SOLUTION BRIEF

Safeguarding Healthcare

Identity security is patient safety

Healthcare organizations face a growing wave of identity-based threats as attackers target the people and access points connected to sensitive clinical systems. Rather than breaching infrastructure directly, threat actors exploit identities through phishing, credential theft, and social engineering to gain legitimate access to electronic health records (EHRs) and other critical systems. Compromised credentials, shared accounts, and weak identity governance enable attackers to move laterally, exfiltrate patient data, and deploy ransomware—all while appearing as authorized users.

The challenge is compounded by complex identity ecosystems spanning clinicians, administrative staff, contractors, and third-party partners. Overprivileged access, unmanaged service accounts, and strict regulatory requirements (such as HIPAA) increase both risk and operational constraints. At the same time, healthcare organizations must maintain seamless access to ensure patient care is not disrupted, limiting the use of high-friction security controls.

These trends highlight the need for continuous identity threat detection—capabilities that assess every digital interaction, from account creation and profile changes to prescription fulfillment, to determine in real time whether it is initiated by a legitimate user or a threat actor.

The impact of the identity crisis in healthcare

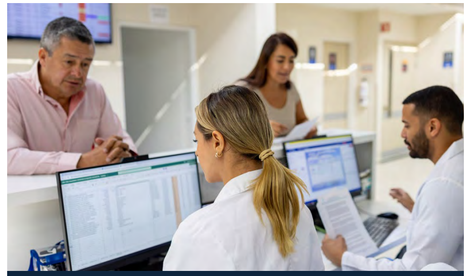
- Patient **data breaches**
- Operational **disruptions**
- Patient **safety risks**
- Regulatory **fines**

The need to move beyond credential-only authentication

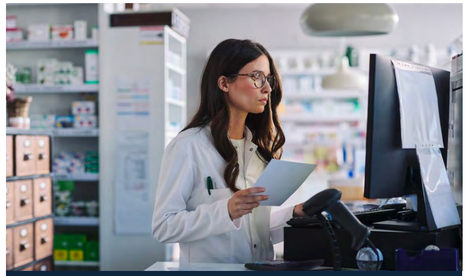
Traditional identity and access management (IAM) solutions focus on verifying whether a user is authorized to access a system or resource. However, modern attackers frequently bypass authentication controls using stolen credentials, social engineering, or AI-powered impersonation techniques.

To combat these threats, healthcare providers must expand their identity security strategy beyond credential-only authentication and incorporate continuous identity threat detection and risk mitigation across all digital interactions.

This includes protecting all identity-related attack vectors across the organization:



Customers



Third Parties

Workforce

Continuous, reliable identity threat detection

Detect identity risk in real time and stop fraud without disrupting legitimate users and patients.

ID Dataweb™ helps you stay ahead of identity fraud and account-related threats while maintaining a seamless digital experience for your customers, third parties, and workforce.

In turn, you can

- Prevent unauthorized access to EHR systems
- Reduce insider and credential risk
- Avoid fraudulent account creation
- Maintain compliance

Typical use cases
Account creation
Contractor and employee onboarding
Account login
Call center fraud prevention
Credential reset
Account recovery
Delegates assignment
High-risk interactions (i.e., patient record access)
Identity database hygiene
And more...

The ID Dataweb solution

The ID Dataweb platform combines:

- Adaptive identity verification
- Behavioral analytics
- Device and credential intelligence
- AI-driven risk scoring
- Expert human insights

Together, these capabilities detect and prevent identity attacks in real time while minimizing friction for legitimate users.

Unlike traditional identity verification tools that are static and siloed, ID Dataweb delivers dynamic, multi-layered risk orchestration that adapts to evolving threats.

The cloud-native platform:

- Deploys quickly
- Integrates easily with existing identity infrastructure
- Supports low-code policy customization
- Continuously evolves with the threat landscape

Safeguarding every identity attack vector

The traditional security perimeter has disappeared. Stolen credentials are widely available, and static security controls cannot keep pace with modern threats. ID Dataweb helps healthcare providers adapt with a single platform that protects all identity attack vectors.

ID dataweb

The ID Dataweb advantage

Quick and easy implementation

- Flexible integration options
- Pre-built templates
- OpenID Connect support

Scale and adapt easily

- Low-code platform
- Easy updates
- Robust APIs and SDKs

Tailor the solution to your needs

- Industry's broadest range of authoritative identity data sources and risk signals, giving you the flexibility to tailor identity verification and adapt to any use case you require
- Full identity lifecycle coverage

One platform. One vendor. Comprehensive identity protection.

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