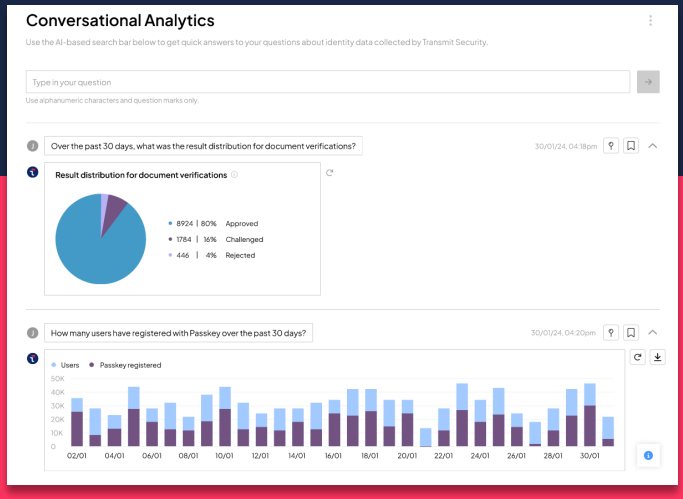
Transmit Security
Fonctionnalités de détection et prévention de la fraude



Nos fonctionnalités évoluent !

Découvrez l'ensemble de nos capacités

Février 2024

Détection

Transmit Security

Transmit Security propose une véritable solution de multi-détection. Plutôt que de créer une solution pour résoudre des modes opératoires de fraude spécifiques (malware/MITM, réseau, …) notre solution est conçue pour fonctionner à travers de nombreux types de détections différents. En conséquence, les modèles d''IA sont capables de répondre d'évoluer naturellement pour répondre aux nouveaux modes opératoires.

Nos capacités de détection en temps réel

Général

- Évaluation du risque en continu
- Détection multi-méthodes : Appareil, Réseau, Comportemental, Événement
- Détection de confiance
- Threat intelligence inclut
- Détection de prise de contrôle de compte
- Détection de fraude à l'ouverture de nouveaux comptes
- Efficacité de détection prête à l'emploi
- Machine Learning avancé

Détection de bots

- Credential stuffing
- Bots d'inscription/ouverture de compte
- Haute vélocité
- Détection de frameworks d'automatisation
- Détection de bots comportementaux

Connaissance du réseau

- Tor endpoint
- Proxy, Proxy anonyme
- VPN
- Réseaux de bots
- Réputation IP frauduleuse
- Hébergement/centres de données
- Organisations (Gouvernement, Éducation, Entreprises)
- Données de consortium de réseau
- Listes de confiance/refus IP/ASN
- Décalage de fuseau horaire

Analyse des transactions

- Profilage de compte et de transaction et anomalie - payeur, bénéficiaire, détails de transaction

Analyse post-détection

- Détection de campagnes
- Détection de réseaux de fraude
- Détection d'anomalies en série temporelle
- Comptes mule

Connaissance des appareils

- Empreinte d'appareil
- Inadéquation d'appareil
- Usurpation d'appareil
- Machines virtuelles
- Détection d'émulateur mobile
- Détection de logiciels malveillants mobiles (Sécurité d'application mobile étendue)
- Détournement de session
- Prise de contrôle d'appareil et chevaux de Troie d'accès à distance
- Fermes d'appareils
- Réputation d'appareil
- Appareil compromis
- Site web compromis
- Liaison cryptographique d'appareil (device crypto binding)
- Sites web et domaines de phishing
- Données de consortium d'appareils
- Appareils de confiance/défi/refus

Profil utilisateur et analyse des événements

- Appareils de confiance
- Lieux de confiance
- ASN de confiance
- Langues de confiance
- Fuseaux horaires de confiance
- Biométrie comportementale et détection d'anomalies
- Analyse de l'interaction avec l'appareil - mouvements de souris, frappes, etc.
- Anomalies des motifs d'activité
- Anomalies d'utilisation de l'appareil
- Anomalies d'utilisation du réseau
- Voyage impossible
- Méthodes de saisie des identifiants
- Arnaques d'ingénierie sociale (y compris Chatbot basé sur LLM)
  - Fraude au faux banquier - manipulation des utilisateurs pour qu'ils effectuent un virement vers un compte de fraudeur
- Listes d'utilisateurs de confiance/défi/refus

Les détections de campagnes d'attaques, réseaux de fraudes, anomalies et comptes mules sont effectuées de manière continue et spécifique à chaque client.
Nous récupérons plus d'un milliard de données issues de différents flux, d'analyses du dark web, etc., et pouvons les corréler à ce qui se passe chez un client spécifique.

