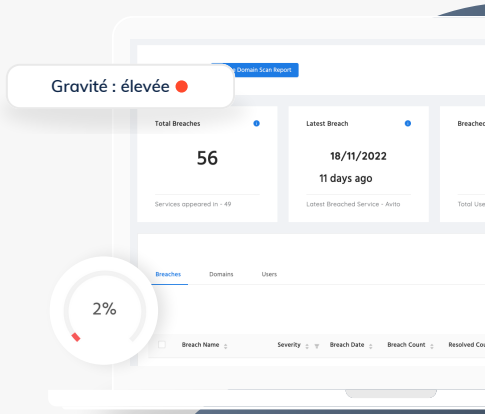
Défendez votre entreprise grâce à une surveillance proactive des brèches



Protégez votre entreprise contre les dangers cachés du Dark Web grâce à une surveillance exploitable du Dark Web et à des alertes instantanées en cas de brèche.

Réduire les risques existants

Identifiez les données utilisateur sensibles actuellement accessibles aux hackers.

Prévenir les futures brèches

Recevez des alertes instantanées par e-mail lorsque des utilisateurs sont détectés dans les dernières brèches.

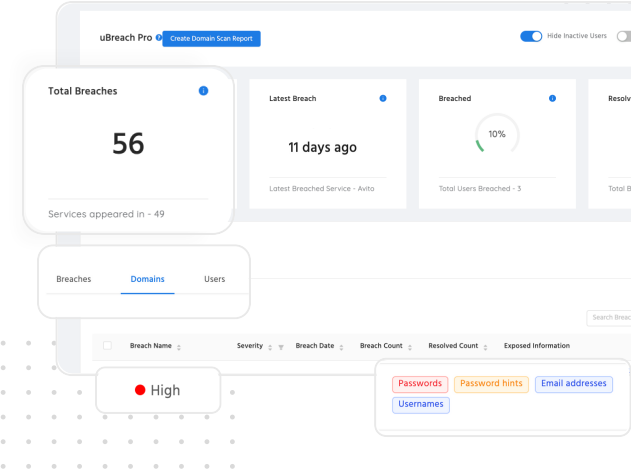
Atteindre la conformité

Démontrez vos efforts en matière de protection des données et de conformité réglementaire.

Prévenir les cybermenaces avant qu'elles arrivent

À une époque où la sécurité numérique est primordiale, les entreprises ne peuvent pas se permettre de rester aveugles aux dangers qui se cachent dans l'ombre du Dark Web. Les informations d'identification des utilisateurs et les données sensibles, une fois exposées, deviennent des outils pour les cybercriminels, entraînant des failles de sécurité potentielles, des pertes financières et des atteintes à la réputation.

Notre service avancé de surveillance du Dark Web offre une ligne de protection essentielle, identifiant et atténuant de manière proactive ces risques avant qu'ils ne dégénèrent en crises.



Notre service ouvre la voie en matière de surveillance du Dark Web

Cybersécurité améliorée

Réduisez considérablement les cyber-risques humains et prévenez les failles de sécurité coûteuses.

Alertes proactives en cas de brèche

Gardez une longueur d'avance sur les menaces grâce à des notifications instantanées par e-mail pour les utilisateurs et administrateurs concernés.

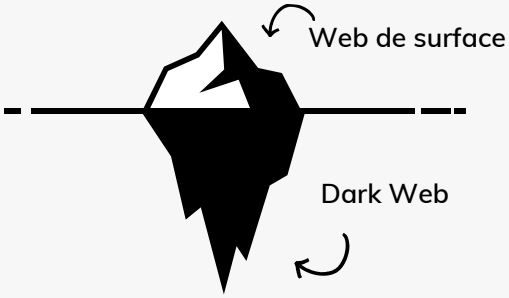
Couverture complète

Étendez la protection à tous les comptes de messagerie utilisateur associés à votre domaine.

Comprendre l'impact du risque

Réduisez votre score de risque humain continu en résolvant rapidement les brèches des utilisateurs.

Le Dark Web : un terrain idéal pour les attaques ciblées



Dans le paysage numérique actuel, où les cybermenaces se cachent partout, la protection des informations sensibles de votre entreprise n'est pas seulement une nécessité : c'est un impératif. Alors que le dark web devient un marché florissant pour les identifiants d'utilisateurs et les données confidentielles volés, les entreprises dépourvues de solutions de surveillance robustes se trouvent à la croisée de risques croissants et de crises potentielles.

24,6B

Un rapport de Digital Shadow a révélé que 24,6 milliards d'ensembles complets de noms d'utilisateur et de mots de passe circulent sur les marchés cybercriminels.

Ces 24,6 milliards de combinaisons de nom d'utilisateur et de mot de passe proposées à la vente sur le Dark Web affichent une augmentation de 65 % depuis 2020.

Le rapport Threat Horizons 2023 de Google Cloud révèle que 86 % des brèches impliquent le vol d'informations d'identification, y compris des informations confidentielles. noms d'utilisateur et mots de passe.

Pourquoi votre entreprise devrait-elle se concentrer sur la lutte contre les menaces du Dark Web ?

Risque accru d'accès non autorisé

Les informations d'identification des utilisateurs volées étant librement disponibles sur le dark web, les entreprises sont confrontées à un risque accru d'accès non autorisé à leurs systèmes et à leurs données sensibles.

Attaques ciblées d'ingénierie sociale

La disponibilité d'informations personnelles et professionnelles sur le dark web permet aux cybercriminels de tromper les employés et de compromettre la sécurité.

Risques/amendes en matière de réglementation et de conformité

L'exposition de données sensibles sur le dark web peut entraîner des brèches de la conformité réglementaire, entraînant des amendes et une atteinte à la réputation.