SOLUTION BRIEF

Adding Risk and Reputation to Your Authentication Process

An understanding of how risk powers adaptive authentication

Leveraging Device Reputation to Balance Security and Usability

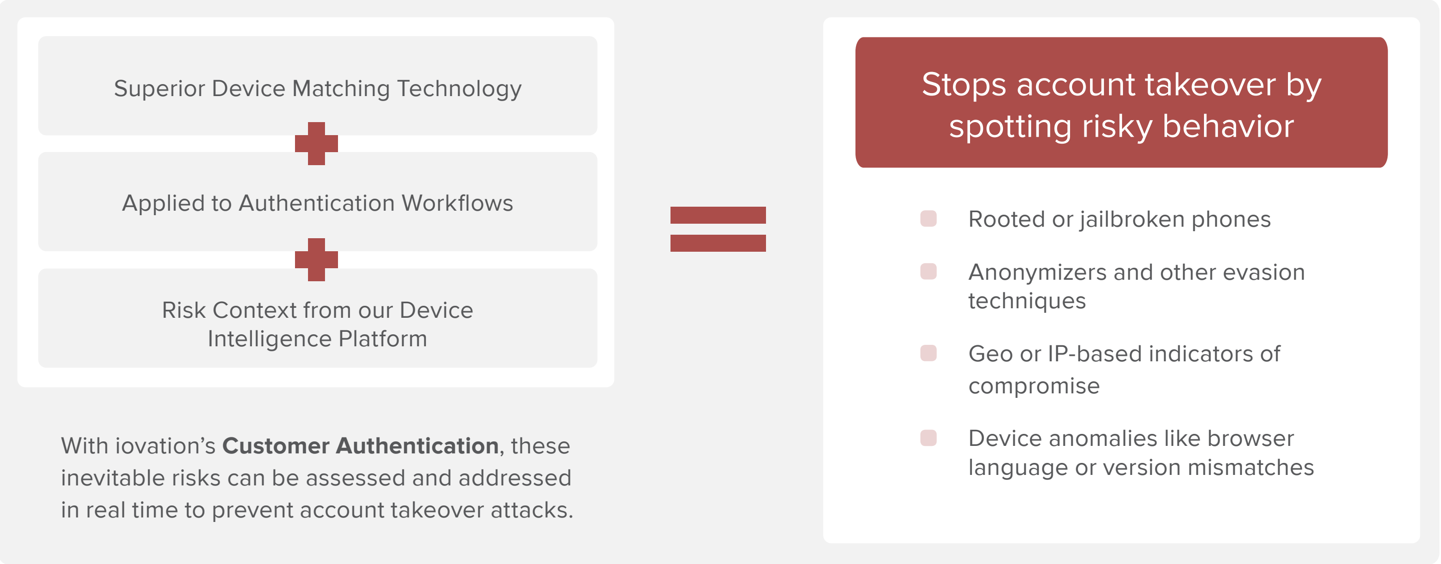
Good security habits die hard. Despite the fact that device recognition has made significant advances – with hundreds of attributes merging to create a dynamic, nearly irrefutable digital fingerprint – there are some who still have questions about authentication methods that seem invisible to the end user.

- **Does device-based authentication account for known risks and anomalies?**
- **Can it defend against device spoofing?**
- **Can it be seamlessly augmented, as needed, by traditional methods such as KBA and OTP??**

iovation's **Customer Authentication** is the only transparent, device-based authentication solution that simultaneously checks against a full spectrum of risk indicators in real-time, while scrutinizing the reputation details of millions of known-bad devices.

This includes checking to see if the device is explicitly authorized to access an account, tapping into iovation's Global Device Intelligence Platform to check for fraud history, uncovering any suspicious transaction behavior such as coming through an anonymizing proxy, and evaluating related devices and accounts.

By applying iovation's superior device matching capabilities, coupled with precise risk and reputation data, to authentication workflows, **Customer Authentication** allows product and security teams to offer customers stronger security and a vastly improved online experience.



Superior Device Matching Technology

+

Applied to Authentication Workflows

+

Risk Context from our Device Intelligence Platform

=

Stops account takeover by spotting risky behavior

- Rooted or jailbroken phones
- Anonymizers and other evasion techniques
- Geo or IP-based indicators of compromise
- Device anomalies like browser language or version mismatches

With iovation's **Customer Authentication**, these inevitable risks can be assessed and addressed in real time to prevent account takeover attacks.

Integrating Risk Elements

By using data elements mined from a variety of risk sources, online businesses can instantly slow down, stop or reroute an automated authentication event, increasing overall usability without increasing risk.