Ceci diffère des données de consortium pour deux raisons :

- Nous n'imposons pas un modèle de "donner pour recevoir". Les données clientes restent intactes et privées.
- En utilisant des mécanismes de détection multiples, nous sommes capables d'intégrer de nombreux types d'informations dans les modèles, et de traiter automatiquement de nouveaux modes opératoires.

transmit security

Administration

L'expérience d'administration est essentielle pour tirer le meilleur parti des données collectées et analysées. Transmit Security offre des outils pour faciliter l'onboarding de nouveaux administrateurs (SSO pour accéder à la console), mais également pour automatiser vos processus de lutte contre la fraude. Notre puissant outil de détection en continu sur l'ensemble des données de risques, vous permet de corréler automatiquement plusieurs actions de différents utilisateurs et appareils pour détecter des campagnes d'attaques ou des réseaux de fraudes. Combiné à notre outil de workflow, vous pouvez ainsi automatiser le blocage temporaire d'utilisateur, d'IP, etc.

Transmit Security

Nos capacités de d'administration

Configuration et personnalisation

- Support multi-applications
- Interface de règles de décision de risque
- Interface d'étiquettes de retour
- Interface de politique de sensibilité de détection

Sécurité

- Audit d'activité administrateur
- SSO fédéré (via OIDC)
- Accès basé sur le rôle
- SOC 2
- Données chiffrées
- Protection WAF
- Données chiffrées et signées
- Protection anti-rejeu
- Protection anti "Homme-du-Milieu" (MitM)

Gestion de cas / d'analyses

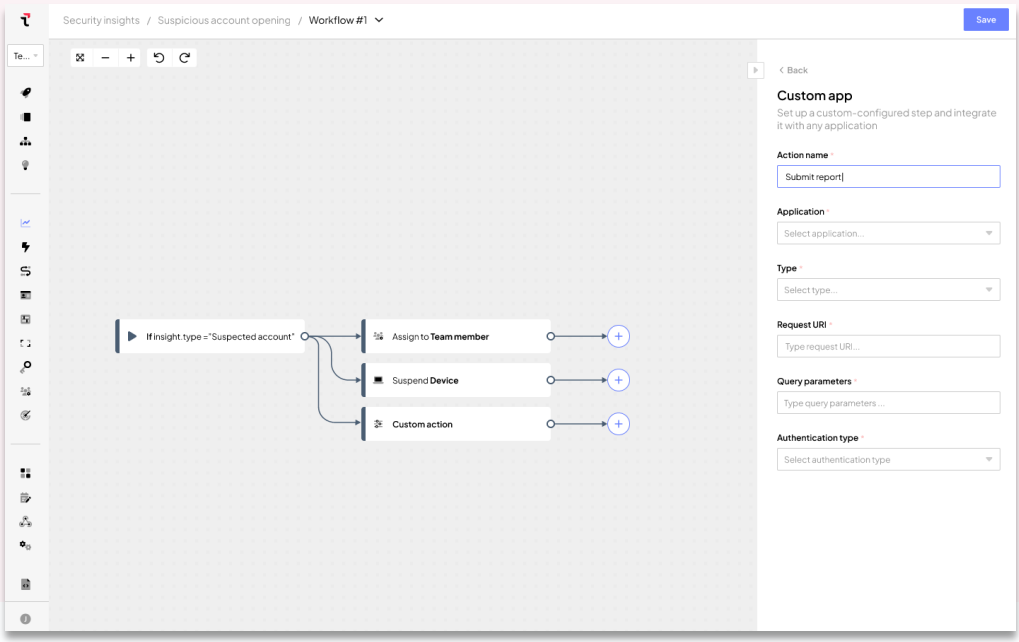
- Services d'analyste de sécurité en temps réel, 24/7
- Centre de notification et d'incident gérable
- Workflows automatisés et playbooks

