Entrust Datacard™

Entrust Datacard Device Reputation

Leverage Analytics to Improve Security and Reduce User Friction

With digital business on the rise, user and customer demands are quickly evolving to frictionless yet secure experiences. Customer attraction and retention is critical to business success and requires users - such as employees, customers and consumers - to conduct business anytime, anywhere without the worry of fraudulent activity.

And as mobile and cloud technologies emerge, organizations are changing the way they do business by implementing more efficient internal processes, enhancing user experiences, and offering new products and services. Entrust Datacard equips you with the tools to meet the demands of digital business transformation with trusted identities and next generation authentication at its core.

Entrust Datacard Device Reputation allows organizations to provide their users a transparent, secure experience by only enabling step-up authentication when a user's registered device is elevated as a risk.

Recongize, Detect and Stop Fraud in its Tracks

Entrust Datacard Device Reputation is part of our next generation platform and uses best-of-breed device identification, dynamic risk context, and analytics from a global intelligence network to transform static, single-factor authentication processes into adaptive multi-factor solutions. Device reputation recognizes and detects fraudulent behavior across all types of internet devices including desktop, mobile and tablets, even prior to login, and integrates with websites and applications.

The Power of Three – Next Generation Authentication

Trusted identities and a powerful authentication platform are essential to digital business success. Companies are no longer looking for a single-point solution, and now searching for a next generation authentication platform that will empower their users while fighting against fraud.

Breadth, Depth & Flexibility

Device reputation and other sources of insight can all be used in our Entrust IdentityGuard adaptive engine, and paired with a wide-range multi-factor solutions. With over 17 authentication methods - including mobile push authentication – extensive scale of use cases, adaptive authentication capabilities, and a comprehensive portfolio of integrations, you can address your immediate needs today and quickly adapt as your digital business evolves. We provide you with the authentication platform of choice for the demands of digital business.

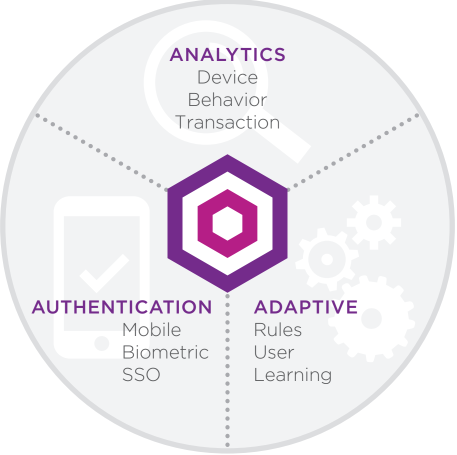
+1-888-690-2424

entrust@entrust.com
entrust.com

@EntrustDatacard
+entrust
/EntrustVideo
/EntrustSecurity

Benefits

- Provide a transparent, frictionless user experience
- Stops fraud and abuse in real-time, prior to login
- Find subtle patterns with powerful analytics to fight fraud more effectively
- Make data-driven decisions with detailed fraud evidence
- Deep analytics and machine learning quickly adapt to changing fraud trends
- Prevent previous fraudulent-flagged devices from accessing your network and Enterprise application
- Gather risk information about the device before login



Entrust Datacard Device Analytics

Identify Fraud Patterns

To help you accurately separate the fraudsters from your trusted users, identify risky device behaviors including:

- Evasion Techniques: Identify fraudulent transactions that originate by:

  • Redirecting or concealing the use or location of a device through TOR networks and proxy servers

  • Artificially simulating a mobile device and it's operating system through a desktop application
- Device anomalies: Includes location mismatches, time zone and IP address changes, too many devices per account, and exceeded velocity thresholds
- High-risk locations, IPs, and ISPs: Includes high-risk geographic locations or known bad IPs, ISPs, or locations that violate your specific business policy

Advanced Analytics

Our advanced fraud prevention and detection capabilities extend your protection to fraud patterns that you are most concerned about. For example, Device Reputation can inform you:

- If a particular device has been used to access multiple accounts within a particular time period
- When many devices have been used to access a single account
- If the device has a history of specific types of fraudulent activity
- When the device is linked to other devices or accounts associated with fraud
- Whether the device has violated specific policies that you have defined such as geolocation, chat abuse, spending limits or cheating

All of this information is gathered and analyzed in the milliseconds before the device logs in to your network

Key Features

Device ID and Registration: Affirm user identity by matching device fingerprints with a high degree of accuracy, and explicitly pairing known good Device IDs with the user's account.

