FICHE PRODUIT AKAMAI

# Account Protector

## Bloquez les fraudeurs et préservez la confiance en vous protégeant contre l'usurpation de comptes

**Comment savoir si un utilisateur est authentique ou s'il s'agit d'un imposteur ? Vos clients comptent sur vous pour faire la distinction entre les deux.**

Tandis que la généralisation des transactions digitales et l'adoption de nouveaux actifs numériques se poursuivent, les risques et les conséquences d'une usurpation de comptes sont plus importants que jamais. Votre capacité à développer votre activité digitale et à protéger vos clients repose sur le maintien de la confiance dans un environnement où les tactiques de fraude évoluent constamment.

Les abus liés aux comptes, tels que l'ouverture frauduleuse de comptes (fraude par ouverture de compte) et le piratage de comptes, représentent des défis et des coûts importants pour les entreprises de tous les secteurs. Les comptes compromis et les faux comptes peuvent avoir de graves conséquences financières et sur la réputation pour les organisations. Lorsqu'un compte est compromis, les pirates peuvent l'exploiter librement, en drainant les soldes, en effectuant des transactions frauduleuses, en désactivant des fonctionnalités de sécurité telles que l'authentification multifactorielle ou en volant des informations personnelles sensibles. Les faux comptes, quant à eux, peuvent être utilisés pour profiter de promotions telles que des essais et des crédits gratuits, exécuter un trafic artificiellement gonflé et inonder les plateformes de spams ou de contenus inappropriés. L'impact de ces attaques est considérable et les entreprises sont exposées au risque de perte de confiance de la part de leurs clients, de perte de millions en raison de la fraude, d'amendes réglementaires et d'atteinte à leur réputation.

## Akamai Account Protector

Account Protector est une solution de sécurité conçue pour prévenir les usurpations de comptes tout au long du cycle de vie d'un compte, en utilisant l'apprentissage automatique et un ensemble important d'indicateurs de risque et de confiance pour déterminer la légitimité d'une demande d'utilisateur. Cette solution permet d'analyser le comportement en temps réel afin d'identifier les signes subtils d'activité frauduleuse, de la création du compte à la connexion, et même au-delà. Si un comportement suspect ou anormal est détecté, Account Protector fournit des options d'atténuation immédiates pour maintenir une expérience utilisateur fluide, telle que le blocage et la prise de mesures en bordure de l'Internet, l'exécution de défis cryptographiques et comportementaux, l'exécution d'un contenu alternatif et bien plus encore.

### Avantages pour votre entreprise

**Renforcez la confiance, de votre côté comme du leur :**
identifiez les interactions légitimes, réduisez les frictions pour les utilisateurs et protégez ces derniers contre les activités frauduleuses.

**Développez des protections adaptées à votre entreprise :**
tirez parti des détections automatiques de bots et de la capacité à comprendre les profils de la population d'utilisateurs en fonction de la façon dont ils interagissent avec votre site.

**Bénéficiez d'une vision et d'une visibilité approfondies :**
prenez des mesures en toute confiance sur la base de signaux et d'indicateurs transparents.

**Réduisez les retombées de la remédiation :**
réduisez les coûts et les ressources nécessaires pour enquêter sur les comptes compromis, remplacer les actifs volés, etc.

**Prenez de meilleures décisions en matière de sécurité et d'identité basées sur les données :**
intégrez notre solution à des outils de lutte contre la fraude, des SIEM et d'autres outils de sécurité pour utiliser les signaux de risque et de confiance d'Account Protector afin d'augmenter la précision et d'améliorer votre investissement dans ces outils.