Simulateur d'attaque

- Simulation de MO d'attaque
- Formation MO d'attaque
- Activation MO d'attaque

Rapports

- Exportation de données brutes - contexte de recommandation, signaux et raisons
- Interrogation en langage naturel basée sur l'IA
- L'IA est utilisée dans tous les modèles, en utilisant un LLM pour permettre l'interrogation de n'importe quelle donnée et effectuer des investigations et analyses approfondies par le biais de requêtes en langage naturel.
- Tableaux de bord et visualisations personnalisés
- Vue consolidée qui permet une analyse en temps réel, analyse post-détection, investigation, automatisation des alertes et des processus opérationnels et analyse globale de la fraude.
- Signaux de risque avancés
- Exportation de données au format CSV
- Expérience d'investigation riche
- Vue détaillée de l'utilisateur
- UI d'analytique riche et visualisations
- Tableau de bord d'analyste général
- Interface de streaming d'événements programmatique (API)
- Intégration SIEM générique
- Connecteurs SIEM natifs intégrés (Splunk, etc.)
- Notifications et alertes en temps réel
- Vue centralisée des incidents de haute gravité



Une campagne d'attaque détectée ? Un compte suspect vient d'être ouvert ?

Utilisez nos **workflows** pour orchestrer vos processus de travail:
- assignez le dossier à un collègue automatiquement;
- bloquez un appareil temporairement
- envoyez un rapport par mail ou sur votre messagerie d'entreprise
- utilisez nos connecteurs génériques (API) pour réaliser des actions personnalisées (bloquer les IP, envoyer des informations, …)

transmit security

Outils développeurs

L'expérience développeur est essentielle pour assurer une bonne utilisation du produit.
Nous mettons à disposition des facilités d'intégration pour éviter d'être bloqué par des bloqueurs de publicité, mais également des API pour automatiser le surentraînement de nos algorithmes pour votre contexte spécifique.

Transmit Security

Nos facilités pour les développeurs

Cross canal

- Web
- iOS
- Android

API

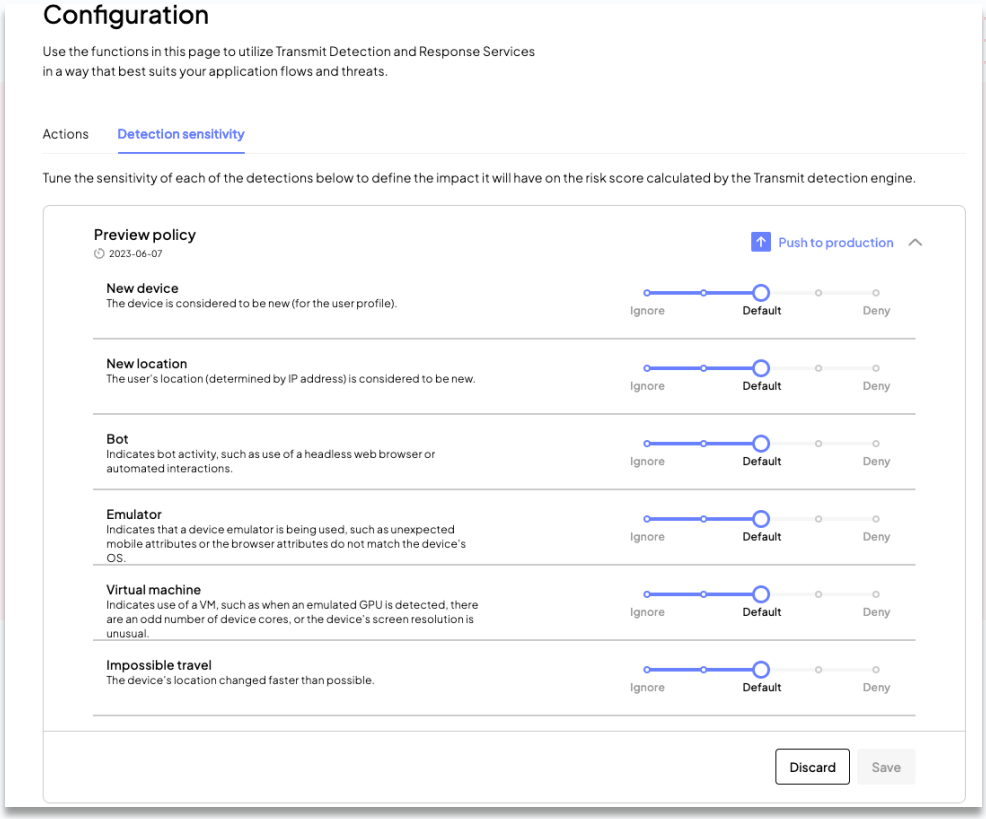
- Recommandation en temps réel
- Règles statiques
- Étiquettes (labels)
- Politiques de sensibilité

