Identity Rules

INDUSTRY BRIEF

PUBLIC SECTOR · GOVERNMENT, AGENCIES, DEFENSE.

Identity visibility across sovereign and legacy environments.

Government and defense agencies handle critical data on stacks mixing AD, mainframes, private cloud and regulated SaaS. Identity Rules consolidates everything in one sovereign model.

NIST 800-53 | ISO 27001 | LOCAL MANDATES

60%[1]	**45 : 1**[2]	**10x**[3]
of breaches start with compromised identity	non-human to human identities	faster to deploy than traditional IGA

Sources: 1) IDSA 2024. 2) CyberArk 2024. 3) Internal customer pilot data, 2025.

Typical blind spots in this sector

Officials with broad access 01

Mid- and senior-level staff with cross-system privileges. Per-official, per-mandate traceability with history.

Legacy + cloud in one model 02

AD, mainframes, SAP systems, private cloud and regulated SaaS. One identity view for auditors and CISO.

Sovereign deployment 03

On-premise on your own data center, no public-cloud dependency — same engine as the SaaS version.

Evidence for oversight 04

Reports for internal control bodies, transparency authorities and supreme audit institutions.

Identity Rules

INDUSTRY BRIEF

• OUTCOMES

What improves with Identity Rules

✓

Easier regulatory compliance

Centralized evidence for internal-control inspections and supreme audit bodies.

✓

Reduced espionage risk

Detect compromised accounts and suspicious movements before exfiltration.

✓

Data sovereignty preserved

100% on your infrastructure — no data leaves.

• WHY IDENTITY RULES

01

Speed to Value

Up to 10x faster to deploy. No long IGA projects, no months of integration, no new infrastructure stack.

02

Lower Cost & Complexity

Cuts TCO by avoiding the operational overhead of traditional IGA. Same engine for SaaS or on-prem.

03

AI-Driven Identity Intelligence

Turns identity data into actionable insights. Accelerate detection, investigation and response with a conversational copilot.

04

SOC-Ready

Immediate context on identities, accounts and privileges to speed up incident detection and response.

NHI COVERAGE

45 : 1[2]

NHIs already outnumber humans 45 to 1 — and they're where modern attacks start.

Service accounts
AD, Linux, DB, applications — who created them and who uses them today.

API keys & tokens
Inventory, owner, last used and rotation status.

Bots and CI/CD
Pipelines, automations and scripts that hold credentials.

Workload identities
IAM roles in AWS/Azure/GCP, Kubernetes service accounts.

AI agents
Anthropic, OpenAI and other LLM keys — what they can touch and with which privileges.

OAuth applications
Third-party apps with delegated access to your tenants.

READY TO DIG DEEPER

Book your Identity Risk Assessment

idrules.ai/en/industries/public-sector

Guillermo Cataneo
Founder & CEO
guillermo@idrules.ai
linkedin.com/company/identityrules