PingOne Fraud

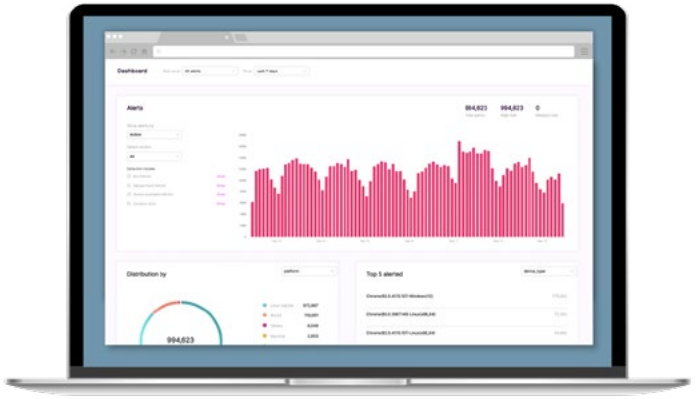
ProofID PingIdentity

DATASHEET

PingOne Fraud combines real-time behavioral navigation, behavioral biometrics, device attributes and much more to detect sophisticated fraud attacks that bypass other detection tools, while ensuring a hassle-free customer experience for trusted users. It conducts individual customer session analysis and produces a risk score to incorporate into your fraud detection policies. PingOne Fraud removes the need for organizations to choose between a lower fraud rate and a customer-friendly application. An easily deployed light SDK solution, PingOne Fraud supports both mobile and web environments.

