Always moving forward

Advancing a digital future for the freight and logistics ecosystem

About Mastercard

"We work to connect and power an inclusive digital economy that benefits everyone, everywhere by making transactions safe, simple, smart and accessible. Using secure data and networks, partnerships and passion, our innovations and solutions help individuals, financial institutions, governments and businesses realize their greatest potential. Our decency quotient, or DQ, drives our culture and everything we do inside and outside of our company."

Who we serve

Consumers

Small & medium businesses

Governments & public sector

Large enterprises

Banks & credit unions

Evolution of commerce

Commerce

eCommerce/mCommerce

Quick Commerce

AI Generated Image

"It is about the science of getting the right product to the right place, at the right time in the right condition, and at the right cost."

"The COVID-19 pandemic has revealed the global and immediate nature of our modern economy, and how reliant it is upon a worldwide supply chain"

Source: https://www.thebusinessresearchcompany.com/report/freight-and-logistics-global-market-report and https://www.mastercard.com/global/en/business/large-enterprise/mastercard-enterprise-partnerships/global-trade-freight-solutions/freight-whitepaper.html

5.5%

CAGR growth as a sector 2024 to 2033

90%

of everything we consume is shipped by sea that was transported via a port

28

times on average a consignment owner or shipper interacts with different entities.

1/2

of all global business transactions are still manual and paper based, costing the trade ecosystem over $500B each year

50%

of the cost of trade is linked to Document processing

Advancing a digital future for the freight and logistics ecosystem

Digital business models and automating manual processes could reduce back-office and operations costs by up to 40%

The digitization of port ecosystems

1. From straightforward replacements of cash-against-documents processes
2. Integrating payment systems within these digital automation projects can further drive efficiency
3. Enabling real-time payment confirmation
4. Increased transparency in payment events

Improving invoice accuracy, reducing disputes

1. Hyper-automation technology revolutionizes the Freight Audit sector and significantly improves invoice accuracy while reducing disputes.
2. Enhances transparency and accuracy in freight invoicing with minimal impact on legacy systems
3. Transforms vendor relationships
4. Delivers substantial return on investment.

Embedding payment and financing into workflow automation

1. Embedding payments and financing into workflow automation enhances efficiency in the procure-to-pay process
2. Improves reconciliation and reduces collections effort
3. Links embedded finance to payment events, extending value propositions to the freight ecosystem
4. Uses a global network of financial institutions to open access to new capital sources.

Data driven insights can optimize outcomes

1. Data-driven insights can optimize outcomes by improving supply chain decisions
2. Nearly all logistics experts interviewed by Accenture in 2021 expressed concerns over the lack of data capabilities, visibility, and insights
3. Establishing standards and sharing secure data across the trade ecosystem can provide all parties with information on progress, impact, and accountability
4. This transparency leads to better decisions, increased

Mastercard initiatives in advancing a digital future for the freight and logistics ecosystem

DIGITAL INDUSTRIES EUROPE OPERATORS OCTOBER 10, 2024

Vodafone JV, Mastercard target logistics with tie-up

Vodafone Group and Sumitomo Corporation's JV Pairpoint partnered with Mastercard to launch a machine-to-machine (M2M) autonomous payments system for logistics industry.

Technology Integration

- Pairpoint's platform integrates with Mastercard's global payment processing system, Mastercard Gateway
- Aims to authorize transactions between vehicles and other machines

Target Audience

- Fleet operators
- Freight operators
- Shipping operators
- Logistics operators

System Capabilities

- Direct vehicle payments at designated charging or fuel stations
- Pre-approved transactions along a route for freight companies
- Includes port storage and terminal handling fees

Source: https://www.mobileworldlive.com/industry/vodafone-jv-mastercard-target-logistics-with-tie-up/

Dubai Ports World and Mastercard

Enterprise Partnership & MEA Government Engagement

(Middle East & Africa briefly)