Quick-starters

- Angular
- React
- Vanilla

Général

- Contournement des bloqueurs de publicités - Domaine personnalisé
- Intégration basée sur CDN
- Intégration basée sur gestionnaire de balises
- Intégration directe dans l'application



Sensibilité de détection

Transmit Security vous permet d'influencer directement le score de détection grâce aux curseurs de sensibilité de détection.

Considérez-vous l'utilisation d'un nouvel appareil comme plus risqué ? Alors augmentez le curseur correspondant. Le score de risque en sera directement affecté.

Règles statiques

T

transmit security

Plateforme

Transmit Security

Détecter les bots, comportements suspects et ingénieries sociales ne suffisent pas à bloquer les fraudeurs. Il est nécessaire d'avoir des moyens de challenger l'utilisateur et d'adapter le parcours en fonction du risque. Nos outils de vérifications d'identité, d'authentification forte, et d'orchestration permettent de répondre à ces besoins.

Les capacités de notre plateforme

Orchestration

- Service d'orchestration d'identité
- Service d'orchestration de fraude (inter-fournisseurs)

Général

- Vue et analyses globales des utilisateurs
- Services d'IDP et d'authentification

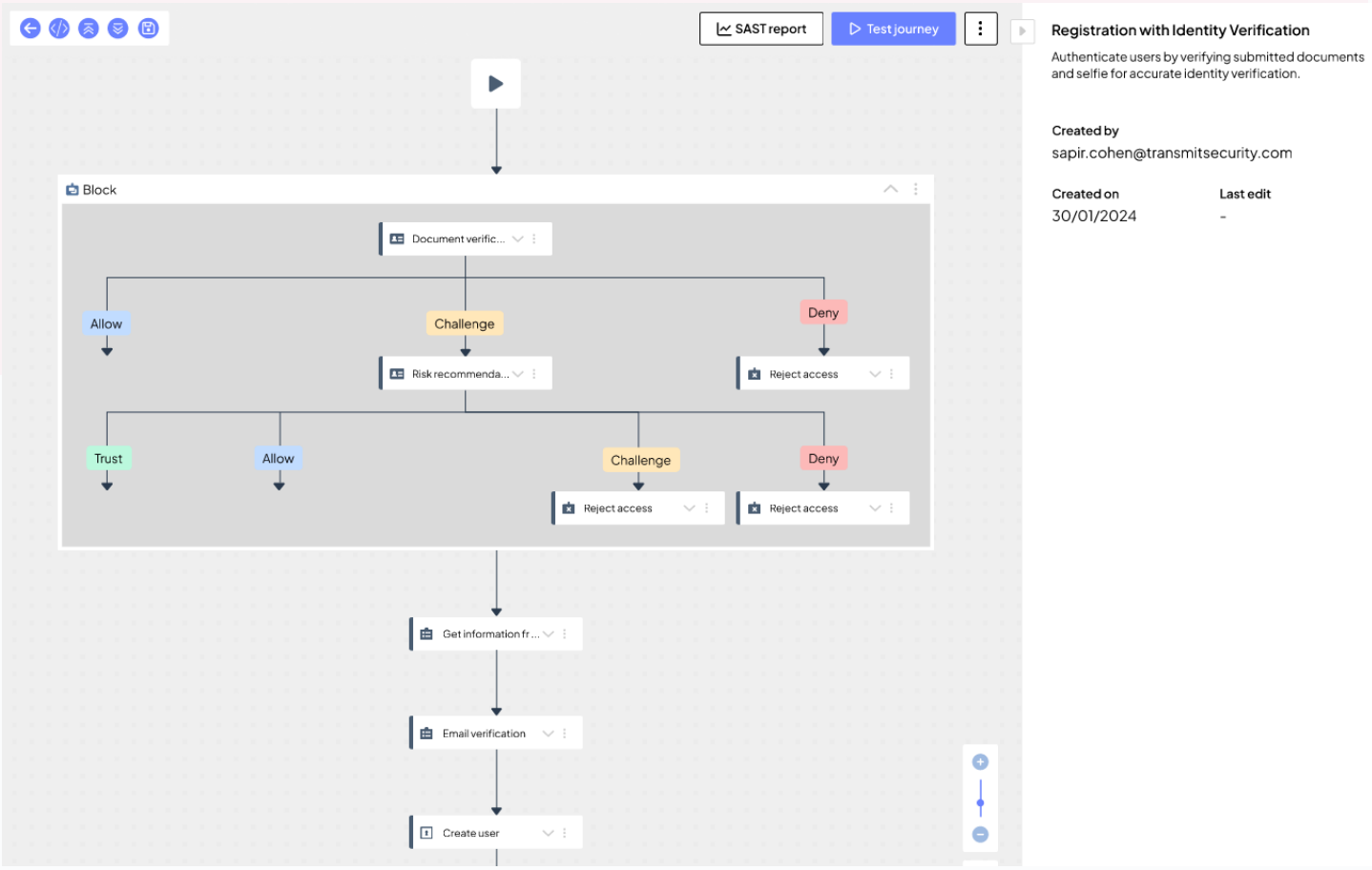
Vérification

- Services de vérification - identifiants personnels (email, numéro de téléphone)
- Services de vérification - Authentification par photo d'identité
- Services de vérification de pièce d'identité et preuve de vie

Répondez aux menaces en temps réel avec l'orchestration

Que faire une fois qu'une menace a été détectée ? La mise en place de parcours adaptatifs peut se révéler longue et compliquée. Avec notre outil d'orchestration, la mise en place de logique d'orchestration est simplifiée : plus besoin de développer une logique serveur avec un langage de programmation, tout peut se faire visuellement, en drag and drop.

Notre outil d'orchestration peut également se révéler être un atout précieux pour assembler les informations de plusieurs éditeurs, et en sortir une décision contextualisée.



transmit security

Architecture Cloud

Fort de notre expérience, nous avons redéfini notre architecture Cloud de zéro pour permettre une évolutivité sans couture, ainsi que la possibilité de s'appuyer sur les dernières avancées en termes d'intelligence artificielle pour aider à la post-analyse.