Slow Down = Step Up

Stop = Deny

Reroute = Fraud Team

Browsers

- List of system fonts
- Random sample of 15 fonts
- Accepted character sets in HTTP header
- Accepted languages in HTTP header
- Browser user agent comment string
- Browser name, version, language
- System OS
- Cookie writes excluded
- Whether JavaScript is enabled
- Flash version
- List of browser plugins
- Screen resolution
- Simbar toolbar GUID from HTTP header
- Time zone offset in minutes

iOS Devices

- WiFi (or Bluetooth) MAC Address
- Network configuration
- iOS Device Model
- Battery level / AC mode
- Device orientation
- File system size
- Physical memory
- CPU type / count / speed
- Number of attached accessories
- Proximity sensor detected
- Screen brightness and resolution
- System uptime
- iOS Device Name (MD5 Hash)
- OS Name and/or version
- Device advertising UUID
- Kernel version
- iCloud Ubiquity Token
- Application Vendor UUID / name/version
- Locale language / currency code
- Simulator in use
- Carrier mobile network code
- Carrier name
- Latitude/longitude/ altitude
- Process name

Android Devices

- Model and device model
- Device hardware version
- Manufacturer
- OS build time
- Network Operator ID & Name
- Sim Operator ID & Country
- System uptime in seconds
- Device plugged in
- CPU type
- Physical memory
- Unique build fingerprint of app
- Android SDK Level
- Android build number (DISPLAY)
- Android device system version
- Detected attempt at hiding root detect
- Kernel version (was AKV)
- Android locale country code
- Desktop wallpaper
- Running emulator
- Time zone
- Ringtone
- Unique subscriber ID

Using a Device Reputation Check

Knowing if and when a device previously deemed as "good" has been subsequently used for fraud is critical. Similarly, knowing if the device has since been associated with other accounts or devices that present high risk is also a key component of assessing risk.

iovation's **Customer Authentication** service can instantly check the reputation of a device at registration or other key points in the consumer's online journey. This check compares the current fingerprint of the consumer's device to iovation's library of more than 3 billion devices from around the globe. If the device in question has become associated with risky activity or suspected fraud—directly or indirectly, and initially or since it was last seen—a step-up authentication or a fraud alert can be easily triggered.

A reputation check builds a blackbox, iovation's proprietary encrypted information package, which returns any accounts that have been flagged by other iovation subscribers around the world as being linked to:

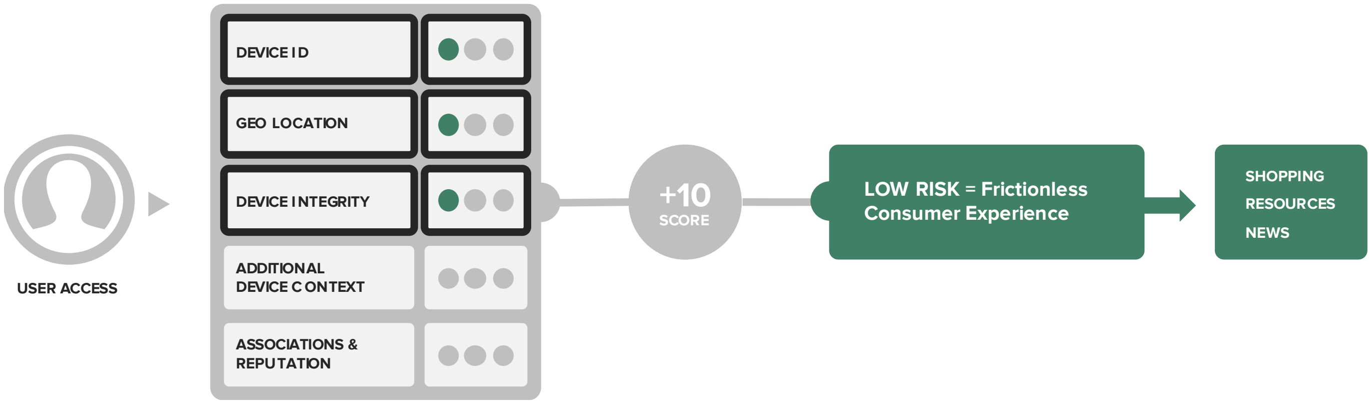
- Chargebacks
- Identity theft
- Account takeovers
- Online scams
- Phishing
- Loan Default
- Collusion
- 46 types of fraud

Reputation Check Workflow

Following is an example of how businesses can evaluate the riskiness of a device, and take specific actions based on the result of the device authentication event, increasing overall usability without increasing risk.