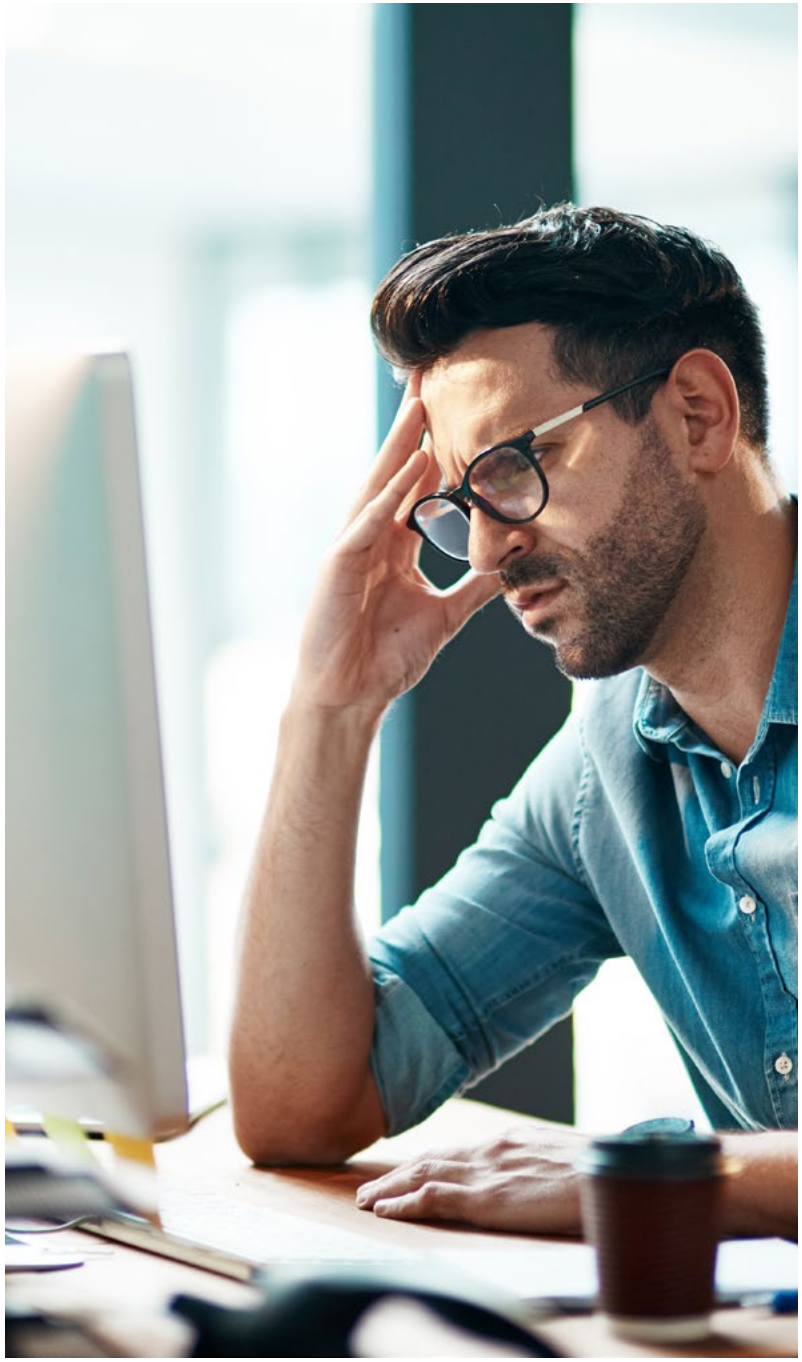
Features & Benefits

- Cloud-based real-time online fraud detection
- Evaluate the unknown/known session from inception to close
- Adapt to new and emerging fraud patterns by combining dynamic behavioral data with advanced machine learning
- Detect online fraud prior to checkout or purchase
- Use unique user behavior insights for smarter online fraud detection
- Permit legitimate customer sessions to go uninterrupted
- Access dashboards and reports for online fraud insights
- Create a risk score to differentiate between fraudsters and legitimate customers
- Understand alerts based on session-level explainability and visualisation
- Analyze system-wide insights to understand when and how your business is being defrauded



Categories of Fraud Signals Evaluated

- U.S. and international driver's licenses
- ISO-based international passports
- European ID cards with three-line MRZ code



EVALUATE BEHAVIORAL BIOMETRICS TO DETECT ONLINE FRAUD

PingOne Fraud leverages behavioral data to identify a user's intent, helping fraud fighters accurately distinguish between fraudsters and legitimate customers. Fraudsters have distinct behavioral patterns, while bots and emulators have their own distinct behaviors. Recognizing the intent behind these behaviors is the key.

Behavioral Biometrics

PingOne Fraud's technology continuously analyzes hundreds of data points generated by the innate physical interactions between a human and a device such as mouse movements, keystroke dynamics and mobile gestures analysis. These data points are used to differentiate between legitimate and fake user behaviors (such as bots), as well as between legitimate and fake devices (such as emulators). Rather than looking for known signatures of these tools, PineOne Fraud looks at normal interactions and alerts whenever an anomaly is presented, including the newest and most sophisticated attacks.

