Vertrauen in die digitale Wirtschaft sichern.

Lösungen, die speziell entwickelt wurden, um die Menschen zu unterstützen, die die vernetzte Wirtschaft von heute schützen.

CYBERSICHERHEIT

August 2024

Mastercard Cybersecurity-Lösungen im Überblick

Lösung	Leistungsversprechen
RiskRecon	RiskRecon ist eine Lösung zur Überwachung der IT-Risiken von Drittanbietern, die sicherstellt, dass Lieferanten und Zulieferer Ihre Sicherheitsanforderungen einhalten und Ihre Vermögenswerte nicht gefährden.
Systemic Risk Assessment (SRA)	SRA überwacht und bewertet proaktiv komplexe, sich entwickelnde Geschäftsrisiken über mehrere Dimensionen hinweg in Ihrem gesamten Netzwerk von Geschäftsbeziehungen. Dabei werden verschiedene Dimensionen von Katastrophen-, Cyber-, Umwelt-, Governance- (ESG), geopolitischen, finanziellen und Sanktions- bzw. Restriktionsrisiken berücksichtigt.
Cyber Quant	Cyber Quant bewertet den Reifegrad Ihrer Sicherheitspraktiken und priorisiert sie entsprechend ihrer geschäftlichen Auswirkungen, indem es die potenziellen finanziellen Auswirkungen von Cybersecurity-Risiken berechnet.
Cyber Front	Cyber Front simuliert dynamische Cyber-Angriffe, um so kontinuierlich Sicherheitslücken und Fehlkonfigurationen zu erkennen und zu beheben. Cyber Front gibt Antworten auf wichtige Fragen zum Schutz Ihres Unternehmens.

Zielgruppe DORA- und NIS2-regulierte Unternehmen und KMUs

RiskRecon

Identifiziert und priorisiert Cyber-Risiken in Ihren Geschäftsbeziehungen mit Drittanbietern

Wenn jedes Unternehmen auf Dutzende oder sogar Hunderte von Drittanbietern und Zulieferern angewiesen ist, mag es nicht überraschen, dass 59 % der Unternehmen von einer Datenschutzverletzung durch einen Drittanbieter betroffen sind.[1] RiskRecon hilft dabei, das Risiko durch Drittanbieter zu minimieren, indem das Programm die Cyberumgebung von Unternehmen mit einer Online-Präsenz proaktiv überwacht und mögliche Schwachstellen identifiziert, bevor Kriminelle sie ausnutzen können.

Beziehungen mit Drittanbietern setzen Ihr Unternehmen einem erhöhten Cyber-Risiko aus

$10,5 Bio.

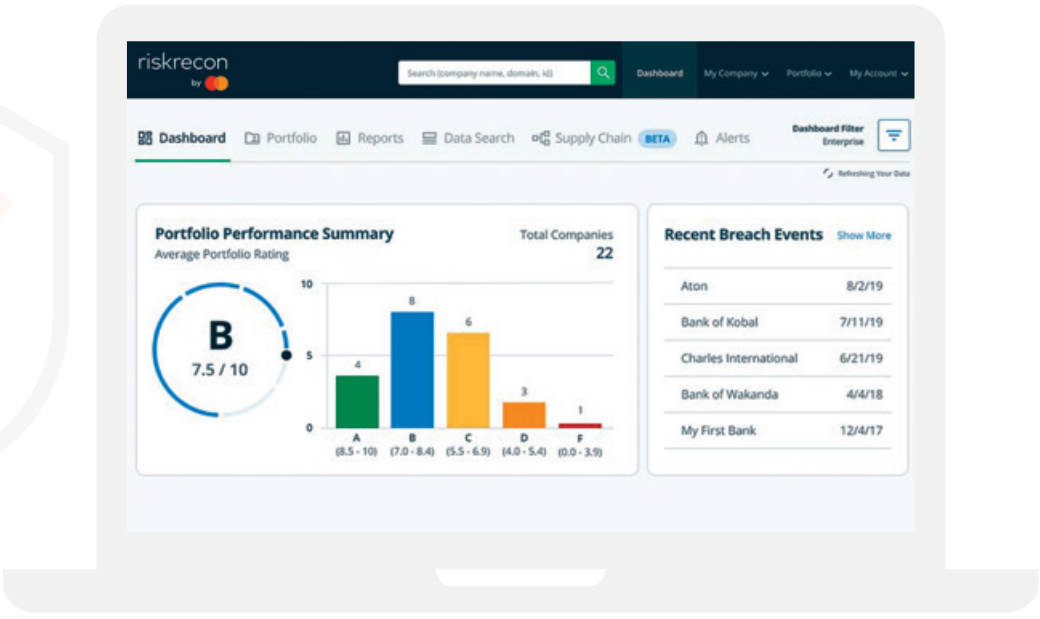
Geschätzte jährliche Kosten der weltweiten Cyberkriminalität[2]

