SOLUTION BRIEF

Safeguarding the Public Sector

Trust in government depends on identity security

Public sector organizations face growing identity-based threats as they manage broad and complex ecosystems spanning citizens, employees, contractors, and third-party partners. Rather than breaching systems directly, attackers exploit identities through phishing, credential theft, and social engineering to gain legitimate access to government services and internal systems. This enables identity fraud in citizen services—such as benefits abuse or fraudulent account changes—as well as unauthorized access to sensitive data, all while appearing as trusted users.

The challenge is compounded by legacy infrastructure, fragmented identity systems, and limited visibility across access points. Overprivileged accounts, weak deprovisioning, and inconsistent security controls across agencies further expand the attack surface. At the same time, public sector organizations must meet strict privacy and regulatory requirements while delivering accessible, low-friction digital services to citizens.

These trends highlight the need for continuous identity threat detection—capabilities that assess every digital interaction to determine in real time whether it is initiated by a legitimate user or a threat actor.

The impact of the identity crisis in the public sector

- Service **disruptions**
- Identity fraud **losses**
- **Erosion** of public trust
- Compliance **risk**

The need to move beyond credential-only authentication

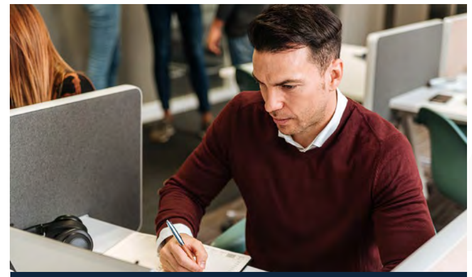
Traditional identity and access management (IAM) solutions focus on verifying whether a user is authorized to access a system or resource. However, modern attackers frequently bypass authentication controls using stolen credentials, social engineering, or AI-powered impersonation techniques.

To combat these threats, public sector agencies 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 citizens.

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

- Reduce fraud in citizen services
- Improve identity visibility
- Meet compliance requirements
- Ensure public trust

Typical use cases

- Account creation (i.e., DMV)
- Contractor and employee onboarding
- Account login
- Call center fraud prevention
- Credential reset
- Account recovery
- Age and document verification
- High-risk interactions (i.e., address change)
- 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 public sector agencies adapt with a single platform that protects all identity attack vectors.

IDdataweb

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.

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