Transmit Security

Notre architecture Cloud et ses bénéfices

Multi-Région

- États-Unis
- Canada
- Union Européenne
- Chaque région est silotée

Disponibilité

- Plus de 99,99%

Passage à l'échelle

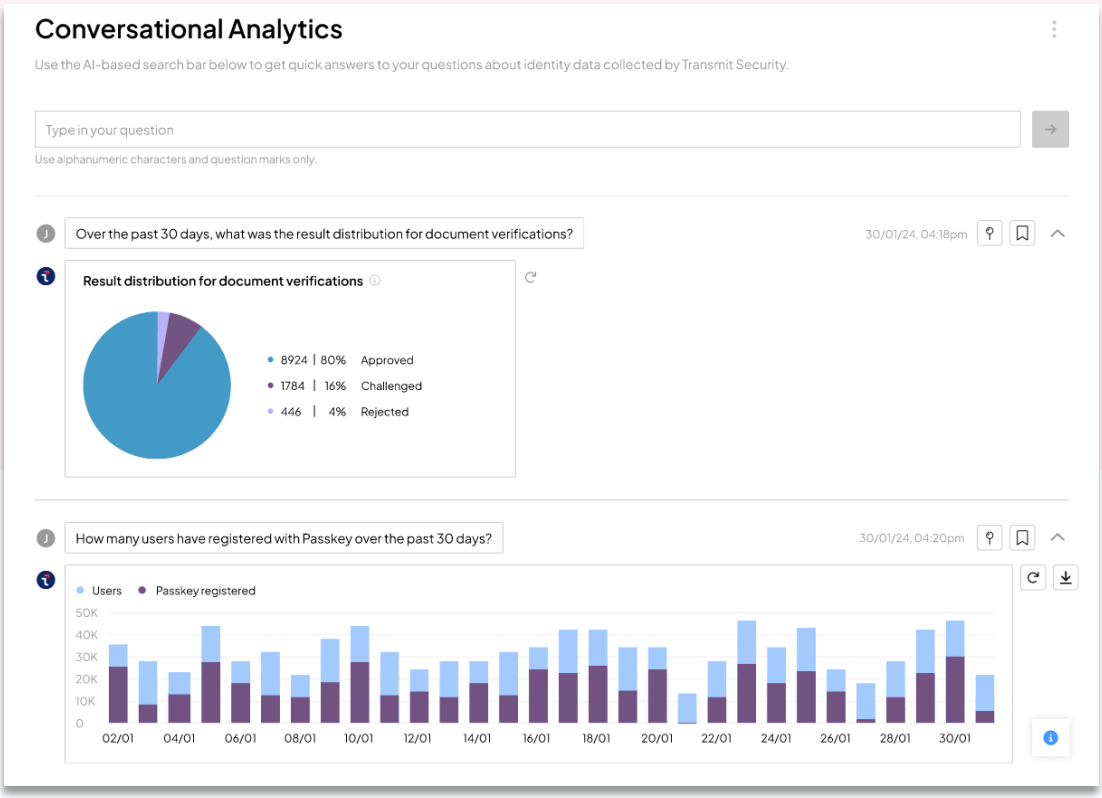
- Mise à l'échelle horizontale pour plus de 100 000 transactions par seconde

Une architecture Cloud Native qui s'appuie déjà sur les dernières avancées de l'IA

Notre architecture dernière génération permet de tirer le meilleur parti de nos systèmes de détections. En développant nous-même toutes les capacités de détection (fingerprint, bot, émulation, comportement, etc.), nous sommes en mesure de normaliser les données collectées via tous les canaux (web, mobile, call center, kiosque, …).

Non seulement cela nous permet d'optimiser le taux de faux négatifs et faux positifs, mais cela nous a également permis de développer un outil intuitif de navigation dans cet ensemble de données, basé sur l'utilisation du langage naturel.

Maintenant, n'importe quel expert métier peut simplement poser des questions écrites pour obtenir des graphiques, tableaux et informations sur les types de fraudes rencontrées, les appareils et IP vues les plus régulièrement, etc.