Device Change Tolerance: Weaker device-based authentication systems are defeated by the natural drift caused by updates, new apps or even new fonts. And fuzzy matching technology takes expected changes of the device into consideration to minimize unnecessary "negative" responses and create "acceptable risk" boundaries.

Reveal Hidden Connections: Understanding how a device links to known bad activity or other users will allow you to automatically enforce step-up authentication challenges if risk thresholds are exceeded.

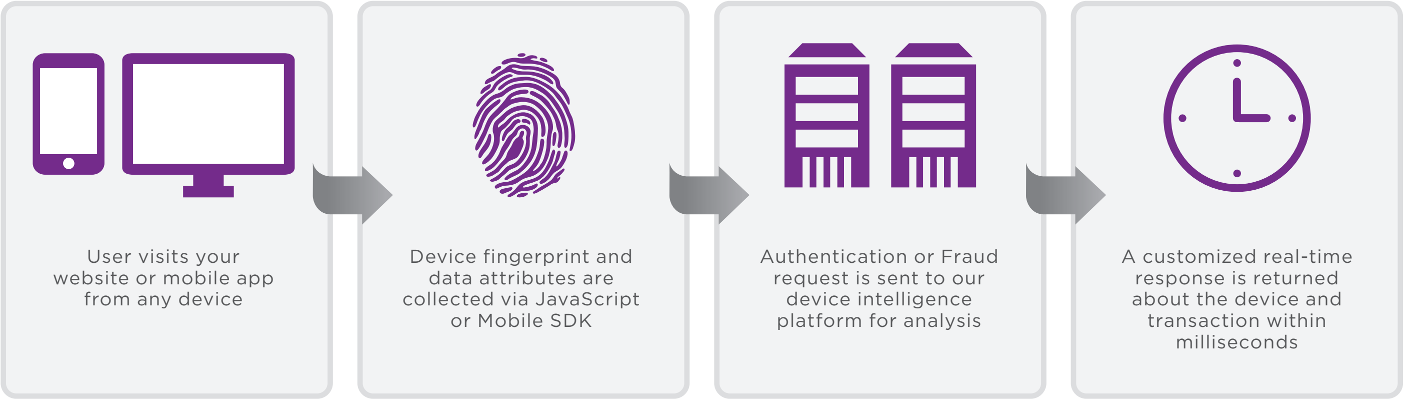
Evasion Detection: Proxy piercing detects proxy servers that are often employed by fraudsters and scammers, while leveraging advanced techniques to unmask TOR networks, VPNs, mobile VMs, emulators or other anonymizing activity.

Global Device Intelligence Platform: Real-time device analytic feedback from thousands of risk analysts flags suspicious accounts and devices immediately.

"PII-less" Precision: Recognition technology uses hundreds of device attributes and their unique orientation with each other to instantly identify a device without the need for the user's personally identifiable information.

How Entrust Datacard Applies Device Reputation

Adding layered security to reduce user involvement, provides a seamless and transparent experience, and only relies on multi-factor authentication when needed – giving organizations the right balance between security and usability.