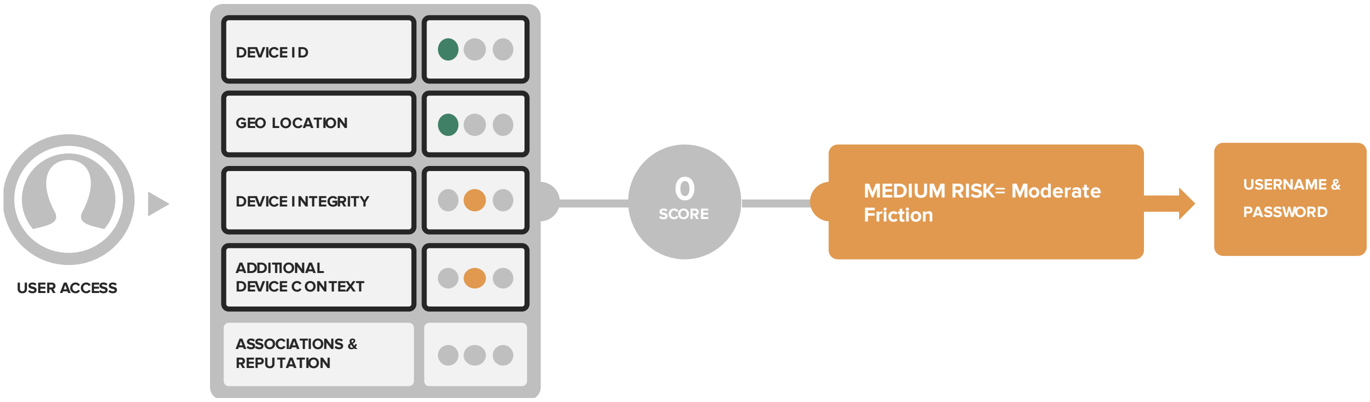
USER 1

A user who visits your site checks out with a Device ID, Geolocation, and Device Integrity result that look good. The device is labeled LOW RISK and the customer is seamlessly allowed into your site to access the resources available to them.


USER ACCESS
DEVICE ID
GEO LOCATION
DEVICE INTEGRITY
ADDITIONAL DEVICE CONTEXT
ASSOCIATIONS & REPUTATION
+10
SCORE
LOW RISK = Frictionless Consumer Experience
SHOPPING
RESOURCES
NEWS

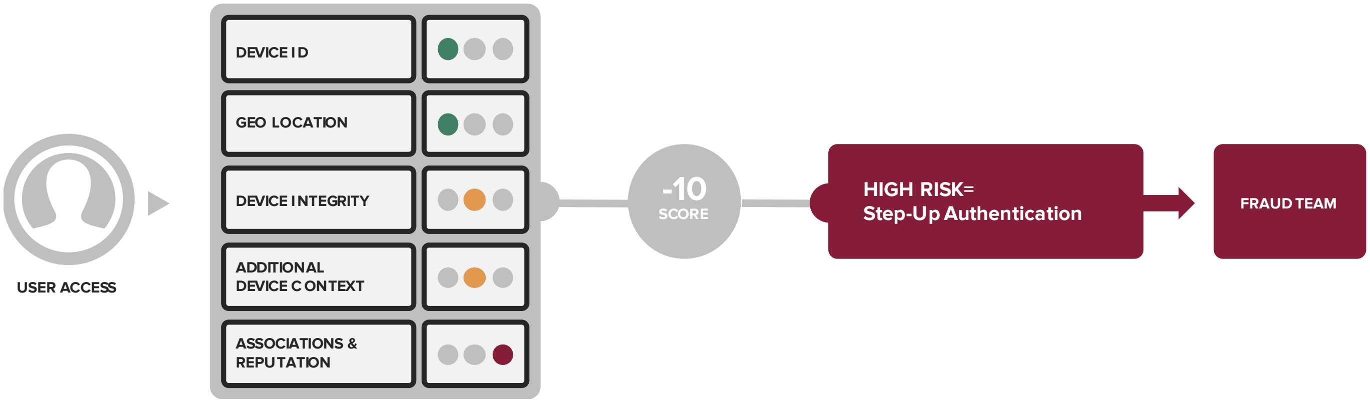
USER 2

For this user, a Device Integrity and context data check reveals potential issues that could impact your business in a negative way. As a result, the device is labeled MEDIUM RISK and the user is required to provide a username and password in order to gain access to your site.


USER ACCESS
DEVICE ID
GEO LOCATION
DEVICE INTEGRITY
ADDITIONAL DEVICE CONTEXT
ASSOCIATIONS & REPUTATION
0
SCORE
MEDIUM RISK= Moderate Friction
USERNAME & PASSWORD

USER 3

In this case, the user's device shows associations with other devices that are linked to fraudulent activity. The device is labeled HIGH RISK and referred to the fraud team for follow-up action. The user is not allowed to gain access to your site.


USER ACCESS
DEVICE ID
GEO LOCATION
DEVICE INTEGRITY
ADDITIONAL DEVICE CONTEXT
ASSOCIATIONS & REPUTATION
-10
SCORE
HIGH RISK= Step-Up Authentication
FRAUD TEAM

Never before has this level of risk and reputation insight been available for real time authentication events. iovation provides the balance between strong security and great usability you've been looking for.

iovation®

To learn more about **Customer Authentication** and schedule a demo, please contact us or visit www.iovation.com.

PORTLAND • PH +1 (503) 224-6010 • EMAIL info@iovation.com **LONDON** • PH +44 (0) 800 058 8731 • EMAIL uk@iovation.com