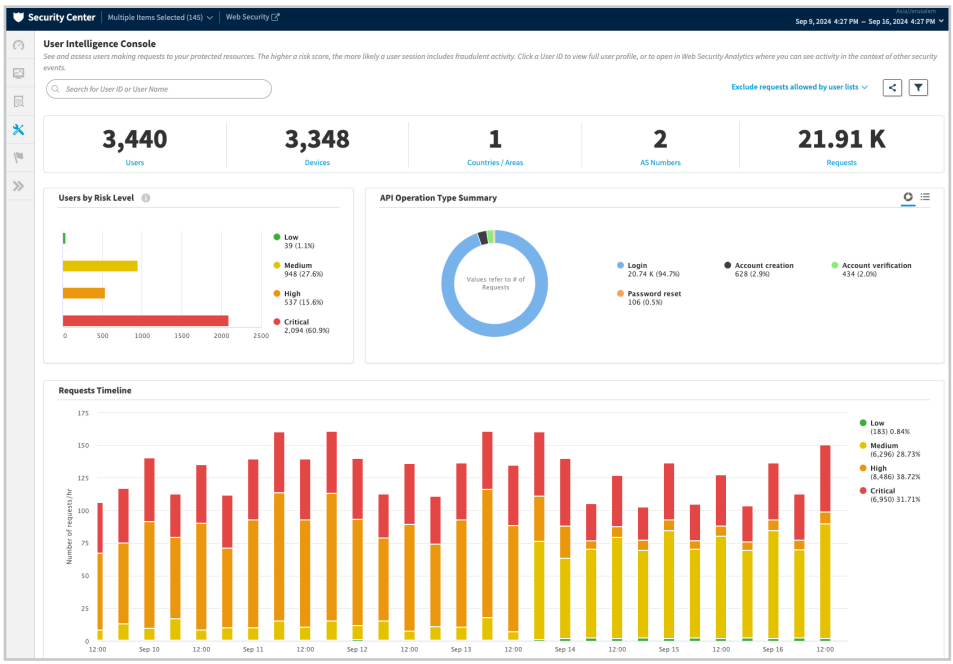
## Bénéficiez d'une défense globale contre les usurpations de comptes

Préservez les comptes utilisateur des abus tout au long de leur cycle de vie, en fournissant une protection avancée contre les usurpations de compte, les attaques par piratage de compte et les schémas d'attaque qui en découlent.

**Usurpation d'ouverture de compte** : atténuez la création de faux comptes utilisés pour profiter de promotions, exécuter un trafic artificiellement gonflé, tester des informations de cartes de crédit volées, accumuler des stocks, et bien d'autres choses encore.

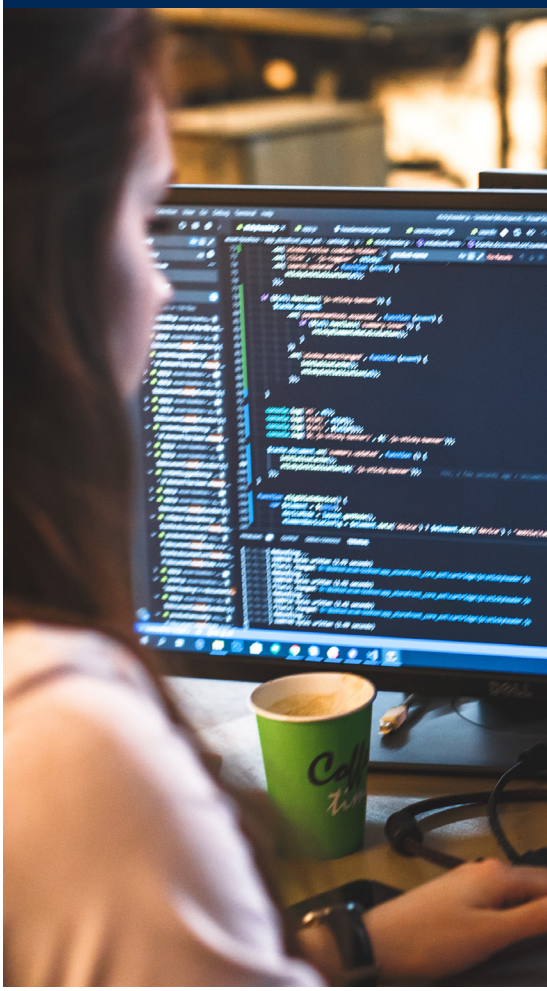
**Prise de comptes** : protégez-vous contre les imposteurs qui accèdent à des comptes clients légitimes pour les déposséder de leur valeur, voler des données sensibles et commettre des transactions frauduleuses.

**Attaques sophistiquées de bots malveillants** : protégez les comptes d'utilisateurs contre le credential stuffing, la manipulation des stocks et autres attaques automatisées souvent lancées conjointement à une usurpation ou un piratage de compte visant à dérober des produits de valeur, de l'argent ou d'autres actifs précieux.