Behavioral Anomalies

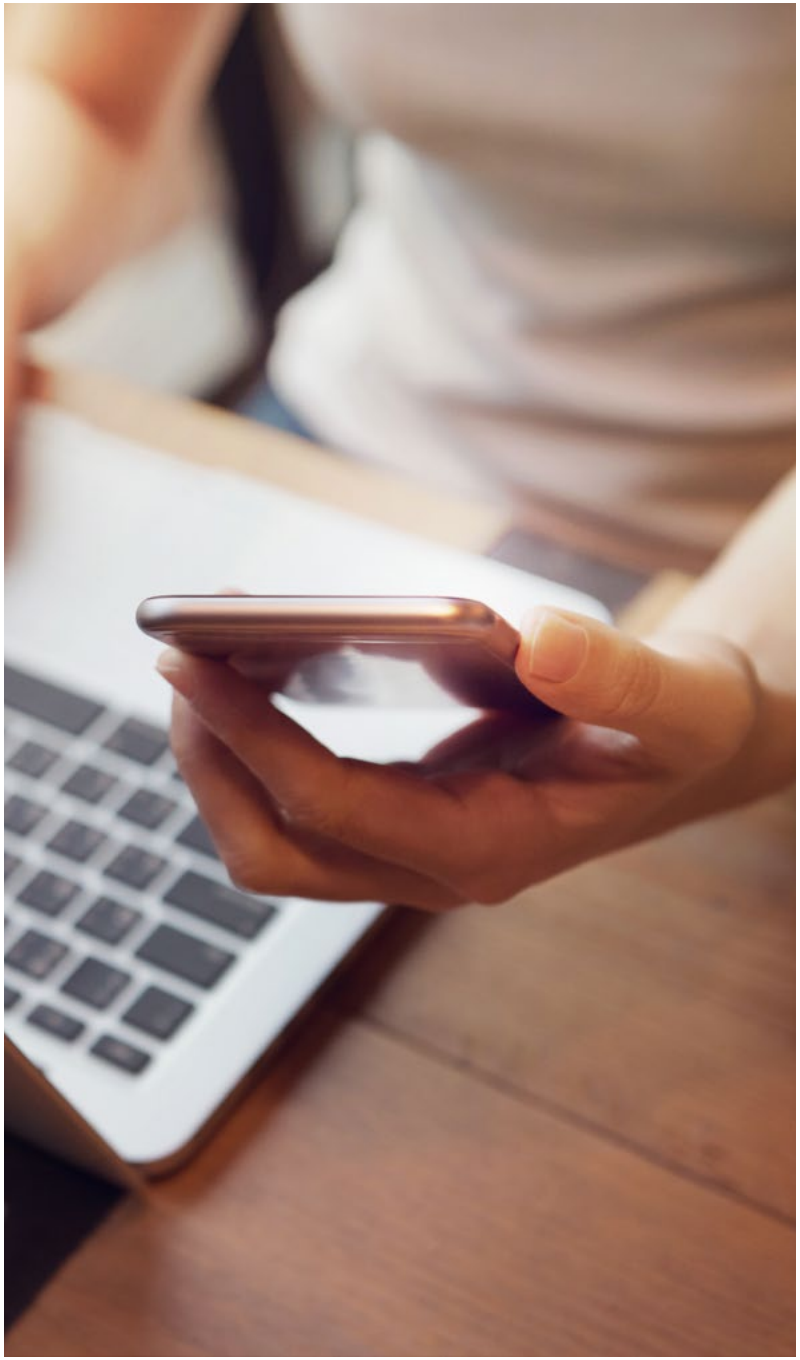
The interactions of a user with a website or application differ between legitimate customers and fraudsters. Fraudsters aim to carry out attacks quickly and efficiently and move on to their next target. Examples of deviations from normal user behaviors include moving between or filling out fields in a registration form too quickly or going directly to change the shipping address instead of browsing and adding items to the cart. Recognizing these actions allows our technology to determine a user's intent and detect fraudulent activities.

