DATA SHEET

ID Dataweb Threat Detection Playbook

Attack vectors, use cases, and identity data sources

Digital identity is now the primary security perimeter for organizations. Attackers increasingly exploit weaknesses across the identity lifecycle — from account creation to account recovery — using automation, stolen credentials, and synthetic identities.

The modern identity threat landscape

Identity attacks are evolving rapidly, fueled by automation, large-scale credential theft, and increasingly sophisticated fraud techniques. Common tactics, techniques, and procedures (TTPs) used by threat actors include:

Account Takeover (ATO)
Attackers leverage stolen credentials, phishing, malware, or session hijacking to gain access to legitimate user accounts.

Credential Stuffing
Automated bots attempt millions of login attempts using leaked username/password combinations.

Synthetic Identity Fraud
Attackers create fraudulent identities by blending real and fabricated data to open accounts or bypass verification controls.

Bot-Driven Abuse
Automated systems generate fake accounts, scrape data, and abuse promotions or incentives.

Social Engineering
Attackers manipulate users into performing actions or divulging confidential information.

Privilege Escalation
Compromised identities are used to elevate access and move laterally within systems.

Impersonation
Threat actors pose as trusted individuals to manipulate a victim into taking actions that benefit the attacker, such as transferring funds, revealing credentials, or sharing sensitive data.

Insider Threats
Employees or contractors misuse legitimate access intentionally or unintentionally.

Any attack surface. One unified platform.

The ID Dataweb™ SaaS platform provides continuous identity threat detection and adaptive authentication across customer, workforce, and third-party (e.g., contractors, suppliers) environments — helping organizations stop identity fraud while maintaining seamless user experiences.

Customers

Third Parties

Workforce

dataweb

Common identity security use cases

The ID Dataweb platform safeguards digital interactions across the entire identity lifecycle. Leveraging one of the industry's most comprehensive libraries of authoritative identity data sources and risk signals, it enables a wide range of use cases across workforce, third-party, and customer environments. Examples include:

Use Case	**Secure Account Creation** Attackers often exploit signup workflows to create synthetic or automated accounts.	**Intelligent Account Login Protection** Valid credentials no longer guarantee legitimate access.	**Account Takeover Detection** Account compromise often occurs silently after authentication.	**Account Recovery Protection** Recovery workflows are frequently targeted by attackers attempting to bypass authentication.	**Credential Reset Protection** Password resets provide attackers with an easy path to account control.	**Profile Change Protection** Attackers often modify account details to maintain control or prepare for financial fraud.	**Call Center & Help Desk Fraud Prevention** Support channels are a common target for identity-based social engineering.	**Data Hygiene** Identity fraud thrives in outdated, duplicate, and polluted identity databases.
Common Threats	• Synthetic identities • Bot-driven registrations • Stolen personal data • Promotion abuse	• Credential stuffing • Phishing and MFA fatigue attacks • Session hijacking • Automated login abuse	• Attackers using valid credentials • Subtle behavioral anomalies • Delayed detection	• Social engineering attacks • Knowledge-based authentication abuse • Automated recovery attempts	• Stolen personal data used for verification • Automated reset abuse • Weak verification processes	• Email or phone number changes • Address and payment manipulation • Privilege escalation through profile updates	• Impersonation using stolen personal data • Pressure tactics against agents • Inconsistent verification procedures	• Duplicate or stale accounts • Synthetic identities persist over time • Limited visibility into identity risk
ID Dataweb Protection	• Real-time identity risk assessment • Bot and synthetic identity detection • Frictionless onboarding for legitimate users	• Behavioral and contextual risk analysis • Detection of compromised identities • Adaptive step-up authentication	• Continuous identity behavior monitoring • Real-time anomaly detection • Automated containment workflows	• Identity risk evaluation during recovery • Detection of abnormal behavior patterns • Adaptive step-authentication	• Risk analysis during reset attempts • Behavioral anomaly detection • Dynamic authentication requirements	• Continuous post-login identity monitoring • Real-time detection of high-risk profile changes • Adaptive controls for sensitive updates	• Real-time identity risk signals for agents • Detection of scripted fraud attempts • Guided adaptive authentication	• Continuously assess identity risk across databases • Identify suspicious, dormant, or high-risk accounts • Support cleanup and governance initiatives
Outcome	• Higher-quality accounts • Reduced identity fraud exposure • Cleaner user databases	• Reduced account takeovers • Improved login security with minimal friction	• Reduced identity fraud losses • Faster response to identity compromise	• Fewer fraudulent recoveries • Reduced operational support costs	• Reduced fraudulent credential resets • Stronger overall account security	• Identity fraud prevented before financial or reputational damage occurs	• Reduced call center fraud • Faster call handling • Increased agent confidence	• Cleaner identity data • Reduced attack surface