69 countries with a population of 1.7Bn

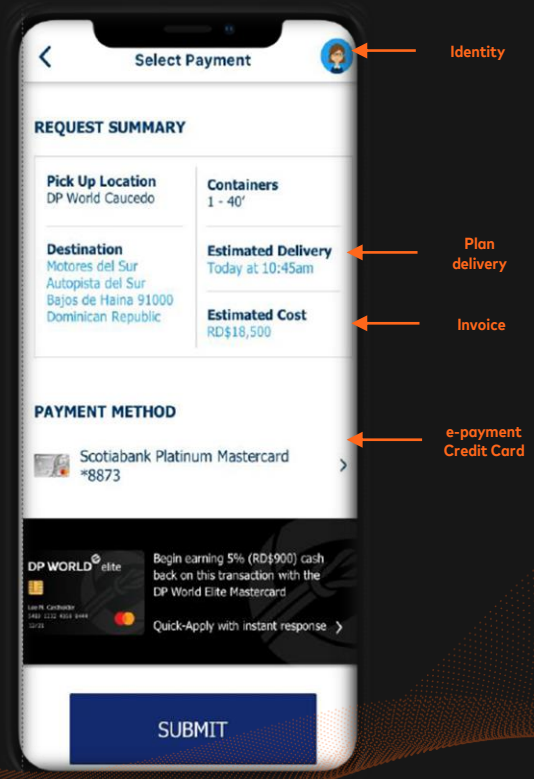
Resource rich region – 75% of OPEC's oil, 99% of the world's chromium, 68% of cobalt and 54%of gold

Young and connected – 10 youngest countries in the world with 85%+ mobile penetration(45%+ smart phone)

High Mobile Money penetration –445M mobile money accounts vs. 286M bank accounts

Highly diverse – home to the richest (Qatar) and poorest(Somalia) country in the world

Key products: Debit, Services, QR



In May 2020, DP World (DPW) and Mastercard announced the launch of a program to digitize port ecosystems payments

The enouncement was a major milestone in the 18-month collaboration between Mastercard and DP World

The outcome reflected an internal team partnership between Enterprise Partnerships, the Government Engagement team as well as regional product and country account teams

The program was launched in the Dominican Republic as the Trade Card to facilitate payment services at its terminals and logistics partners for SME customers

The plan is to scale the program to other key port terminals in Asia, Middle-East and Africa as well as other markets in Latin America & Caribbean

Some of our partners

DP WORLD RAISTONE CAPITAL FINASTRA


Threat Protection

LANDSCAPE

Malicious cyberattacks are on the rise, leaving organizations vulnerable to devastating cyber events

Businesses of all shapes, sizes and industries struggle to defend against growing threats and challenges:

- Trouble identifying risks
- Fear of losing private data
- Implementing the right security tools that will not interrupt business processes
- Inadequate labor resources to create more secure measures
- Compliance and regulatory pressures regarding application, network and data security

$4.45m

The average cost of a data breach reached an all-time high in 2023[1]

277

days on average required to identify and contain breaches[1]

1 in 3

Only 1/3 of companies discovered the breach through their own security teams[1]

1. IBM, Cost of a Data Breach Report 2023.

IMPACT

Security challenges are growing in the era of digital and cloud transformation

Financial Loss

In 2023, the average cost of a data breach on a small company was $3.3 million and for enterprises $5.4 million.[1]

1

Reputation Damage

Reputation harm can take away years of investments. 52% of breaches in 2023 involved some form of customer personal identifiable information (PII).[1]

2

Operational disruption

25% of destructive attacks left organizations' systems inoperable.[1] Such disruptions, and attacks on business and software supply chains, can cripple a business.

3

Sophisticated Attacks

Hackers and data miners continue to become more sophisticated. Distributed Denial of Service (DDoS) attacks rose 15% in only 6 months, from 1H to 2H 2023.[2]

4

1. Small company: <500 employees; enterprise: >25K employees. IBM, Cost of a Data Breach Report 2023.
2. NETSCOUT, DDoS Threat Intelligence Report, Issue 12, 2H 2023.

What are DDoS attacks?

DDoS attacks occur when a hacker uses a bot-network to flood a website/network with traffic or requests until it crashes.

Who?

DDoS attacks are often conducted by actors from the categories:

- Hactivist
- Nation-state sponsored actor
- Financially motivated actors
- Competitors and disgruntled staff/customers/...

Why?

Reasons for them attacking varies from:

- Creating physical, digital or financial harm/gains
- Society or societal harm
- Reputational harm
- Data theft
- Way to breach system to implement malware

What are web application attacks?

Web app attacks occur when a hacker utilizes vulnerabilities in the application or OS to either break it, to gain access to the server or data stored on the server.

Who?

Web application attacks are often conducted by these actors:

- Financially motivated actors
- Hactivist
- Nation-state sponsored actor

Why?

Reasons for them attacking varies from:

- Extortion / financial gain
- Data theft (often to sell data on darkweb or ransom)
- Reputational harm
- Creating digital harm / compromise data
- Society or societal harm
- Way to breach system to implement malware

What are bot attacks?

Bots simulate human activity on a computer and are normally used to automate useful tasks. However, some can also be malicious.

Who?

- Cyber terrorists
- Cyber criminals
- Hactivists
- Nation state sponsored

Examples

- Search engine crawlers
- Customer service chatbots
- Pricing bots

- Spam bots
- Malware botnets
- Credential stuffing bots

Why?

