

OpenText Aviator

Use case scenarios: Government & Public Sector



Government & Public Sector made simple



Why it's hard today

- Rising cyber threats against citizen data
- Slow, manual review of citizen case file docs
- Time-heavy compliance reporting and audits
- Security protocols delay critical services
- High case volumes strain staff and delay services



Powered by OpenText

- **OpenText™ Application Security Aviator™**
- **OpenText™ Content Aviator™**



Wins for everyone

- **Cybersecurity agent:** Get AI-driven anomaly detection, vulnerability insights, and faster triage to protect sensitive government systems and data.
- **Government program manager:** Need secure, AI-assisted access to program records, policies, and citizen case files for faster, impartial outcomes.

The big payoffs

- ▶ **Strengthen cybersecurity defense**
AI-driven monitoring reduces threats and improves protection of sensitive data.
- ▶ **Trusted access to sensitive content**
Delivers insights from documents securely, ensuring compliance with strict public sector regulations.
- ▶ **Better policy & program outcomes**
Provides decision-makers with clear, data-driven insights to design policies and allocate resources.

Let's get started...

Regulatory & Compliance:

Automate compliance checks and reporting, reducing audit preparation time and ensuring standards are met.

Records & Information Management:

Secure and organize sensitive records, enabling fast, controlled access to authorized staff.

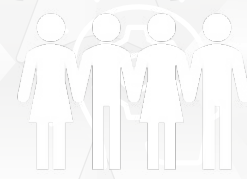
Cybersecurity & IT Security:

Detect anomalies, identify vulnerabilities, and reduce incident response times.

Case Management & Public Services:

Summarize citizen case files, extract key insights, and accelerate service delivery.

Explore Government & Public Sector scenarios



Identify program candidates and fraud red flags

I'm a government case manager turning complex claims into quick, confident decisions. With AI surfacing evidence, checking eligibility, and spotting fraud risks instantly, I speed investigations, strengthen compliance, and secure benefits programs.

Let's go



Ensure citizen benefits program app is secure

I'm a government cybersecurity agent spotting risks before they spread. With AI flagging vulnerabilities, suppressing false alarms, and logging clean audit trails, I cut noise, boost audit pass rates, and keep citizen data secure.

Let's go

Identify program candidates and fraud red flags

I'm a government case manager investigating a benefits program claim eligibility.

1 Gather the evidence

Sample prompt: "Provide a summary of the program applicant case file workspace."

Impact: All submitted documents surfaced with a clear summary.

2 Dig into the details

Sample prompt: "Tell me more."

Impact: Applicant highlights extracted for quick review.

3 Check eligibility fast

Sample prompt: "Does this applicant meet the criteria of this benefits program?"

Impact: Compares inputs to program rules and provides a clear recommendation.

4 Spot the red flags

Sample prompt: "What are the red flags connected to this benefits application or applicant?"

Impact: ID docs are cross-checked against image libraries—fraud risks flagged immediately.

5 Secure the process

Lower risk, faster investigations, and greater confidence in decisions — OpenText Aviator automates fraud detection, ensures compliance, and speeds up case resolution for government programs.

See it in action!

Next generation benefits program assistance with AI.

Unlock the possibilities:

- **Uncover fraud risks instantly**
Flag suspicious information and mismatched documents in real time.
- **Accelerate eligibility reviews**
Cut decision cycles from days to minutes.
- **Increase investigator productivity**
Automate evidence gathering and reduce manual workload.
- **Improve compliance and confidence**
Ensure consistent case decisions at scale.

Ensure citizen benefits program app is secure

I'm a government cybersecurity agent checking an application for security vulnerabilities.

1 Spot the red flags

A routine application scan uncovers a critical SQL injection vulnerability in a benefits program app that has been newly upgraded.

Action: OpenText Aviator sends a results summary and flags the issue as “Critical with remediation required.”

Impact: High-risk issues flagged instantly—no manual digging.

4 Validate the finding

After review, I confirm the finding is a false positive. OpenText Aviator updates the status automatically.

Action: OpenText Aviator changes status and logs the reason with a complete explanation.

Impact: One less issue to chase. One more step toward a clean audit.

2 Zero in on what matters

Results are reviewed and dozens of issues are caught—highlighting the most urgent and suppresses the rest.

Action: OpenText Aviator categorizes 32 critical, 20 high, and 1 low-severity issue and auto-suppresses known non-issues.

Impact: Prioritize and assign top issues fast, without being overwhelmed.

5 Close the loop

Security and dev teams resolve real issues together and track audit status in real time.

Impact: Risk reduced, compliance maintained, no security gaps missed.

3 Trace the issue

Click into a flagged issue to learn more. OpenText Aviator shows history, AI analysis, and risk status.

Action: OpenText Aviator provides a detailed rationale for marking an issue as “Not an Issue.”

Impact: Full visibility with clear trusted audit trails exposed.

6 Strengthen security posture

Stronger citizen data protection, and faster, more confident reviews — OpenText Aviator helps teams identify true vulnerabilities, cut false positives, and speed up audits.

Confidently manage risk with AI at your side.

Unlock the possibilities:

- **Heightened security**
Safety of citizen data.
- **Higher audit pass rates**
For cleaner reports and fewer false alarms.
- **Fewer post-deployment patches**
Catching risks before they reach production.
- **Shorter audit time**
Faster validations and AI-supported documentation.

See it in action!



 **Limitless**