Die Überwachung der Cyber-Risiken durch Drittanbieter kann unzuverlässig, kostspielig und zeitaufwändig sein

40 X

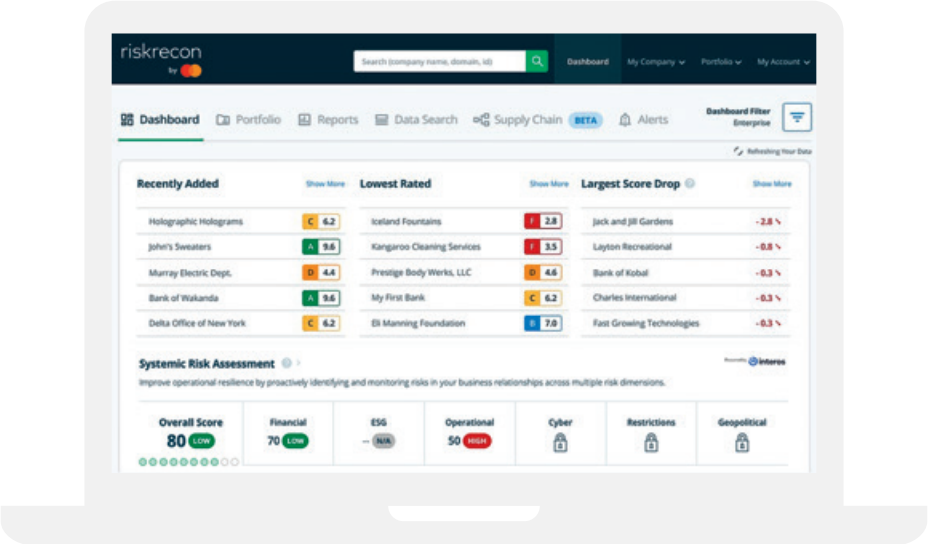
Die Wahrscheinlichkeit, Opfer von Ransomware zu werden, ist 40-mal geringer, wenn Unternehmen über eine gute Cybersicherheitshygiene verfügen[3]

RiskRecon Dashboard liefert Ihnen eine Risikobewertung auf der Grundlage von neun Sicherheitsbereichen und vergleicht Ihre Cyberhygiene mit der Ihrer Wettbewerber.



1. Ponemon Institute, Data Risk in the Third-Party Ecosystem, gefördert durch Opus, 2018
2. Cybersecurity Ventures - Cyber Warfare in the C-Suite 2022 Report
3. Cybersecurity Ventures Ransomware Market Report 2022

Bewerten Sie effektiv Ihr Cyber-Risiko durch Drittanbieter



- Aggregierte Einstufung des **Cyber-Risikos** für alle bewerteten Drittanbieter und externen Dienstleister
- **Warnmeldungen** bei Problemen, die Risikoschwellen überschreiten
- Detaillierte **Berichte** über alle aufgedeckten Sicherheitslücken zum Herunterladen
- **Benchmarking** von externen Dienstleistern und Drittanbietern anhand standardisierter Compliance-Richtlinien und untereinander
- **Umsetzbare Risikopläne**, die über das Kollaborationsportal leicht mit externen Dienstleistern und Drittanbietern ausgetauscht werden können
- **Aggregierte Scores des systemischen Risikos, die über alle Geschäftsbeziehungen hinweg für finanzielle, ESG- und operative Risikodimensionen über Mastercard Systemic Risk Assessment** (zusätzliche Produktfunktion, die in RiskRecon eingebunden werden kann) **ausgewertet werden**

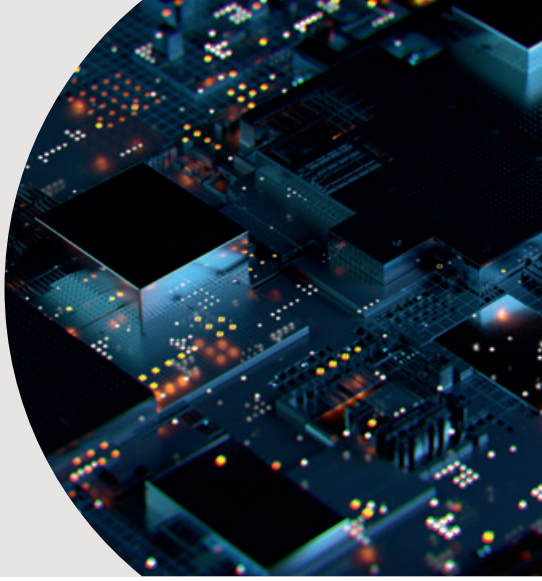
Präzise, automatisierte Risikobewertungen helfen, Verluste zu reduzieren und gleichzeitig Zeit und Ressourcen bei der Behandlung von Cyber-Risiken einzusparen.

