



TRUSTID Device Fingerprinting

Trail-blazing technology to keep fraudulent devices at bay

It's risky business out there

Being able to identify the device used by an online buyer and whether it has any association with past fraud is a hotspot today for e-commerce organizations - and also a problem area. Fraudsters have taken quantum leaps over existing cookie-based device identification approaches, making them largely ineffective. And that despite cookie-based device identification being a fairly recent innovation. Given the sheer number of fraudulent masterminds around the world today, it is increasingly risky to conduct business online. That's just how the cookie crumbles!

Trust in our ID technology

TrustID, the MerchantRMS Device Fingerprinting solution, is a powerful tool that is light-years ahead of existing technologies, and of the fraudsters. TrustID's state-of-the-art features leverage composite device ID technology that helps to readily sort out the bad guys from the good customers.

Our Proxy-Buster feature combats fraudsters who try to hide their actual location using proxy servers, plus our geo-location technology determines in real-time if the transaction request is being sent through a proxy or VPN, even if the criminal uses a Dark Net such as TOR. TrustID can also detect if a Bot Net is being used.

No stone left unturned

We enable merchants to identify the individual PC, tablet, smartphone or other device being used by an online buyer and the characteristics of that device.

Typically these device characteristics are thoroughly examined:

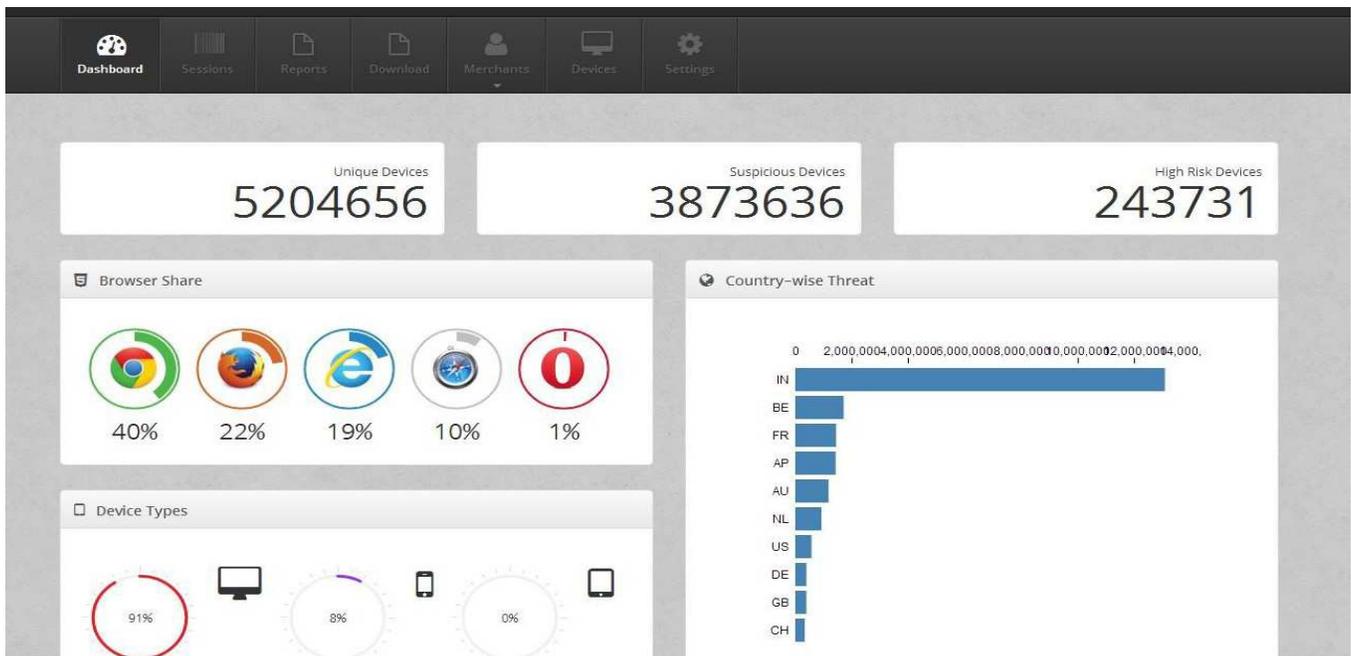
- ⇒ Network
- ⇒ Connection Security Parameters
- ⇒ Operating System
- ⇒ Flash
- ⇒ HTTP
- ⇒ JavaScript Features
- ⇒ Browser.

The device information is matched against our mammoth database of devices used for e-commerce transactions, which now tracks over 150 million devices worldwide, with new devices added daily. Even if the device is seen for the first time, TrustID accurately profiles any potential risks.

Better control, bigger picture

In addition to this device information, MerchantRMS tracks the online buyer's geo-location, IP address, access network, and local time to check for any discrepancies with where they claim to be located. By checking all these different layers within the device, MerchantRMS TrustID creates and maintains a unique Device ID - even when fraudsters modify the system settings to try and hide their true identities. And this all happens in a fraction of a second, invisibly to the buyer.

Furthermore, our **Nexus** feature associates device anomalies with known fraud patterns and helps to create specific rules to optimize fraud parameter detection, irrespective of the device.



Loaded to beat fraud

- ⇒ Know instantly when a device with fraud history connects to your e-commerce platform
- ⇒ Geo-locate your customers
- ⇒ Expose discrepancies between geo-location and time-zone or proxy IP address, plus any language mismatch
- ⇒ Profile any potential risk when a new device with no prior history makes a connection
- ⇒ Expose related accounts and devices involved in fraud
- ⇒ Assesses past behavior of the device and velocity checks.



ABOUT MerchantRMS

Online payment fraud, every time it occurs, affects multiple parties involved and is a huge drain on your company's time and resources. MerchantRMS is trusted by some of the world's top brands and payment services providers to guard against online payment fraud. With state-of-the-art technology and a blazingly fast platform, MerchantRMS counters fraud with élan, letting e-commerce businesses concentrate on what they do best.

MerchantRMS uses not one, but a complete suite of advanced technologies to defend businesses against fraud. With a simple-to-integrate API, it can instantly start protecting your business. While stopping fraud will cut your losses, once fortified by MerchantRMS you can accept more business with confidence and drive up your online sales.