- Disrupt service (Denial of Service)
- Spam/fraud
- Credential stuffing/credit card stuffing
- Data/content scraping
- Privelaged access (account take overs)

Current fraud attack vectors

Brute Force Attacks – bots and scripts for large-scale attacks

Authorization Manipulation – circumventing issuer's controls

Scams and Phishing – obtaining card credentials and OTP

Fraudulent Merchants – monetizing fraud attacks efficiently

Scam and Phishing

Threat Protection provides security to a wide range of use cases

Manufacturing
Safeguarding critical infrastructure and business to avoid financial loss and reputational damage.

Government
Countering advanced persistent threats (APTs) and safeguarding critical infrastructure.

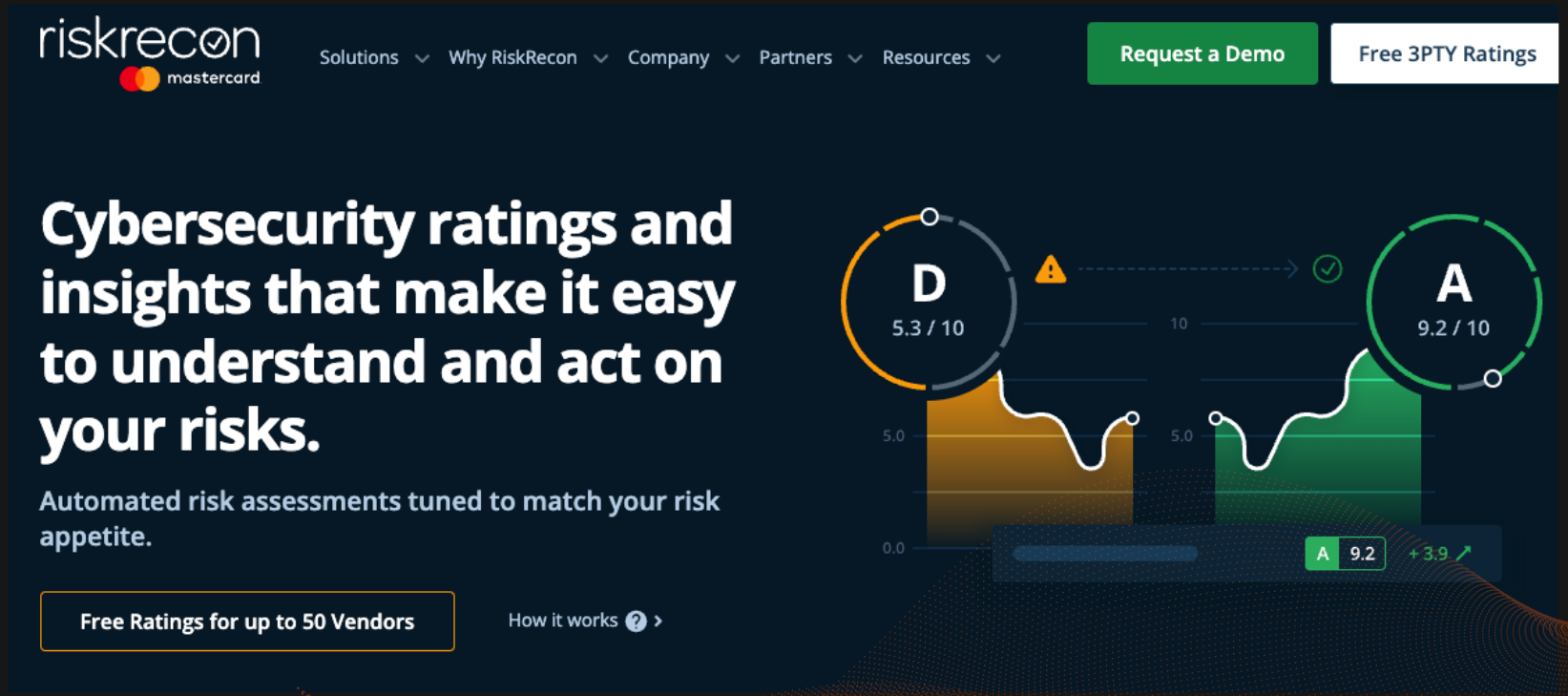
Fintechs and SaaS vendors
Securing cloud infrastructure and enhancing IoT security to prevent privacy breaches and more.

Merchants and e-commerce
Securing business infrastructure while protecting personal data and customer privacy.

Healthcare
Protecting against privacy breaches and safeguarding critical infrastructure.

Financial services
Ensuring compliance with data protection regulations, securing business infrastructure and protecting personal data and customer privacy.