## Protégez, faites confiance et profitez de l'expérience de l'utilisateur

Analysez les risques et arrêtez les abus en temps réel, en surveillant continuellement les comptes tout au long de leur cycle de vie pour détecter les signes de comportement suspect dès qu'ils se produisent.



## Principales fonctionnalités

**Protection complète du cycle de vie des comptes** : identifie et analyse les risques encourus par les utilisateurs à tout moment, de la création du compte aux activités post-connexion comme les mises à jour de compte, les modifications de mot de passe et les paiements.

**Évaluation en temps réel des risques liés à la session de l'utilisateur :** évalue les risques et la confiance tout au long de la session utilisateur pour évaluer si une demande émane d'un utilisateur légitime ou d'un imposteur.

**Renseignements liés aux adresses e-mails :** analyse la syntaxe d'une adresse e-mail et l'utilisation anormale d'un e-mail pour détecter les schémas malveillants.

**Renseignements sur les domaines de messagerie** : évalue le modèle d'activité provenant de domaines de messagerie individuels, y compris les domaines jetables et l'utilisation excessive d'un domaine de messagerie.

**Reconnaissance mondiale des utilisateurs de confiance** : fournit une visibilité sur le comportement des utilisateurs sur le réseau Akamai afin de prendre des décisions plus éclairées concernant la fiabilité d'une connexion.

**Profils comportementaux des utilisateurs** : dresse un profil comportemental d'utilisateur selon les emplacements, les réseaux, les terminaux, les adresses IP et le temps d'activité observés précédemment afin de reconnaître les utilisateurs qui reviennent.

**Profils de population** : regroupe les profils d'utilisateurs de votre entreprise en un super-ensemble, ce qui permet de comparer les variations de comportement à l'ensemble des utilisateurs pour la détection des anomalies.

**Réputation de la source** : évalue la réputation de la source en se basant sur l'activité malveillante passée observée chez tous les clients d'Akamai, y compris un grand nombre des sites Web les plus importants, les plus fréquentés et les plus fréquemment attaqués au monde.

**Indicateurs** : appuie l'évaluation de chaque demande par des indicateurs de risque, de confiance et généraux afin d'évaluer le risque d'usurpation de compte. Les indicateurs sont fournis avec le score final de risque de l'utilisateur et peuvent être utilisés pour l'analyse.

**Détections des bots sophistiqués** : détecte avec précision les bots inconnus dès la première interaction grâce à une variété de modèles et de techniques d'apprentissage automatique et d'IA. L'analyse du comportement de l'utilisateur/de la télémétrie, l'empreinte du navigateur, la détection automatisée des navigateurs, la détection des anomalies HTTP, le taux élevé de demandes et plus encore en font partie intégrante.

**Analyses et rapports** : fournit des rapports en temps réel et historiques. Analysez l'activité sur des points de terminaison individuels, enquêtez sur un utilisateur spécifique, examinez les utilisateurs par niveau de risque et obtenez des informations approfondies.

**Mesures de riposte avancées** : fournit un large éventail d'actions qui peuvent être appliquées pour mettre fin aux abus, y compris l'alerte, le blocage, le retard, le défi cryptographique et comportemental, le contenu alternatif, et bien plus encore. Les entreprises peuvent également entreprendre différentes actions en fonction de l'URL, du moment de la journée, de la géolocalisation, du réseau ou du pourcentage de trafic.

**Injection d'en-tête** : envoie des informations sur les risques pour l'utilisateur à des fins d'analyse et d'atténuation en temps réel. Un en-tête de demande supplémentaire est injecté dans la demande transférée avec des informations sur le score de risque de l'utilisateur, ainsi que les indicateurs de risque, de confiance et généraux qui ont contribué à ce score, afin de permettre une analyse plus approfondie et une atténuation en temps réel.

**Automatisation grâce à l'apprentissage automatique** : actualise automatiquement les caractéristiques et comportements utilisés pour identifier les activités frauduleuses humaines et les bots, des schémas comportementaux aux derniers scores de réputation sur la plateforme Akamai.

**Intégration SIEM (en option)** : intègre les informations sur les risques pour les utilisateurs dans les outils SIEM pour les clients qui souhaitent bénéficier d'une visibilité plus intégrée de la sécurité. Vous pouvez enrichir la valeur de vos outils existants grâce aux informations fournies par Account Protector.

## Contactez votre représentant Akamai ou visitez la page Akamai.com pour en savoir plus.