PENTESTERRA

GOV EDITION

Penetration Testing for Air-Gapped & Sovereign Environments

Government agencies and critical infrastructure operators require absolute data sovereignty and air-gap compatibility. Pentesterra GOV Edition deploys entirely on-premises - no external connectivity, no telemetry, full control.

GOV EDITION CAPABILITIES

Full On-Premises Deployment

API server, web console, worker nodes, and scanner nodes - all running inside your data center.

→ No external connectivity required at any point

Air-Gap Support

Offline KB and CVE update channels deliverable via portable media.

→ Threat intelligence updates on your schedule

Enhanced Toolsets (GOV Contract)

Additional exploitation capabilities and advanced evasion toolsets.

→ Available under GOV contract for authorized offensive testing teams

Sovereign Data Control

All scan data, findings, and reports stay within your jurisdiction.

→ No telemetry or data leaves the installation

Audited Validation Workflows

Every scan action is logged with an immutable audit trail.

→ Compliance packages meet national and sectoral standards for authorized testing

Advanced Evasion Mode

Stealth probe strategies for testing mature defenses.

→ Adaptive payload timing, traffic shaping, IDS/WAF evasion

PENTESTERRA

GOV EDITION

WHY AGENCIES CHOOSE GOV EDITION

Nothing leaves the installation

The console, API, workers, and scanner nodes all run inside your data center.

→ No telemetry, no cloud dependency, no update channel reaching the internet unless you open one

Built for isolated and classified networks

Knowledge-base and CVE updates ship on portable media for strictly air-gapped segments.

→ Scanner nodes operate in isolated enclaves, report over a controlled, audited channel

Every action is accountable

Each scan and exploitation step is written to an immutable audit trail.

→ Compliance packages formatted for national and sectoral authorized-testing standards

WHAT GOV EDITION INCLUDES

- ✓ Full on-premises deployment - API, console, workers, and scanner nodes, no external connectivity
- ✓ Offline KB / CVE update channel deliverable via portable media on your schedule
- ✓ Sovereign data control: all scan data, findings, and reports stay within your jurisdiction
- ✓ Immutable, per-action audit trail for every scan and exploitation step
- ✓ Enhanced exploitation and evasion toolsets available under GOV contract for authorized teams
- ✓ Compliance evidence packages aligned to national and sectoral authorized-testing standards

FAQ

Can Pentesterra run in a fully air-gapped network?

Yes. The entire platform runs on-premises with no outbound connectivity. Knowledge-base and CVE updates are delivered as signed offline bundles on portable media.

Where does scan data live, and does anything phone home?

All scan data, findings, and reports remain inside your installation and your jurisdiction. GOV Edition sends no telemetry and has no usage-reporting channel.

How is authorized offensive testing kept accountable?

Every scan action and exploitation step is written to an immutable audit trail with operator attribution and timestamps. Evidence packages are formatted to meet national and sectoral standards for authorized penetration testing.

What is included under a GOV contract that is not in the standard editions?

Additional exploitation capabilities, an advanced evasion mode (adaptive payload timing, traffic shaping, IDS/WAF evasion), and the offline update tooling for air-gapped operation.

Request a GOV briefing

Full on-premises, air-gap ready, sovereign data control.

Request GOV Briefing

info@pentesterra.com · pentesterra.com/solutions/government