1. **Verringerung finanzieller Verluste** durch den Schutz Ihrer Online-Umgebung vor den Gefahren einer Kompromittierung
2. **Mehr Kontrolle und größere Flexibilität** durch die Durchführung von Bewertungen so oft wie nötig bei so vielen Drittanbietern wie nötig
3. **Einsparung von Zeit und Ressourcen** durch automatisierte Risikobewertungen
4. **Zuverlässigere und genauere Bewertungen** durch die Erhebung überprüfter öffentlich zugänglicher Daten
5. Hilft bei der Einhaltung **von Vorschriften**, z. B. DORA, NIS2, ISO-27001, GDPR usw.

RiskRecon ist einfach zu implementieren, da keine Programmierung oder Integration erforderlich ist. Melden Sie sich einfach an und stimmen Sie den Bedingungen in der Anwendung zu, um loslegen zu können.

Cyber Quant

Bewertet und priorisiert Cybersicherheitsrisiken auf Basis der Quantifizierungen von finanziellen Auswirkungen



Cyberangriffe führen zu erheblichen finanziellen Aufwendungen

Zur Verbesserung der Rentabilität von Investitionen in die Cybersicherheit müssen Unternehmen ihre Cyber-Risiken ganzheitlich verstehen. Mastercard Cyber Quant ermöglicht es Unternehmen, ihre Risiken zu reduzieren, indem sie die Fähigkeiten im Bereich der internen Cybersicherheit mit einem beratenden Ansatz bewerten, der umsetzbare Erkenntnisse liefert, die die Bedeutung und die Auswirkungen potenzieller Risiken qualifizieren und quantifizieren.

Cyber Quant verfolgt einen umfassenden, zielgerichteten Ansatz zur Verbesserung der Fähigkeiten Ihres Unternehmens im Bereich Cybersicherheit und stellt Optionen vor, die Investitionsentscheidungen und Ressourcenzuweisungen verbessern.

Wissen Sie, welche der Sicherheitslücken das größte Risiko für Ihr Unternehmen darstellen?

Identifizieren Sie kritische Sicherheitslücken, indem Sie den Reifegrad von über 50 Cybersicherheitsfähigkeiten und die Bedeutung jeder einzelnen bewerten.

Wie hoch ist das finanzielle Risiko von Sicherheitsverletzungen für Ihr Unternehmen?

Quantifizieren Sie unternehmensspezifische Cybersicherheitsrisiken und berechnen Sie die potenziellen finanziellen Auswirkungen eines Sicherheitsverstoßes.

Wie entscheiden Ihre Unternehmens- und Sicherheitsverantwortlichen, wo sie investieren sollen?

Priorisieren Sie die nächsten Schritte zur Verbesserung der Sicherheitslage und zur Verringerung des Risikos, indem Sie Simulationen durchführen, um die Maßnahmen mit dem größten ROI zu ermitteln.

Cyber Quant liefert Ihren Cyber-Risiko-Score, berechnet die finanziellen Auswirkungen des Cyber-Risikos und priorisiert die nächsten Schritte in nur drei Wochen*.

Das Team von Mastercard arbeitet mit dem Kunden zusammen, um eine schnelle und ganzheitliche Risiko-bewertung seines Cyber-sicherheitsprogramms in ca. 3 Wochen mit Unter-stützung durch den Kunden durchzuführen (insgesamt 20-30 Stunden).

Woche 1
Projektbeginn und Datenerfassung

Überprüfung der folgenden Punkte in einer dreistündigen Online-Sitzung:

- Gesamtengagement
- Fragebogen
- Skripte für die Erhebung technischer Daten
- Modell zur Risikobewertung
- Beschreibungen der Ergebnisse

Woche 2
Bewertung und Analyse

Durchführung der folgenden Schritte, um die Bewertung abzuschließen:

- Überprüfung von 51 Kriterien im Bereich der Cybersicherheit durch Meetings
- Überprüfung der Bewertung im Hinblick auf technische Genauigkeit
- Abgleich der Ergebnisse mit Bedrohungsinformationen
- Auswertung der Ergebnisse mithilfe von Simulations-modellen

Woche 3
Zusammenfassung und detaillierter Bericht

Bestimmung des Risiko-Scores und der finanziellen Auswirkungen:

- Zuweisung eines Reifegrads der Kontrollen und finanziellen Auswirkungen
- Abbildung von Kontroll-abhängigkeiten
- Vorbereitung der Abschluss-berichte zur Überprüfung
- Bereitstellung von Risiko-bewertungen, finanziellen Auswirkungen und Berichten auf Führungsebene

*Cyber Quant Essentials erster Bewertungszyklus

Cyber Front

Ein umfassender, risikoorientierter Ansatz für Investitionen in die Cybersicherheit

Was macht Cyber Front?

