Mastercard Trusted Device

How far does your device intelligence go to stop fraud?

97% of all fraud comes from an anomalous device or network but many tools fall short. Enhanced device intelligence blocks that fraud from your environment while recognizing your good customers.

PROBLEM

One Device Away

Your users are one device away from your environment, making this piece of technology the core link. However, most device intelligence technologies recognize devices through cookies that expire in 22–25 days or device fingerprints that have a 40% collision rate.

Common device intel flaws

40%

COLLISION RATE OF DEVICE FINGERPRINT

A device fingerprint uses device attributes (model, operative system, browser plug-ins,...) to build a fingerprint. The collision rate shows how likely it is to see two or more devices with the same fingerprint. Confusing a device for another one has a direct impact on false declines and customer frustration.

22–25 days

THE AVERAGE LIFESPAN OF AN ID THAT RELIES ON COOKIES (LOCATION, CONNECTION, IP...)

Like having a security platform with the memory of a goldfish. It keeps forgetting about good users and high-risk devices every few days.

SOLUTION

Mastercard Trusted Device,
powered by NuData

3-6 months

IS THE AVERAGE LIFESPAN OF THE DEVICE DATA

0%

COLLISION RATE GLOBALLY

Resilient

ACROSS DEVICE BREAKS

NuData Security
mastercard

HOW

Trusted Device looks at the device data from three angles:

1 **USER AGENT COMPARISON**

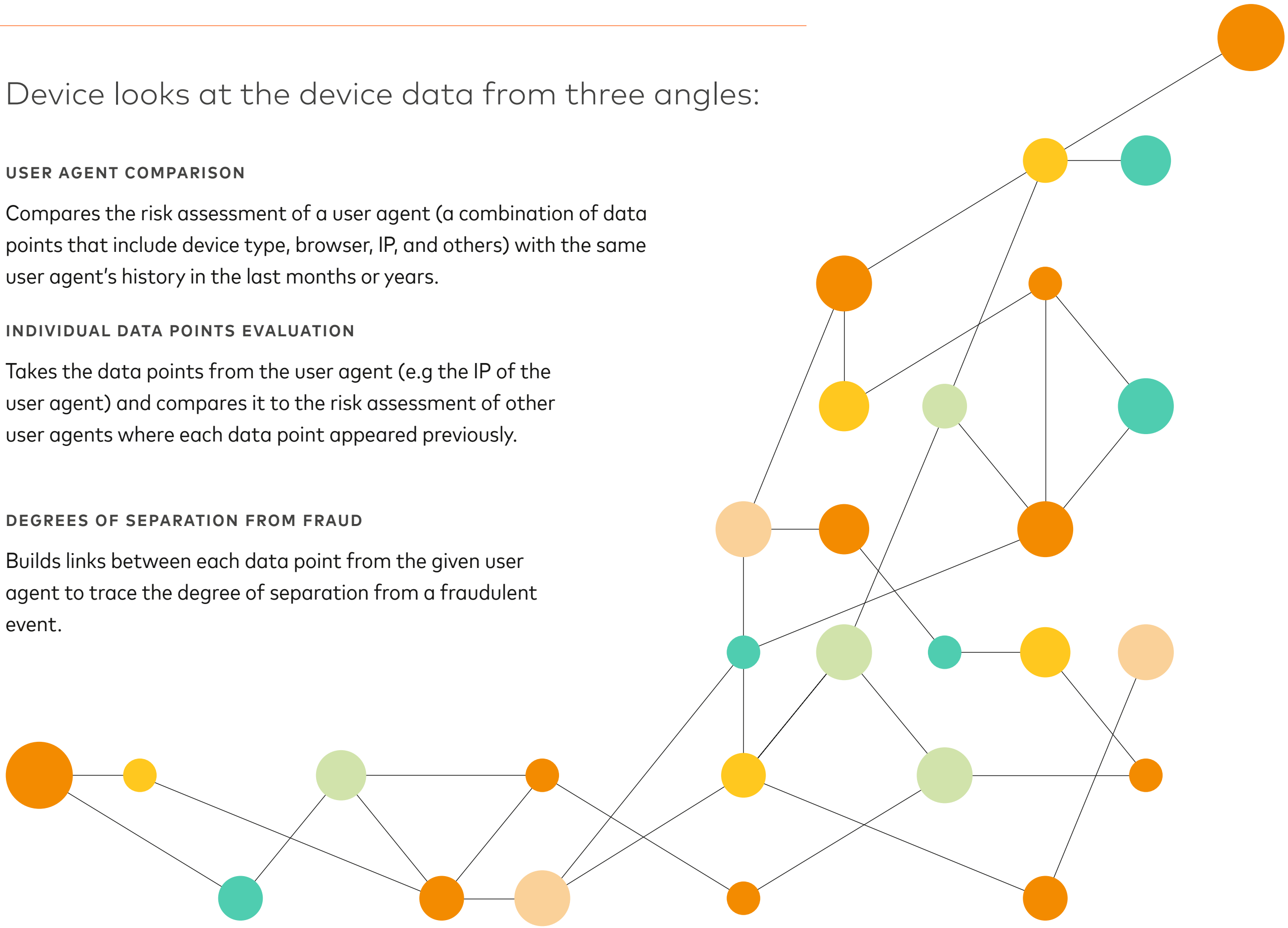
Compares the risk assessment of a user agent (a combination of data points that include device type, browser, IP, and others) with the same user agent's history in the last months or years.

2 **INDIVIDUAL DATA POINTS EVALUATION**

Takes the data points from the user agent (e.g the IP of the user agent) and compares it to the risk assessment of other user agents where each data point appeared previously.

3 **DEGREES OF SEPARATION FROM FRAUD**

Builds links between each data point from the given user agent to trace the degree of separation from a fraudulent event.



IP address + Device fingerprint + Device history = Unique identifier 0% collision rate

In 2023 there will be 18.4 billion* mobile devices; NuData will differentiate each and every one of them.

> NuData uses a powerful blend of four integrated layers that include passive biometrics and machine learning capabilities that learn from rapidly changing patterns. NuData's clients leverage this technology to uncover sophisticated mass-scale attacks that otherwise go unnoticed and generate losses.

More specs

Don't just scratch the surface, get more insight with our webinar.

NuData Security
mastercard

*Statista, 2020