

Kiteworks lance des formulaires de données sécurisés avec une sécurité et une souveraineté totale des données

La seule solution de formulaires de données sécurisés qui associe la certification FedRAMP High Ready, la validation FIPS 140-3 et la résidence des données.

SAN MATEO, CA, UNITED STATES, November 18, 2025 /EINPresswire.com/ -- Kiteworks, qui aide les organisations à gérer efficacement les risques liés à l'envoi, au partage, à la réception et à l'utilisation de données privées, annonce aujourd'hui la disponibilité de Kiteworks Secure Data Forms — la seule solution de formulaires sécurisés combinant les plus hautes certifications de sécurité (FedRAMP High Ready, FIPS 140-3), un contrôle total de la souveraineté des données et une surveillance automatisée de la conformité pour les secteurs réglementés. Cette nouvelle offre étend le [Réseau de données privé \(PDN\)](#) de Kiteworks à la collecte de données via le web, révolutionnant la manière dont les entreprises des secteurs financier, de la santé, du gouvernement et du juridique collectent des informations sensibles.

Les formulaires web traditionnels sont devenus le maillon faible de la sécurité des entreprises. Les violations de données coûtent désormais en moyenne [4,44 millions de dollars](#), les amendes réglementaires ont été multipliées par dix en cinq ans et les lois sur la souveraineté des données couvrent plus de 100 pays. Les générateurs de formulaires classiques et les solutions d'entreprise héritées n'offrent ni certifications de sécurité, ni options de résidence des données, ni fonctions de conformité automatisée exigées par les secteurs réglementés — créant ainsi une vulnérabilité majeure lors de la collecte de données.

« Les organisations ne peuvent pas sécuriser les données collectées via des formulaires auxquels elles ne peuvent pas faire confiance », explique Yaron Galant, Chief Product Officer chez Kiteworks. « Chaque formulaire web représente un point d'entrée potentiel pour des informations sensibles — données clients, dossiers patients, informations financières, propriété intellectuelle. En même temps, il offre une large surface d'attaque à exploiter pour les acteurs malveillants. Pourtant, la plupart des entreprises utilisent des solutions de formulaires conçues pour la facilité d'utilisation, pas la sécurité. De plus, les responsables conformité ne peuvent pas vérifier où sont stockées géographiquement les données issues des formulaires. Les RSSI découvrent que leurs formulaires "sécurisés" manquent de résilience au niveau applicatif. Les organisations s'exposent à des violations de souveraineté parce que leur fournisseur de formulaires ne peut pas garantir la résidence des données. Kiteworks Secure Data Forms répond à ces risques en apportant une architecture Zero trust, l'automatisation de la conformité et un

contrôle total de la souveraineté des données à la collecte web de données. »

Sécurité inégalée : des certifications qui prouvent la protection au niveau gouvernemental
Intégrée au Réseau de données privé de Kiteworks, la solution Kiteworks Secure Data Forms obtient la certification FedRAMP High Ready — le plus haut standard de sécurité gouvernemental — prouvant que la plateforme répond aux exigences de sécurité de niveau militaire. La validation cryptographique FIPS 140-3 garantit la conformité de la protection des données grâce à des méthodes de chiffrement vérifiées. Ces certifications, indisponibles chez les générateurs de formulaires classiques ou les solutions héritées, représentent la validation rigoureuse par des tiers exigée par les secteurs réglementés.

La plateforme applique une architecture Zero trust sur l'ensemble du cycle de vie de la collecte de données. Contrairement aux formulaires traditionnels qui reposent sur la sécurité périmétrique, Kiteworks valide en continu chaque interaction, éliminant les risques internes et empêchant les mouvements latéraux en cas de compromission des identifiants. Cette approche répond à la montée des attaques sophistiquées ciblant les points de collecte de données que les organisations considèrent à tort comme peu risqués.

Souveraineté totale des données : garantir l'emplacement des informations sensibles
Les principaux atouts résident dans la robustesse de la sécurité et le contrôle total de la souveraineté des données, absents des solutions concurrentes. Les organisations déploient Secure Data Forms avec des options de résidence régionale des données, garantissant que les informations sensibles ne quittent jamais les juridictions spécifiées. Les données restent dans les régions requises, sécurisées et traitées localement, assurant la conformité au RGPD, à la HIPAA et aux exigences de localisation des données dans plus de 100 pays.

Les établissements de santé collectant des informations sur les patients dans plusieurs pays veillent à ce que les données restent dans les frontières requises. Les entreprises de services financiers maintiennent la séparation régionale des données pour satisfaire les exigences réglementaires. Les agences gouvernementales garantissent que les données des citoyens restent sur l'infrastructure nationale. Les multinationales respectent diverses lois de résidence des données sans multiplier les solutions de formulaires.

La plateforme propose des modèles de déploiement flexibles — cloud, sur site ou hybride — avec des options multi-régions alignées sur les cadres de gouvernance des données existants. Cette flexibilité offre le contrôle de la juridiction dont les responsables de la protection des données ont besoin pour prouver la conformité de la souveraineté lors des audits.

Conformité automatisée : réduisez la préparation des audits de 80 %

La surveillance continue de la conformité suit les soumissions de formulaires selon les exigences HIPAA, RGPD, SOX et PCI DSS en simultané. La plateforme documente automatiquement les flux de données, valide le statut du chiffrement et génère des journaux d'audit — réduisant jusqu'à 80 % le temps de préparation des audits par rapport à un suivi manuel.

Des alertes en temps réel informent les équipes sécurité et conformité en cas d'écart de configuration par rapport aux règles, d'accès inhabituel ou de transfert de données entre régions. Les organisations peuvent répondre instantanément aux questions clés des auditeurs : Où sont stockées ces données ? Qui y a accédé ? Comment sont-elles protégées ? Quelles mesures valident la conformité de la souveraineté ?

Découvrez Kiteworks Secure Data Forms sur kiteworks.com/secure-data-forms.

About Kiteworks

Kiteworks' mission is to empower organizations to effectively manage risk in every send, share, receive, and use of private data. The Kiteworks platform provides customers with a Private Data Network that delivers data governance, compliance, and protection. The platform unifies, tracks, controls, and secures sensitive data moving within, into, and out of their organization, significantly improving risk management and ensuring regulatory compliance on all private data exchanges. Headquartered in Silicon Valley, Kiteworks protects over 100 million end-users and over 1,500 global enterprises and government agencies.

David Schutzman

Kiteworks

+1 203-550-8551

[email us here](#)

Visit us on social media:

[LinkedIn](#)

[Facebook](#)

[YouTube](#)

[X](#)

This press release can be viewed online at: <https://www.einpresswire.com/article/868090856>

EIN Presswire's priority is source transparency. We do not allow opaque clients, and our editors try to be careful about weeding out false and misleading content. As a user, if you see something we have missed, please do bring it to our attention. Your help is welcome. EIN Presswire, Everyone's Internet News Presswire™, tries to define some of the boundaries that are reasonable in today's world. Please see our Editorial Guidelines for more information.

© 1995-2025 Newsmatics Inc. All Right Reserved.