- Bewertet den Reifegrad von Cybersecurity-Tools bzw. -strategien und deren Bedeutung auf Grundlage der jeweiligen Bedrohungen
- Quantifizierung der Cybersicherheitsrisiken in Bezug auf die Größe, den Umsatz, die Region, die Branche und spezifische Risikopunkte des Kunden
- Bewertung der potenziellen finanziellen Auswirkungen von Cybersicherheitsrisiken für die verschiedenen Vermögenswerte

Simulation von dynamischen Cyberangriffen auf die Produktionsumgebung, ohne die Produktionssysteme zu beeinträchtigen, um Sicherheitslücken und Fehlkonfigurationen kontinuierlich zu identifizieren und zu validieren, Reaktionen zu definieren und Ihren Schutz zu verbessern.

Identifikation und Abwehr der wichtigsten Bedrohungen für Ihr Unternehmen mit Penetrationssimulationen.

- Überprüfung, **ob die Sicherheitsinfrastruktur, Konfigurationseinstellungen und Präventionstechnologien wie beabsichtigt funktionieren**
- **Kontinuierliches Testen** der bestehenden Sicherheitsinfrastruktur, ohne dass auf eine Sicherheitslücke zum Scannen von Schwachstellen gewartet werden muss
- Ermittlung der **Wahrscheinlichkeit eines Risikos** durch die Identifizierung von Bedrohungen und Angriffsvektoren
- Gewährleistung, dass das Sicherheitspersonal und die Einsatzkräfte bei **Cyber-Response-Übungen Angriffe erkennen und entsprechend reagieren können**

Arbeitsweise:

Das Team von Mastercard arbeitet mit dem Kunden zusammen, um die Plattform einzurichten, die fortlaufende Tests zur Simulation von Sicherheitsverletzungen und Angriffen auf der Grundlage von mehr als 7.600 einzigartigen Bedrohungen und mehr als 500 einzigartigen Szenarien ermöglicht, was zu einer besseren Identifizierung relevanter Bedrohungen führt.

1. Cyber Front berücksichtigt >7.600 Bedrohungen, die täglich aktualisiert werden
2. Simulierter bösartiger Datenverkehr wird an den Cyber Front Agent gesendet
3. Verbliebener unentdeckter Verkehr wird an den Cyber Front Simulator gemeldet

4. Die getesteten Arten von Sicherheitsverletzungen und Angriffsszenarien sowie die Ergebnisse dieser Tests und die Empfehlungen zur Abhilfe können über das Cyber Front Dashboard abgerufen werden

Bei Cyber Front tragen die Simulationsübungen dazu bei, aktuelle Bedrohungen aufzudecken, denen die Kunden ausgesetzt sind, die durch Fehlkonfigurationen und Schwachstellen, die ausgenutzt werden können, verursacht werden, was zu einer Verringerung des Cyber-Risikos, geringeren Kapital- und niedrigeren Betriebskosten führt.

ethoca by Mastercard

Ethoca Alerts

External Summary • Merchants • Global

Ethoca Alerts ist ein kollaboratives Tool, das Issuer und Händler miteinander verbindet, um Betrugs- und Streitfalldaten auszutauschen und so die Notwendigkeit von Chargebacks zu reduzieren.

$7.3 bill

Globaler E-Commerce Umsatz prognostiziert für 2025[1]

Ausgangssituation

Das Wachstum des E-Commerce führt zu einer stetigen Zunahme von Chargebacks, was Betrug zu einer ständigen Herausforderung macht.

24%

der Verbraucher haben in den letzten 12 Monaten einen Kauf hinterfragt, weil sie ihn nicht erkannt haben[2]

Bis zu $70

Streitigkeiten kosten Händler $15 bis $70 an Betriebskosten[3]

$28 mrd

globale CNP Fraud Verluste erwartet bis 2026[1]

Ergebnis

30m+

Ethoca Alerts hat in den letzten 12 Monaten über 30 Millionen Chargebacks verhindert[4]