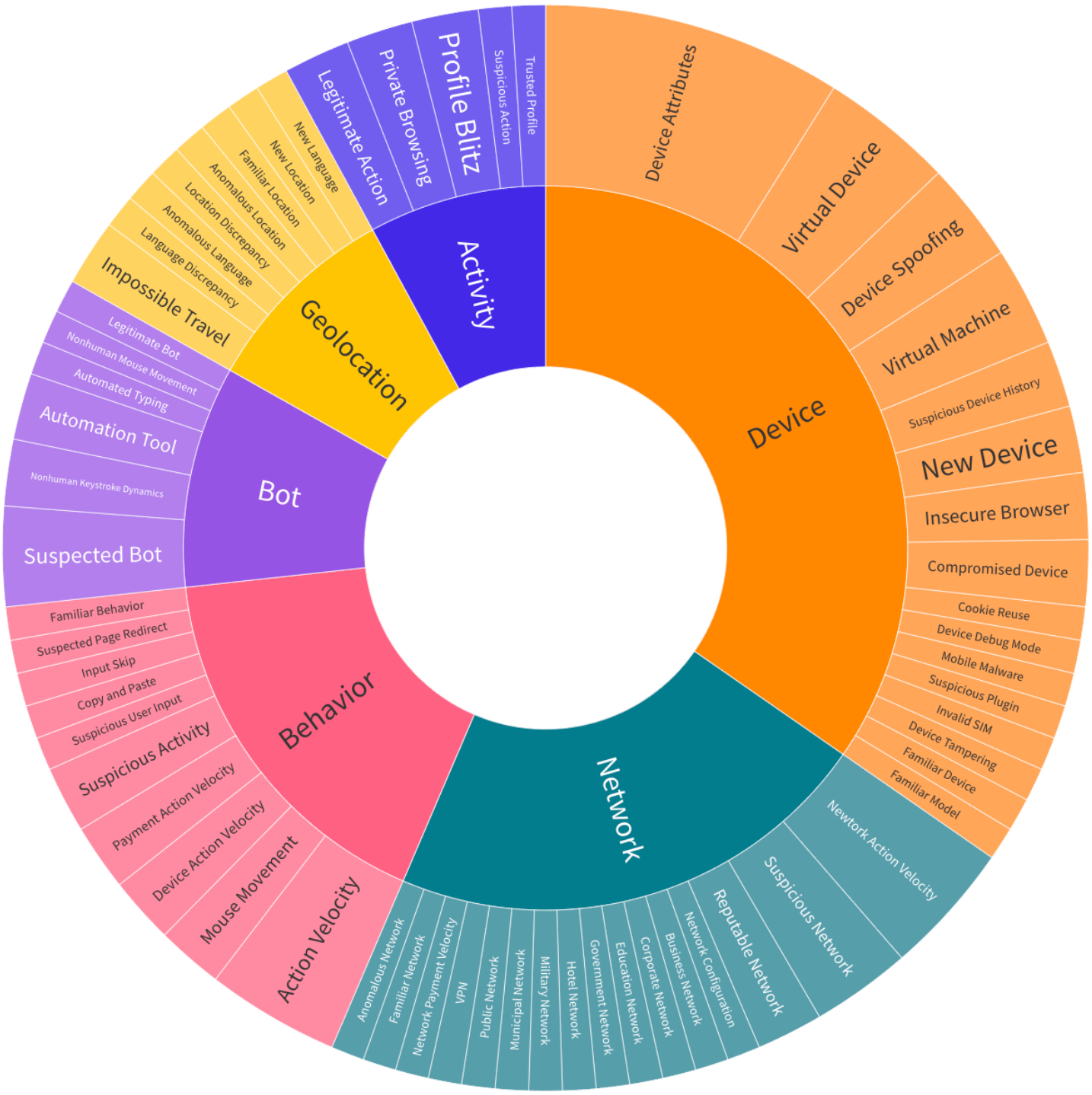


transmit security

Liste des détections

Nous nous appuyons sur des centaines de signaux de détection pour fournir un score précis et réduire le taux de faux négatifs et faux positifs au minimum.
Ci-dessous une roue qui illustre certaines de nos détections par catégorie.

Transmit Security



transmit security

transmit security

KuppingerCole ANALYSTS

Seul fournisseur à avoir reçu le **statut de leader global :** produit, innovation et marché dans 3 rapports du KuppingerCole Leadership Compass.

"The platform has one of the most feature-rich offerings in the passwordless authentication market and would likely be suitable for any type of organization looking to adopt a passwordless solution."

> *We envision a world where businesses no longer compromise between Security and exceptional Customer Experience.*
>
> Mickey Boodaei
> CEO and Co-Founder, Transmit Security

Sophie Belloc
Sales Director
06 79 82 56 30
sophie.belloc@transmitsecurity.com

Erwan Dano
Sales Engineer
07 86 98 40 01
erwan.dano@transmitsecurity.com

ILS NOUS FONT CONFIANCE

TIAA · citi · UBS · NN · Rabobank · America's Car-Mart · Intesa Sanpaolo · AXA · usbank · Cattolica Assicurazioni

Passwordless Authentication Overall Leader · fido Alliance simpler stronger authentication · Gartner Cool Vendor 2020 · AICPA SOC · GDPR Ready · PSD2