User visits your website or mobile app from any device

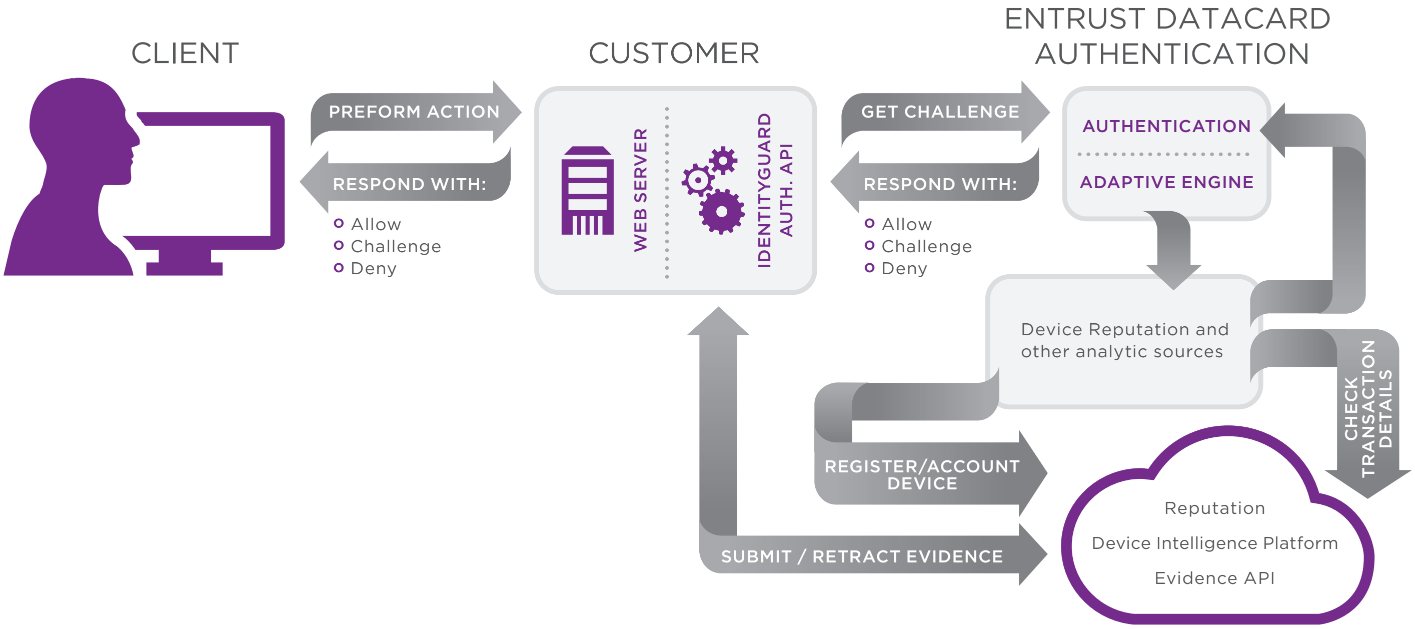
Device fingerprint and data attributes are collected via JavaScript or Mobile SDK

Authentication or Fraud request is sent to our device intelligence platform for analysis

A customized real-time response is returned about the device and transaction within milliseconds

Based on Risk Based Analysis configuration, our solution provides a recommendation such as the below:

- **Allow:** device is trusted and policy says that's all that's required
- **Challenge:** device may be under review and policyidentifies another factor for authentication is required
- **Deny:** device is flagged as untrusted and authentication is refused outright



Use Cases for Financial Institutions and Enterprises

Banking

New Account Creation: Securely offer new services by identity-proofing the integrity of your customer's device when they digitally create an account online or through their mobile device.

Online & Mobile Banking: Empower your users to access account information with a seamless and transparent experience and only enable step-up authentication when risk is elevated.

Transaction Verification: Out of band transaction verification helps defeat advanced fraud attacks by adding a layer of security and assessing the device integrity.

Employee

BYOD Pre-check: Ensure the integrity of your new employee's device before issuing access to company information, tools and resources.

Mobile ID Pre-check: Ensure the user's device has not been associated to any fraudulent activity before a trusted identity is provisioned to the device.

Streamline User Access: Reduce the amount of times a user needs to authenticate by layering device analytics to identify low risk situations.

- On-Premise and Cloud Applications
- Partner and Customer Portals

About Entrust Datacard
Consumers, citizens and employees increasingly expect anywhere-anytime experiences — whether they are making purchases, crossing borders, accessing e-gov services or logging onto corporate networks. Entrust Datacard offers the trusted identity and secure transaction technologies that make those experiences reliable and secure. Solutions range from the physical world of financial cards, passports and ID cards to the digital realm of authentication, certificates and secure communications. With more than 2,000 Entrust Datacard colleagues around the world, and a network of strong global partners, the company serves customers in 150 countries worldwide.

For more information about Entrust products and services, call **+1-888-690-2424**, email **entrust@entrust.com** or visit **www.entrust.com**.

Headquarters
Entrust Datacard
1187 Park Place
Shakopee, MN 55379
USA

Entrust Datacard™