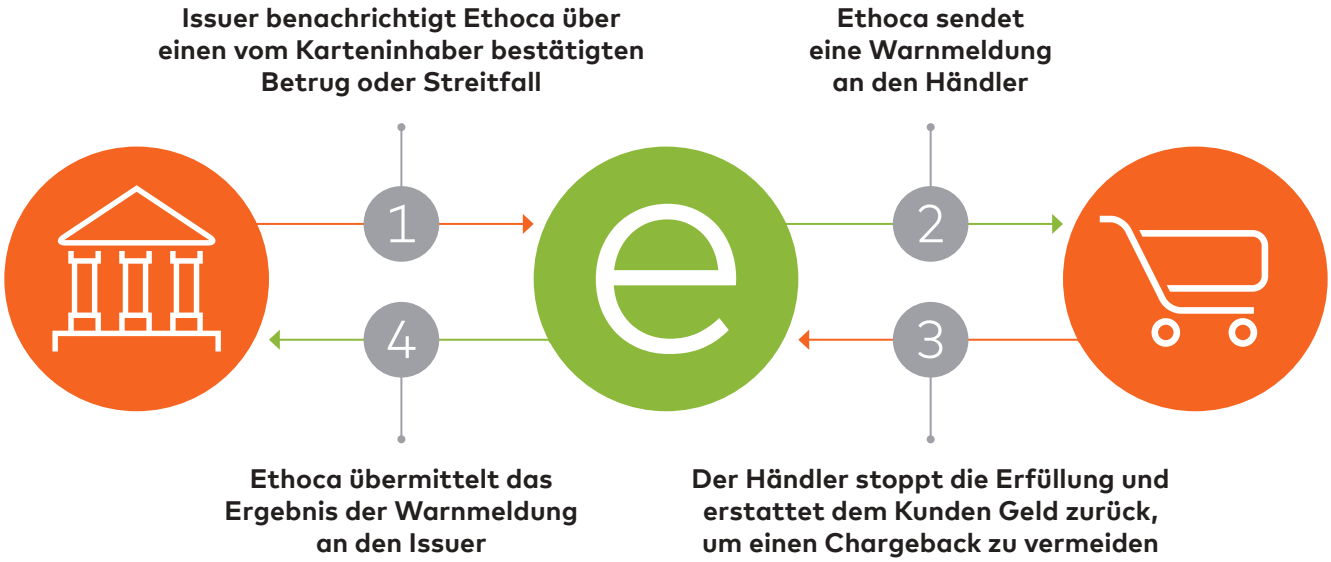
Handlungsbedarf

Ethoca Alerts ermöglicht es Händlern, die Ausführung von Bestellungen schnell zu stoppen, Gutschriften auszustellen und Chargebacks zu verhindern.

1. Ethoca. Chargeback trends and out look. 2023.
2. Datos Insights. Digital Banking and Consumer Clarity: Q4 2023 Survey Findings.
3. https://b2b.mastercard.com/news-and-insights/blog/what-is-a-chargeback/
4. Internal Data. Time period covers September 2023 – September 2024.

HOW IT WORKS

Ethoca Alerts stellt sicher, dass relevante Issuer Informationen schnell an Händler weitergegeben werden.



Durch die Weitergabe von Streitfalldaten ermöglichen Issuer den Händlern:

- Die Bestellung zu stoppen/den Dienst auszusetzen
- Eine Rückerstattung oder Gutschrift an den Kunden vorzunehmen (was einen Chargeback überflüssig macht)
- Mehr betrügerische Transaktionen durch eine Linkanalyse zu erkennen
- Betrugsregeln zu aktualisieren, um zukünftigen Betrug zu verhindern

Vorteile

- **Betrugs-bekämpfung**
- **Chargebacks verhindern**
- **Akzeptanz erhöhen**
- **Zukünftigen Betrug reduzieren**
- **Ähnliche Betrugsmuster erkennen**
- **Zufriedenheit steigern**

Let's get started

Für weitere Informationen wenden Sie sich bitte an Ihren Mastercard-Kundenbetreuer.

Identity Insights for Transactions API

Gewinnen Sie umfassende Einblicke, die Unternehmen dabei helfen, das Routing von Transaktionen zu optimieren, die Entscheidungsfindung vor der Authentifizierung und nach der Autorisierung zu verbessern und gleichzeitig Betrug zu bekämpfen und die Kundenerfahrung insgesamt zu verbessern.

Mastercard Identity Insights for Transactions stärkt das Vertrauen von Unternehmen in die Authentifizierung und Autorisierung von Transaktionen

Mit Mastercard Identity Insights for Transactions (IIT) können Sie risikoorientierte Entscheidungen mit größerer Sicherheit treffen – mittels einer einzigen API. Mit einer einzigen API erhalten Sie die Fähigkeit, das „Wer" und das „Was" hinter einer Transaktion mit umfassenden Identitäts- und Geräteinformationen zu verstehen.
Auf der Grundlage von Milliarden globaler Datenelemente, darunter Einblicke in digitale Transaktionen, ermöglicht es IIT den Teams, endlich das Gleichgewicht zwischen Haftungsverschiebungen, niedrigen Betrugsraten und einem hervorragenden Kundenerlebnis zu finden.

