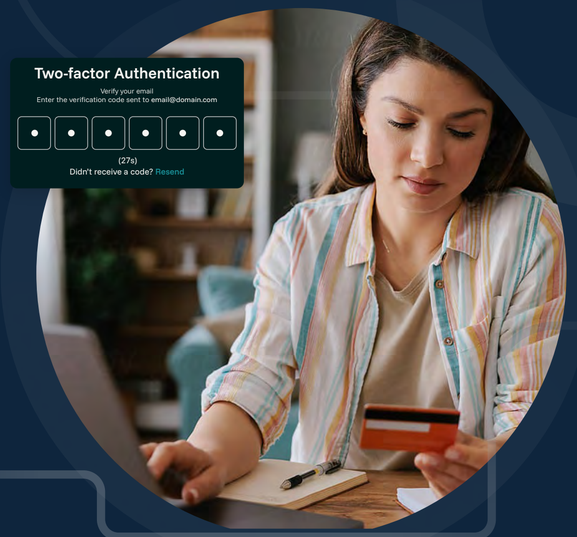
DATA SHEET

ID Dataweb Industry Coverage

Identity threat detection and risk mitigation across critical industries

Digital transformation has created massive opportunities for organizations to engage customers, third parties (e.g., contractors, suppliers), and their workforce through digital channels. However, these same channels have become the primary attack vector for identity-based threats.

Today's attackers rarely hack systems—they take over identities. Stolen credentials, synthetic identities, phishing campaigns, automation, and AI-powered impersonation are driving a new wave of identity fraud targeting organizations across every sector.



Protecting digital interactions across every industry

ID Dataweb™ helps enterprises stay ahead of identity fraud and account-related threats with real-time detection and mitigation while maintaining a seamless experience for their workforce, third parties, and customers.

The ID Dataweb SaaS platform enables organizations across different industries to:

- Detect identity risk across the entire digital lifecycle
- Stop account takeover and identity fraud in real time
- Protect customers, employees, and third parties
- Maintain low-friction user experiences
- Orchestrate identity verification across multiple identity data sources and risk signals
- Integrate seamlessly with existing IAM and security systems

With hundreds of millions of identity verification and risk transactions processed, ID Dataweb delivers proven identity threat detection at enterprise scale.

IDdataweb

A unified platform for all varying market needs

With one of the industry's most comprehensive libraries of authoritative identity data sources and risk signals, the platform supports a wide range of identity security use cases and can be applied across numerous industries. Examples include:

eCommerce

Attackers target eCommerce environments at massive scale by exploiting customer identities, promotions, and checkout flows.

Typical Identity Challenges	Typical Use Cases
• Password reuse across multiple sites • Compromised credentials from phishing and token theft • Limited visibility across hybrid environments • Security focused only on authentication	• Customer account creation • Loyalty program enrollment • Login authentication • Account recovery • Fraud detection during checkout • Identity database hygiene

Financial Services

Financial institutions face highly sophisticated and well-funded attackers targeting high-value identities and financial assets. Identity fraud can result in direct financial loss, regulatory exposure, and reputational damage.

Typical Identity Challenges	Typical Use Cases
• Phishing and social engineering targeting customers and employees • Synthetic identities and mule accounts • Privileged access abuse and insider threats • Balancing strong security with seamless digital banking experiences	• Account opening (in-branch or digital) • Customer authentication and login • Call center fraud prevention • Credential reset and account recovery • High-risk transaction monitoring • AML identity verification

Gaming

Gaming platforms and lotteries experience extreme-scale identity abuse used to cheat systems, steal digital assets, and monetize fraud.

Typical Identity Challenges	Typical Use Cases
• Bot-driven account farming • Account takeover of high-value players • Fake identities used to bypass controls • Event-driven attack spikes	• Age and location verification • Account recovery • Fraud prevention during in-game transactions

Insurance

Insurance providers face rising fraud driven by identity abuse across policy creation, customer portals, and claims processing.

Typical Identity Challenges	Typical Use Cases
• Fraudulent claims using stolen or synthetic identities • Account takeover of customer and agent portals • Insider abuse and privileged access misuse • Weak identity verification during onboarding	• Policy onboarding • Claims identity verification • Agent and workforce onboarding • Account login and recovery • High-risk claims validation

Healthcare

Healthcare organizations rely on trusted identities across clinical staff, contractors, and patients—making identity the primary attack vector.

Typical Identity Challenges	Typical Use Cases
• Phishing and ransomware targeting clinical staff • Shared credentials and unmanaged accounts • Weak governance across contractors and affiliates • Overprivileged access to clinical systems	• Workforce onboarding • Patient portal authentication • Credential reset and account recovery • Identity verification for patient data access • Identity database hygiene

Live Entertainment

Ticketing platforms face intense identity abuse during high-demand events.

Typical Identity Challenges	Typical Use Cases
• Bot-driven ticket scalping • Account takeover of fan accounts • Fake accounts bypassing purchase limits • Loyalty and promotion abuse	• Fan account creation • Loyalty program verification • Ticket purchase validation • Account takeover prevention

Public Sector

Government agencies manage complex identity ecosystems that include citizens, employees, contractors, and service providers.

Typical Identity Challenges	Typical Use Cases
• Identity theft in citizen services • Phishing attacks targeting government employees • Legacy IAM systems with limited visibility • Strict regulatory and privacy mandates	• Citizen account creation • Workforce and contractor onboarding • Credential reset and recovery • Address change verification • Secure access to digital government services

Travel & Hospitality

Airlines, hotels, and travel platforms operate across highly distributed environments with constant identity abuse targeting loyalty programs and booking systems.

Typical Identity Challenges	Typical Use Cases
• Loyalty program account takeover • Fraudulent bookings and refund abuse • Bot-driven scraping and inventory abuse • Securing staff and third-party access across properties	• Loyalty program enrollment • Account login and authentication • Fraud detection during bookings • Account recovery and credential reset • Identity verification for high-risk transactions

dataweb

ID Dataweb: one platform for identity protection

Across industries, organizations rely on ID Dataweb to detect identity threats in real time, protect the entire identity lifecycle, orchestrate risk signals across multiple data sources, deliver adaptive authentication with minimal friction, and integrate seamlessly with existing identity and access management (IAM) systems.

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