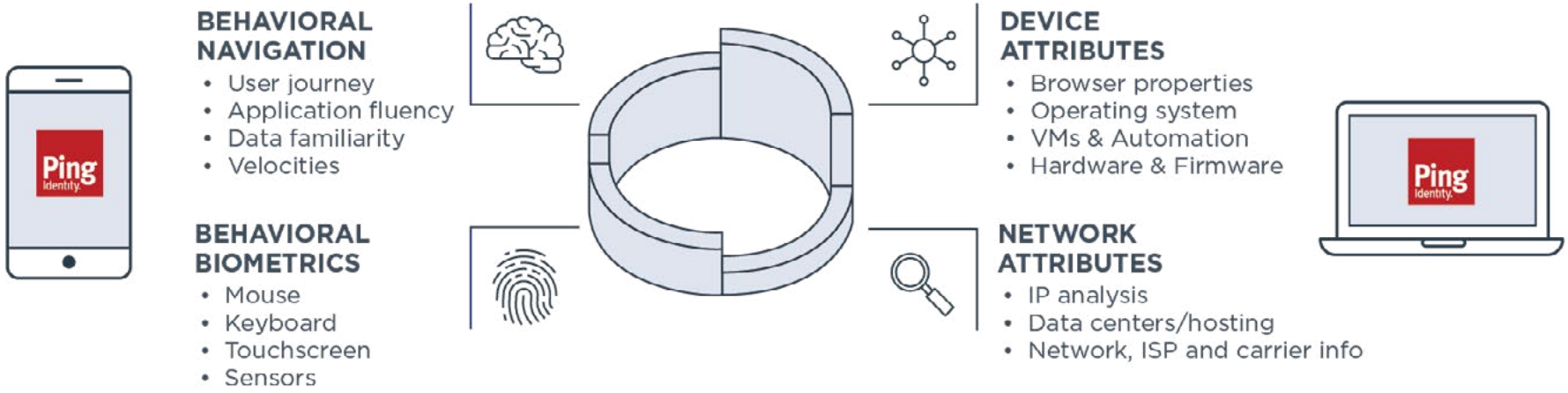
Bot Detection

Automated scripts, or bots, allow fraudsters to scale up their attacks, rendering current fraud detection tools obsolete. Multi-dimensional data analyzed by our machine learning algorithms automatically distinguish between human and non-human users. That means fraud detection no longer relies on rigid solutions that ultimately allow fraud that was previously undetected to go unnoticed. Attempts to monetize stolen credit card details or user credentials are stopped immediately.

Device Intelligence

Similar to how our technology separates human and non-human users, pairing device attributes and behavioral data allows detection and classification of fraudulent devices like emulators or devices running through a cloning app. Identifying if a device has been tampered with or spoofed is easy. Emulators leave a footprint on the OS. Incomplete critical behavioral data like mobile attributes missing accelerator or gyroscope data automatically raise red flags. When a device generates suspicious attributes, there is no need to wait to assess user activities.





ADDRESS MULTIPLE FRAUD USE CASES

As fraudsters continue to adapt to digital channels, PingOne Fraud ensures your customers can securely and easily transact and make purchases. PingOne Fraud presents a unified approach, addressing multiple fraud use cases and threats while providing a frictionless customer experience.

PingOne Fraud Protects Against

- Credentials Stuffing
- Credit Card Testing
- Zero Day Bots
- Emulators
- Account Takeover
- New Account Fraud
- Loyalty Fraud
- Referral Fraud
- Coupon Fraud

ProofID

ABOUT PROOFID ProofID is a global identity security partner, integrator and service provider. Proven specialists, ProofID is committed to delivering pain-free, secure and seamless access and authentication experiences. Trusted by Tier 1 enterprises around the world to design, deliver and manage identity services, ProofID has successfully deployed their technology into regulated financial institutions with dynamic workforce needs, high street retailers that require seamless customer engagement, leading universities and worldwide charities. Their highly skilled team has been awarded more technical accreditations than any other Ping partner and earned Ping's Delivery Partner of the Year Award for three consecutive years. For more information, please visit www.proofid.com.

Ping Identity

ABOUT PING IDENTITY Ping Identity delivers intelligent identity solutions for the enterprise. We enable companies to achieve Zero Trust identity-defined security and more personalized, streamlined user experiences. The PingOne Cloud Platform provides customers, workforce, and partners with access to cloud, mobile, SaaS and on-premises applications across the hybrid enterprise. Over 60% of the Fortune 100 choose us for our identity expertise, open standards, and partnerships with companies including Microsoft and Amazon. We provide flexible identity solutions that accelerate digital business initiatives, delight customers, and secure the enterprise through multi-factor authentication, single sign-on, access management, intelligent API security, directory, and data governance capabilities. For more information, please visit www.pingidentity.com.