Souveräne Risikoentscheidungen

Verbessern Sie Risikobewertungen und die Entscheidungsfindung mit einem vollständigen Überblick über jede Transaktion.

Minimieren Sie die Kundenfriktion

Beseitigen Sie unnötige Kundenfriktion für Transaktionen mit geringerem Risiko oder erhöhen Sie diese, wenn nötig.

Gewinnen Sie bessere Kunden

Erhöhen Sie die Transaktionssicherheit und den langfristigen Kundenwert durch verbesserte Identifizierung.

Verringern Sie Chargebacks

Verringern Sie das Risiko für Acquirer, indem Sie die Betrugsrate in deren Händlerportfolio durch Modelle oder Regeln niedrig halten.

$11 Mrd.

Geschätzte Verluste bei Händlern durch fehlerhafte Ablehnungen.[1]

51 %

Unternehmen geben an, in den letzten 2 Jahren von Betrug betroffen gewesen zu sein. Das ist der höchste Wert in den 20 Jahren der PWC- Marktforschung.[2]

$15,3 Mrd.

Geschätzte weltweite Verluste durch CNP-Betrug im Jahr 2021.[3]

1. E-Commerce Fraud Enigma: The Quest to Maximize Revenue While Minimizing Fraud Report, Aite-Novarica Group, July 2022
2. PwC's Global Economic Crime and Fraud Survey 2022
3. Aite Research Group, Maximizing the Potential of CNP. Okt 2021

Mehr Vertrauen bei Entscheidungen zum Transaktionsrisiko durch prädiktive Signale und Scores

Identitätsrisiko-Score
Wie risikoreich ist diese Transaktion?

Netzwerk Score
Wie werden die Daten verwendet?

IP-Risiko-Score
Deutet diese IP-Adresse auf ein Risiko hin?

Device Risiko-Score
Wird dieses Gerät mit Betrug in Verbindung gebracht?

Device Vertrauensscore
Sind die Einstellungen des Geräts authentisch?

Device Insights Score
Sehen wir hohe Velocity oder Automatisierung?

E-Mail

- Ist gültig
- Passt zum Namen
- Zum ersten Mal beobachtet vor Tagen
- Zuletzt beobachtet vor Tagen
- Registrierungsdatum der Domain

Telefon

- Ist gültig
- Passt zum Namen
- Anschlussart
- Anbieter

Adresse

- Valide Adresse?
- Passt zum Namen
- Zum ersten Mal beobachtet vor Tagen
- Zuletzt beobachtet vor Tagen
- Beziehung zwischen Rechnungsstellung und Auslieferung

IP

- Verbindungstyp
- Zuletzt beobachtet vor Tagen
- Entfernung von der Anschrift
- Geolokalisierung
- Anbieter

Gerät

- Geräteart
- Browser
- Plattform
- Risikohistorien
- Eindeutige Device-ID

Beispiel für den Ablauf der Vorauthentifizierung

1. Der Verbraucher initiiert die Transaktion mit dem Händler.
2. Der Händler fragt die Mastercard Identity Insights for Transaction API direkt oder über einen Partnerkanal ab, um Informationen über die Identität und das Gerät einer Transaktion zu erhalten.
3. Die Informationen werden bei Risikoentscheidungen genutzt, um zu bestimmen, wie mit der Transaktion verfahren werden soll.
4. Je nach Risikoentscheidung wird die Transaktion zur Autorisierung weitergeleitet, durch die Authentifizierung geroutet oder überhaupt nicht bearbeitet.

Identity Insights for Accounts

Dynamische Identitätsdaten zur Optimierung des digitalen Onboardings und zur Prävention von Betrug bei neuen Konten

Gleichgewicht zwischen den Zielen der Kundenakquise und der Betrugsbekämpfung durch Hinzufügen von dynamischen individuellen und gerätespezifischen Erkenntnissen und prädiktiven Signalen zu Ihrem digitalen Kontoeröffnungsworkflow.

Verbraucher auf der ganzen Welt erwarten eine schnelle und einfache digitale Kontoeröffnung.

3 von 5

Verbraucher wechseln nach nur einer schlechten Online-Erfahrung zu einem Mitbewerber.[1]

5 Min.

ist der Punkt, an dem Abbrüche von digitalen Bankanwendungen sprunghaft ansteigen.[2]

70 %

der Verbraucher wollen Finanzkonten online eröffnen, insbesondere in wachsenden Volkswirtschaften.[3]

68 %

der europäischen Verbraucher haben im letzten Jahr einen Online-Antrag abgebrochen, während es 2020 noch 63% waren.[4]

Statische, isolierte Daten beeinträchtigen Unternehmen und Verbraucher gleichermaßen

$56 Mrd.