Managing Third-party Risk



HOW IT WORKS

How is the cyber risk rating determined?

The cyber risk rating is determined by evaluating over **40** criteria across **9** security domains. The impact of all vulnerabilities is analyzed to produce the **cyber risk rating**.

An organization's online web link is used as an input

Security assessments

Evaluate security measures in place to combat risks like malware and ransomware

1. Email security
2. Breach events
3. Network filtering
4. DNS security
5. System Reputation

Infrastructure assessments

Assess software and hardware system risks

Web encryption

6. Application security
7. Software patching
8. System hosting

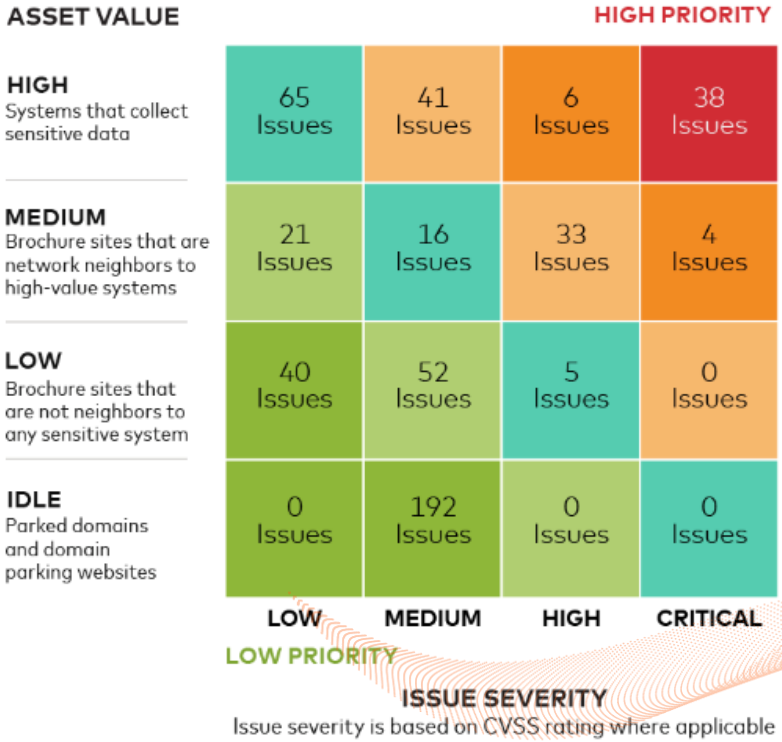
Impact analysis

Analyze the impact each issue uncovered based on its criticality as well as sensitivity of the system where it's identified

Cyber Risk Rating

riskrecon

How It Works



Deep Asset Discovery

Our asset discovery process integrates analyst-assisted machine learning models tailored for each monitored company, ensuring accurate attribution of company assets amid evolving shifts over time.

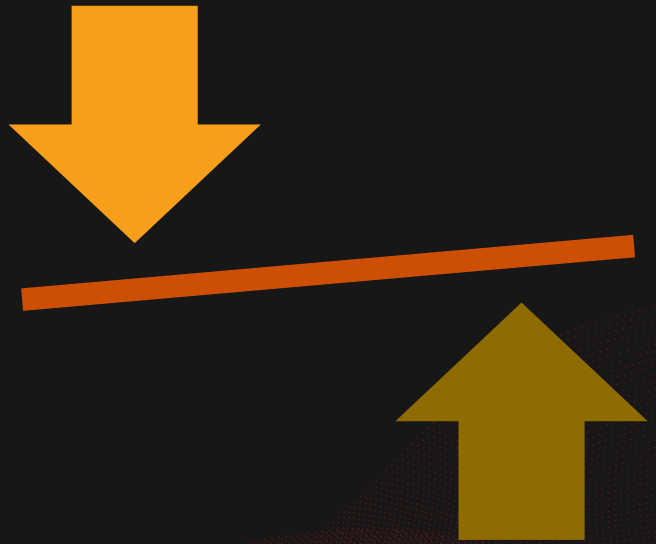
Automated risk prioritization

RiskRecon automatically prioritizes every finding based on issue severity and asset value. The value at risk for each system is determined by discovering:

- authentication
- transaction capabilities
- data types collected include email addresses, credit card numbers & names

Future: Using AI

- Demand Forecasting and Inventory Management
- Route Optimization
- Warehouse Automation
- Warehouse Automation
- Predictive Maintenance
- Customer Experience and Last-Mile Deliver



- Cargo Tracking and Verification
- Anomaly Detection in Transactions
- Document Forgery Detection
- Identity Verification
- Cybersecurity Threat Detection
- Predictive Risk Scoring