité, les cyberincidents peuvent nuire aux marques et à la réputation d'une entreprise.

Les avantages d'un investissement dans la conformité en matière de cybersécurité sont les suivants :

- Éviter les amendes en cas de non-conformité, qui peuvent atteindre 15 000 000 € ou 2,5 % du chiffre d'affaires annuel mondial dans les cas les plus graves pour les entreprises européennes
- Réduire le risque de retards, qui a coûté entre 600 000 à 8 millions de dollars américains par jour aux entreprises du secteur des sciences de la vie, et empêcher les perturbations lors du recrutement pour les essais cliniques
- Prévenir les violations de données, qui représentent un coût moyen de 5,1 millions de dollars américains par incident dans le secteur des sciences de la vie

> **La cybersécurité est bien plus qu'un thème, elle constitue une base fondamentale pour la résilience dans le secteur des sciences de la vie.**

# L'importance de la microsegmentation et de la sécurité des API

Dans les modèles traditionnels de sécurité réseau, les réseaux sont généralement divisés en larges segments, en utilisant des pare-feux basés sur le réseau. Bien que cette approche offre un certain niveau de sécurité, elle ne dispose pas de la granularité requise pour protéger pleinement les environnements distribués actuels. Dans les environnements fédéraux, la segmentation basée sur le réseau entraîne généralement un provisionnement excessif des ressources. Autrement dit, les utilisateurs et les applications ont accès à plus de ressources qu'ils n'en ont réellement besoin. Cela crée des opportunités involontaires de mouvement latéral. À mesure que les attaquants compromettent une partie du réseau, ils peuvent se déplacer vers des zones plus sensibles avec peu de résistance.

Le concept de microsegmentation permet de résoudre ce problème en offrant un contrôle précis du trafic est-ouest au sein du réseau. Dans un environnement microsegmenté, chaque application, charge de travail ou service est isolé des autres, et l'accès est restreint en fonction de stratégies de sécurité spécifiques. Ainsi, les utilisateurs, les terminaux et les applications ne peuvent communiquer qu'avec les ressources auxquelles ils sont explicitement autorisés à accéder. En mettant en œuvre une segmentation orientée applications et basée sur les identités, la microsegmentation limite les dommages potentiels causés par les cyberattaques, réduit la surface d'attaque et applique le principe de Zero Trust.

En matière de trafic réseau nord-sud, les réseaux fédéraux s'appuient de plus en plus sur des API pour faciliter la communication entre les systèmes. Par conséquent, la protection des points de terminaison des API devient une priorité absolue. Les attaques d'API, y compris les attaques par injection, le « credential stuffing » et l'accès non autorisé aux données, ont fortement augmenté ces dernières années. Les agences et services fédéraux ont besoin de solutions complètes de sécurité des API afin de fournir une protection pendant tout le cycle de vie des API. Ainsi, le personnel de sécurité peut découvrir, surveiller et sécuriser le trafic des API en temps réel. La détection des API est particulièrement importante, car il n'est pas rare d'avoir des API dont personne n'a connaissance.

# Une analyse plus approfondie de la cybersécurité et de la conformité

Chaque réglementation liée à la cybersécurité affecte les investissements des entreprises pharmaceutiques dans l'infrastructure, la sécurité et la résilience.

Pour la majeure partie de l'Europe, les réglementations de l'UE, telles que le Règlement général sur la protection des données (RGPD) et la Loi sur la cyberrésilience, définissent des normes spécifiques et uniformes en matière d'infrastructure, de sécurité et de résilience des données. Une autre réglementation, le Règlement européen sur l'IA, inclut des infrastructures de données et des mesures de sécurité supplémentaires pour les entreprises qui explorent l'utilisation des applications d'IA. Toutes les entreprises exerçant leurs activités dans l'Union européenne doivent se conformer à ces réglementations et les sanctions sont appliquées de la même manière par les organismes de réglementation de chaque pays membre.

Au-delà de ces réglementations, la directive sur la sécurité des réseaux et des systèmes d'information (NIS2) signifie que les entreprises du secteur des sciences de la vie doivent vérifier leurs infrastructures et se conformer à des normes supplémentaires nationales en matière de cybersécurité et de résilience. Même les pays ne faisant pas partie de l'Union européenne, comme le Royaume-Uni et la Suisse, ont adopté des politiques similaires en matière de protection des données et de standardisation de la cybersécurité pour synchroniser la continuité des activités et les opérations transfrontalières avec le reste de l'Union.

## Réglementations européennes sur la cybersécurité spécifiques au secteur des sciences de la vie

Enfin, de nombreux pays européens ont également des réglementations supplémentaires en matière de cybersécurité pour les entreprises opérant dans les secteurs des infrastructures critiques ou de la santé et des sciences de la vie. Ces normes varient d'un pays à l'autre, mais sont néanmoins essentielles pour la conformité. Les entreprises du secteur des sciences de la vie doivent déterminer si ces réglementations s'appliquent à chaque pays dans lequel elles réalisent leurs activités.

Le tableau 2 indique les niveaux de lois et de réglementations en matière de cybersécurité auxquels les entreprises du secteur des sciences de la vie opérant en Europe doivent faire face.

| **Réglementations de l'UE en matière de cybersécurité** (Normes européennes) | | |
|---|---|---|
| RGPD | Règlement européen sur l'IA | Loi sur la cyberrésilience |
| **Directives de l'UE en matière de cybersécurité** (Transmises pays par pays au sein de l'Union européenne) | | |
| NIS2 | | |
| **Lois nationales** (Transmises par un seul pays) | | |
| Lois sur la cybersécurité (par exemple, Danemark, Royaume-Uni) | Lois sur les infrastructures critiques (par exemple, Allemagne) | Lois sur la santé et les sciences de la vie (par exemple, France, Suisse) |

**Tableau 2 :** Les lois et réglementations en matière de cybersécurité qui s'appliquent aux entreprises du secteur des sciences de la vie en Europe

À chaque niveau, ces politiques obligent les entreprises du secteur des sciences de la vie à respecter les normes en matière d'infrastructure de données, de sécurité et de confidentialité, de résilience et de reprise. Chaque entreprise doit identifier les bons outils pour protéger ses investissements stratégiques tout en restant en conformité.