Verluste durch Identitätsbetrug allein in den USA im Jahr 2020.[5]

37 %

der Budgets von Betrugsbekämpfungsteams werden für manuelle Überprüfungen ausgegeben.[6]

>55 %

der Verbraucher, die einen neuen Kredit aufnehmen, sind weltweit über 30 Jahre alt.[7]

1. Zendesk Global Customer Experience (CX) Trends Report, 2023)
2. Signicat Battle to Onboard Report, 2022
3. Fico Accelerated Digital-First Mindset, August 2021
4. Bankrate Consumer Survey, December 2021
5. Javelin 2021 Identity Fraud Study
6. The 2021 MRC Global Fraud Survey
7. Transunion Global Research, 2023

IDENTITY INSIGHTS FOR ACCOUNTS

Device Intelligence, persönliche Attribute, Prognosen und Scores in einer einzigen API.

Hauptmerkmale

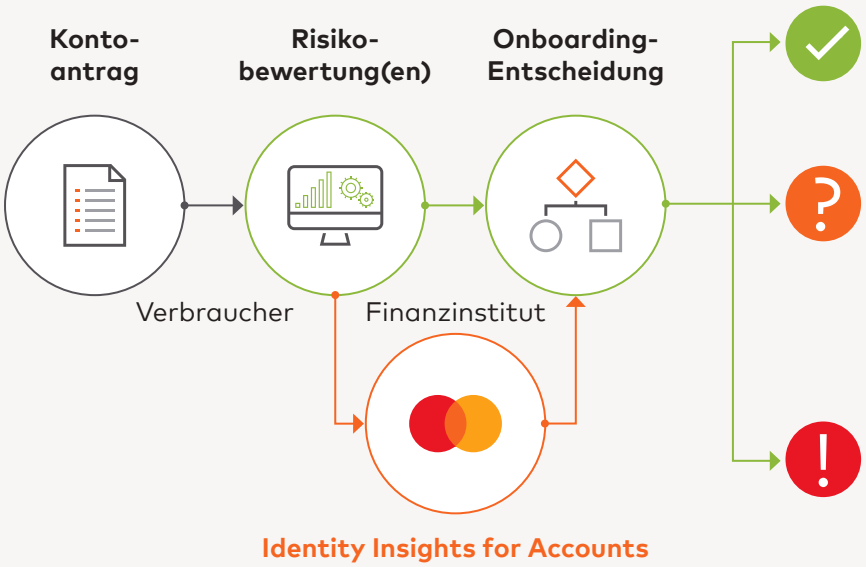
- Prädiktive Scores und auf die Kontoeröffnung zugeschnittene Metadaten
- Validitäts- und Velocity- Checks von Datenelementen und Nutzungsmustern
- Globale, dezentrale Daten und Signale
- Prüfungen der Geräteauthentizität und Automatisierung
- Individueller API-Aufruf und Rückmeldung
- Geräte- und plattformunabhängig

Hauptvorteile

- Vertrauen Sie Ihren Neukunden mit möglichst geringem Risiko und erleichtern Sie somit das Onboarding neuer Kunden
- Steigern Sie die „Financial Inclusion" einer größeren Anzahl von Kunden, auch von Antragstellern, über die wenige Daten verfügbar sind
- Erkennung und Vermeidung von Geräte-Spoofing und synthetischen Identitätsmustern zu einem früheren Zeitpunkt im Prozess der Kontoeröffnung

Arbeitsweise

Sie stellen uns die Details zu den Anwendungen und Geräten zur Verfügung, wir liefern Ihnen die wichtigsten Informationen, damit Sie das Risiko der Bewerber sicher einschätzen können – ohne unnötige Reibungsverluste.



Beispiele für optimiertes Onboarding

Antragsteller mit geringem Risiko

- Geringste Reibungsverluste
- Erlaubnis zum Zugriff auf das Konto vor der KYC-Prüfung

Antragsteller mit mittlerem Risiko

- Erfordernis zusätzlicher Schritte für weitere Verifizierungen (biometrisch, Selfie usw.)
- Eingeschränkter Zugriff auf das Konto, bis die KYC-Prüfung abgeschlossen ist

Antragsteller mit hohem Risiko

- Dokumentanforderungen und manuelle Überprüfungen
- Ablehnung des Antrags

Identity Insights for Login Behavior

Kontoübernahmen verhindern, bevor sie passieren

Kontoübernahmebetrug gefährdet den sicheren und nahtlosen Zugriff auf ein digitales Konto

Es stellt digitale Unternehmen vor große Herausforderungen, wenn sie versuchen, ein sicheres und nahtloses Benutzererlebnis zu schaffen.

