PENTESTERRA

ON-PREM & AIR-GAP

Vulnerability Scanning Inside Your Perimeter

Scan internal networks, AD domains, and air-gapped environments - no cloud dependency required. Scanner nodes deploy inside your infrastructure and report to a central console, keeping all sensitive data where it belongs.

3
Deployment modes: SaaS nodes, PaaS, full on-prem

0
External connectivity needed (air-gap mode)

100%
Scan data stays on your infrastructure

DEPLOYMENT OPTIONS

SaaS + Private Scanner Nodes (Most Popular)

Cloud orchestration with your own scanner nodes deployed inside the network. Scan data never leaves your perimeter.

- → Managed control plane with automatic updates
- → Deploy scanner nodes as Docker containers or VMs
- → Internal targets unreachable from the internet - fully covered
- → Unified results in the cloud dashboard

Dedicated PaaS (Single-Tenant, Enterprise)

A private, single-tenant environment in your preferred cloud region.

- → Isolated control plane - no shared infrastructure
- → Deploy scanner and worker nodes in your private cloud
- → Custom data retention and audit log policies
- → Dedicated support SLA and change-management windows

Full On-Premises (GOV Edition, Air-Gap Ready)

Every Pentesterra component - API, console, workers, scanner nodes - runs inside your data center.

- → No traffic leaves the premises - ever
- → Offline KB and CVE update channels
- → Supports air-gapped and classified environments
- → Enhanced toolsets available under GOV contract

USE CASES

Internal Network Coverage

Scan LAN segments, AD domains, and internal services that cloud-only tools can't reach.

→ Scanner nodes sit inside the network

→ Report to a central console

Regulated and Compliance-Driven Environments

Keep sensitive scan data and findings on-premises.

→ Full audit trails

→ Per-cycle evidence packages that never leave your infrastructure

Air-Gapped and Classified Networks

The GOV Edition runs with no internet dependency.

→ Update channels delivered via portable media

→ Strict connectivity controls respected

OT and Critical Infrastructure

Deploy scanner nodes with conservative scan profiles for OT segments.

→ Passive reconnaissance mode

→ Minimises probe traffic on sensitive control networks

FAQ

What's the difference between the three deployment tiers?

SaaS + private scanner nodes keeps the control plane in the cloud with your own nodes inside your network - the fastest to stand up. Dedicated PaaS gives you a fully isolated single-tenant environment with no shared infrastructure. Full on-premises (GOV Edition) runs every component - API, console, workers, scanner nodes - inside your data center with zero external connectivity.

Do scanner nodes need agents installed on the assets they scan?

No. Scanning is fully agentless. Scanner nodes are deployed once, as Docker containers or VMs, and assess the network around them - there is no host software to install on the assets being scanned.

How does an air-gapped deployment get CVE and threat-intel updates?

The GOV Edition supports offline KB and CVE update channels deliverable via portable media, so a network with strict connectivity controls never has to open an outbound connection to stay current.

Can I start with SaaS nodes and move to full on-prem later?

Yes. All three tiers run the same platform and scanner-node software, so moving from a hybrid SaaS deployment to a dedicated PaaS or full on-premises GOV Edition is a deployment-topology change, not a product migration.

Deploy inside your perimeter

SaaS nodes, dedicated PaaS, or full on-prem - your data never leaves.

Request On-Prem Demo

info@pentesterra.com · pentesterra.com/on-prem-scanning