The ID Dataweb advantage

Continuous Identity Threat Detection

Monitor identity risk across the entire lifecycle — from onboarding to sensitive transactions.

Adaptive Step-Up Authentication

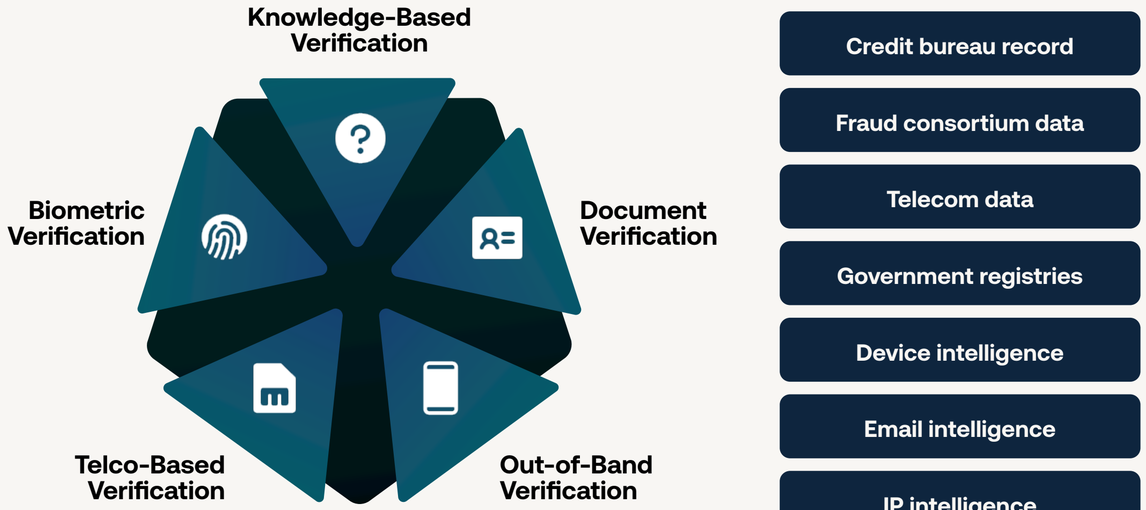
Start with low-friction verification and escalate only when risk increases.

Privacy-Preserving Architecture

Personally identifiable information (PII) is never retained by ID Dataweb.

Identity Orchestration Platform

Leverage a powerful orchestration layer with a large library of authoritative identity data sources and risk signals.



Identity Verification Methods

Verification Data Sources

ID Dataweb aggregates, normalizes, and contextualizes authoritative identity data sources and risk signals from leading industry providers, including:

acuant a GBG company · boku · Trulioo · EQUIFAX · telesign · Mitek · TransUnion · onfido · experian · facetec anchoring identity · incode · AUTHENTICID · LSEG · LexisNexis · Emailage®

Prevent identity fraud. Build trust. Power digital interactions.

With hundreds of millions of identity verification and risk transactions processed, ID Dataweb equips organizations with the tools needed to stay ahead of identity-based threats while delivering seamless digital experiences.

ID dataweb

iddataweb.com

ID Dataweb™ delivers identity threat detection and mitigation solutions to safeguard against identity fraud and account-related threats, all without disrupting the user experience.

Book a demo

iddataweb.com

ID Dataweb, Inc.
5875 Trinity Parkway
Suite 110
Centreville, VA 20120
United States

© All rights reserved. ID Dataweb Inc., 2026