# Mappage des mesures et méthodes de cybersécurité avec les domaines d'investissement

Les investissements des entreprises du secteur des sciences de la vie qui entraînent des avancées techniques et une modernisation, que ce soit pour stimuler la croissance ou en réponse à la croissance inorganique et aux fusions-acquisitions, ont des implications en matière de sécurité qui nécessitent une attention proactive. Le tableau 3 présente les capacités de cybersécurité les plus importantes pour protéger les six thèmes d'investissement des entreprises pharmaceutiques. En utilisant la proactivité comme principe directeur, le tableau organise les méthodes et les mesures pour sécuriser l'infrastructure, l'accès, les applications et les API et faciliter l'allocation des ressources appropriées.

| Comment améliorer la protection | Domaines de réflexion |
|---|---|
| **Sécuriser l'infrastructure**<br>• Renforcer l'environnement externe de votre infrastructure avec un outil d'atténuation des attaques DDoS et un pare-feu d'application Web de pointe<br>• Renforcer l'environnement interne de votre infrastructure avec une solution de microsegmentation | • Hébergement cloud, Big Data et analytique<br>• Fusions-acquisitions<br>• Soins virtuels |
| **Sécuriser l'accès**<br>• Accès réseau Zero Trust<br>• Authentification multifactorielle pour éviter le piratage de compte<br>• Passerelle Web sécurisée | • Hébergement cloud, Big Data et analytique<br>• Intelligence artificielle et apprentissage automatique<br>• Soins virtuels<br>• Fusions-acquisitions<br>• Blockchain et bases de données distribuées |
| **Sécuriser les applications et les API**<br>• Sécuriser les applications Web et les API pour renforcer l'intégrité des données et des résultats d'analyse<br>• Analyser le trafic API pour identifier les anomalies comportementales et les acteurs malveillants | • Hébergement cloud, Big Data et analytique<br>• Intelligence artificielle et apprentissage automatique<br>• Soins virtuels<br>• Cybersécurité : sécurité, conformité et réputation |
| **Faciliter l'allocation des ressources appropriées**<br>• Mener des recherches planifiées sur les menaces et faire des simulations d'équipe rouge<br>• Privilégier les partenaires dont les modèles d'assistance correspondent aux capacités de votre entreprise ; si votre équipe est petite, choisissez des partenaires offrant des services complets, selon vos besoins | • Hébergement cloud, Big Data et analytique<br>• Intelligence artificielle et apprentissage automatique<br>• Soins virtuels<br>• Fusions-acquisitions<br>• Blockchain et bases de données distribuées |

**Tableau 3 :** Les principales fonctionnalités de cybersécurité pour améliorer la protection

# Restez à l'abri des menaces

Bien qu'il s'agisse d'une période dynamique et innovante pour l'industrie pharmaceutique, de nombreux défis doivent encore être relevés. La santé est une cible privilégiée des cyberattaques. Les entreprises pharmaceutiques ne font pas exception à la règle en raison de la valeur élevée des informations de la chaîne d'approvisionnement, des données de santé protégées et de la propriété intellectuelle (comme les brevets) qu'elles détiennent.

La meilleure façon de rester au fait des risques tout en investissant dans votre transformation est de travailler avec un leader de confiance dans le domaine de la cybersécurité adaptée aux soins de santé. Produits, expertise, ressources, il saura vous protéger de manière adéquate contre les cybermenaces potentielles dans cette ère des avancées technologiques. Akamai est l'entreprise de cybersécurité et de Cloud Computing qui soutient et protège l'activité en ligne. Aujourd'hui, Akamai sécurise 8 des 10 plus grandes entreprises pharmaceutiques. Nos solutions de sécurité leaders du marché, nos renseignements avancés sur les menaces et notre équipe opérationnelle internationale assurent une défense en profondeur pour protéger les données et les applications des entreprises partout dans le monde. Les solutions de Cloud Computing complètes d'Akamai offrent des performances supérieures à moindre coût sur la plateforme la plus distribuée au monde. Les grandes entreprises du monde entier dans le secteur pharmaceutique et des sciences de la vie font confiance à Akamai pour garantir la fiabilité, l'évolutivité et l'expertise de pointe nécessaires pour développer leur activité en toute sécurité.

**Contactez Akamai pour en savoir plus sur les solutions qui protégeront les applications qui stimulent votre activité à chaque point d'interaction, sans compromettre les performances ou l'expérience client.**

Akamai

Les solutions de sécurité d'Akamai protègent les applications qui stimulent votre activité à chaque point d'interaction, sans compromettre les performances ou l'expérience client. En tirant parti de l'envergure de notre plateforme mondiale et de la visibilité qu'elle offre sur les menaces, nous travaillons avec vous pour prévenir, détecter et atténuer les menaces, afin de vous permettre de renforcer la confiance en votre marque et de concrétiser votre vision. Pour en savoir plus sur les solutions de Cloud Computing, de sécurité et de diffusion de contenu d'Akamai, rendez-vous sur akamai.com et akamai.com/blog, ou suivez Akamai Technologies sur X et LinkedIn. Publication : 05/25.