73 % der Verbraucher sind der Ansicht, dass Unternehmen für Angriffe mit dem Ziel, Konten zu hacken, und den Schutz von Zugangsdaten verantwortlich sind[1]

12,9 Mrd. Online-Konten wurden weltweit seit 2013 kompromittiert

1 von 4 Anmeldeversuchen ist ein Angriff zum Stehlen von Nutzerinformationen

17 Mrd. Der voraussichtliche Wert der weltweiten Schäden aufgrund von Kontoübernahmen im Jahr 2025

Das Verhindern und Aufspüren von Versuchen zur Übernahme von Konten zahlt sich aus

Optimierte Leistung

Verhindern Sie, dass Betrüger Traffic-Spitzen und Serviceunterbrechungen verursachen

Weniger Chargeback

Vermeiden Sie finanzielle Verluste durch betrügerische Käufe

Geringere Gefährdung

In einer zunehmend digitalen Welt wird es immer schwieriger, Reputationsverlust aufgrund von Hacking-Schlagzeilen zu verhindern

Erhöhte Loyalität

Mehr Sicherheit und weniger Reibungsverluste führen zu mehr zufriedenen Kunden, die bleiben

1. SpyCloud, 2023 Cybersecurity Industry Stats.
https://haveibeenpwned.com/ (January 2024)
Arkose Lans, Economics of Account Takeover Attacks
HUMAN 2023 Enterprise Bot Fraud Benchmark Report

IDENTITY INSIGHTS FOR LOGIN BEHAVIOR

Schaffen Sie ein überzeugendes Benutzererlebnis, das Ihre Kunden schon ab der ersten Anmeldung und jedes Mal danach schützt. Nehmen Sie mit Hilfe von Mastercard's Echtzeitdaten Risikobewertungen vor und überwachen Sie das Kundenverhalten.

Login Behavior bietet Informationen zur Erkennung bösartiger Aktivitäten und verdächtiger Automatisierung, sodass Sie eingreifen und verdächtiges Verhalten möglicherweise abwenden können, noch bevor Benutzerkonten kompromittiert werden.

Wie schützen die spezialisierten Daten von Login Behavior Unternehmen vor bösartigen Akteuren?

Analysieren Sie Details zum Standort

Bösartige Akteure verschleiern in der Regel ihre IP-Adresse, sodass dies ein wichtiges Indiz für die Aufdeckung von Betrug ist. Verwenden Sie unsere Daten, um die Geolocation der IP mit der Zeitzone des Geräts zu vergleichen.

Beobachten Sie das Verhalten Ihrer Kunden

Untersuchen Sie die Aktivität, z. B. wie ein Benutzer seinen Benutzernamen und sein Passwort eingibt.
Bösartige Akteure arbeiten mit wiederholten Eingabemustern, was schnell erkannt wird.

Definieren Sie Geräteattribute

Die meisten Betrüger nutzen die gleiche Umgebung, um ihre Betrügereien zu begehen. Verwenden Sie Daten, um zu vergleichen, ob dasselbe Gerät oder dieselbe IP-Adresse als Quelle für die Anmeldung bei mehreren Konten verwendet wird.

Messen Sie die Velocity der Kundenaktivität und erkennen Sie Anomalien

Überwachen Sie unsere Daten, um festzustellen, ob es verdächtige Eingabewerte gibt, die auf Automatisierung hindeuten.
Auf diese Weise lassen sich Anomalien erkennen, die mehrfache Anmeldefehler kennzeichnen.

Damit Ihre Systeme und Prozesse sicher, geschützt und resilient bleiben

Vielfältiges, globales Netzwerk

Wir nutzen **machine learning** in den Bereichen digitales Banking, digitale Güter, Retail und vielem mehr

Intelligenz nach Maß

Unsere **einzigartigen Risikobewertungen** beruhen auf Milliarden von Gerätedaten, Verhaltens-signalen und Netzwerk-informationen

Privacy by Design

Wir erfassen nur die **minimal erforderlichen Daten** und speichern sie sicher und in Übereinstimmung mit den regionalen Anforderungen

Die ersten Schritte sind ganz einfach...

Kontaktieren Sie uns, wenn Sie mehr über die DORA u. NIS-2 Lösungen von Mastercard erfahren oder unsere Lösungen im Rahmen eines Proof of Concept testen möchten.

Martin Penzes
Director Products & Solutions

E-Mail: martin.penzes@mastercard.com
Mobil: +43-676-362-8240