

The app is a security control plane for the exposed edge.

AYAsec is designed to move beyond a one-off scanner: scope the organization, orchestrate multiple scan engines, normalize evidence, and turn change into an operational signal.

The expert view

- 01
Workspace-scoped visibility

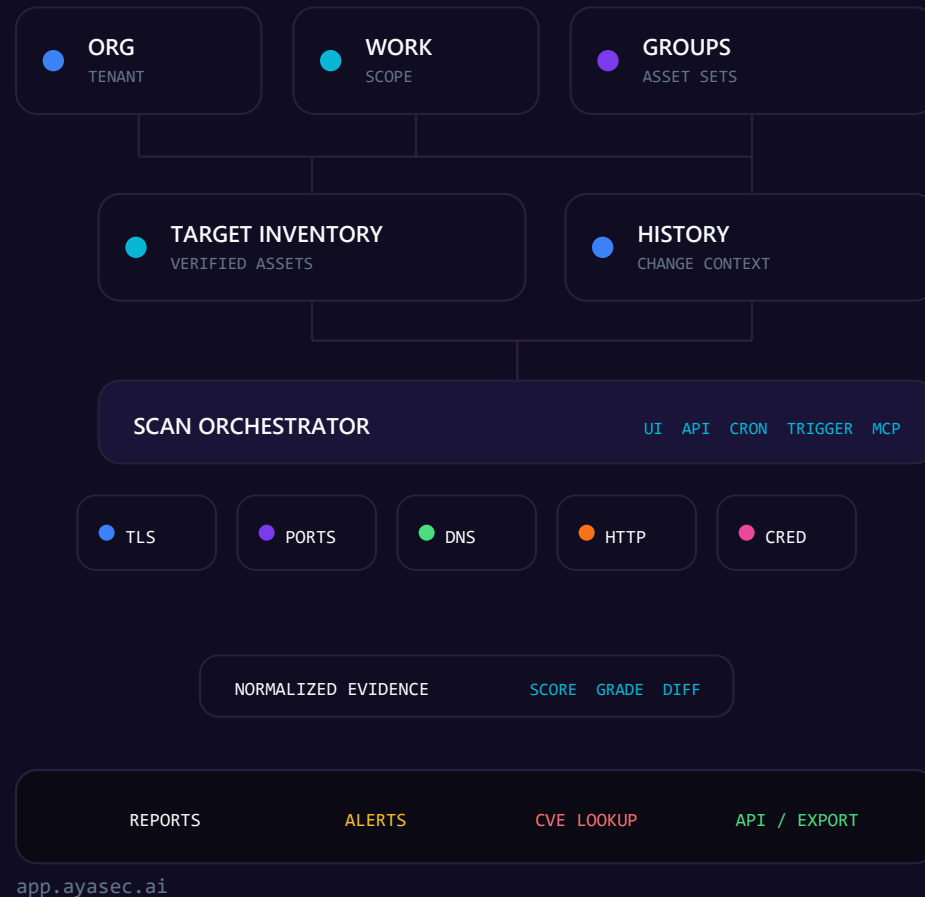
All-Workspaces views, workspace groups, target membership, and posture rollups.
- 02
Multi-engine scan orchestration

TLS, ports, DNS, HTTP, and credibility scans launched by UI, API, schedule, trigger, or MCP.
- 03
Evidence that compounds

Typed findings, scores, grades, CVEs, regression alerts, retained reports, and export paths.

INSIDE THE CONTROL PLANE

One app. Multiple layers of truth.



One asset. Five lenses. One explainable verdict.

The product does not flatten security into a single opaque number. It keeps the scan type, raw evidence, severity, CVE context, and score lineage visible all the way into the report.

● TLS Protocols, ciphers, certificates, key exchange

testssl.sh findings become typed, severity-aware evidence.

● PORTS Open services, versions, scripts, port risk

Confirmed exposure stays separate from filtered noise.

● DNS Records, providers, configuration health

Provider-backed discovery creates a defensible asset boundary.

● HTTP Passive, active, and extended profiles

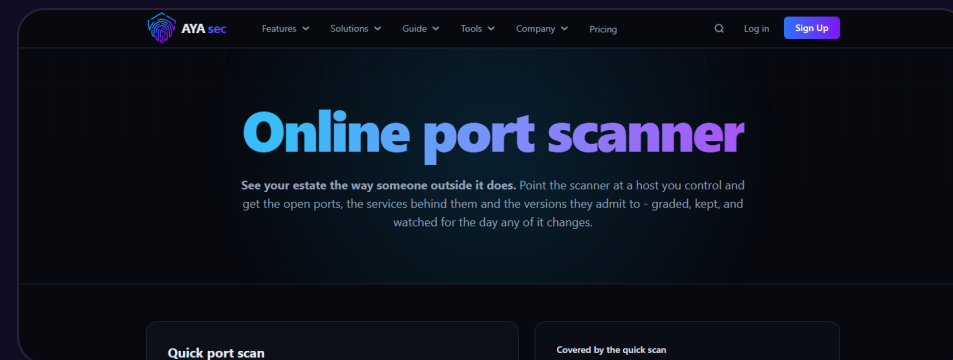
Headers, stack signals, auth-aware checks, and CVE lookup.

● CRED Domain age, reputation, blacklist status

A broader credibility lens for the same target context.

A REAL PRODUCT ENTRY POINT

The scan is only the beginning.



QUICK SCAN

HOST OWNERSHIP / SERVICE INVENTORY

HOW THE VERDICT IS BUILT



Reports synthesize scan types, calculate weighted posture, expose grade history, surface regression alerts, and connect HTTP or port evidence to CVE context.

EXPLAINABLE BY DESIGN

raw finding -> finding -> score -> action

Discovery maps the unknown edge.

The network map connects discovered hosts to shared IPs, providers, and source evidence so each result has a clear next action.

UNKNOWN ASSET MANAGEMENT

Every result has a next action.

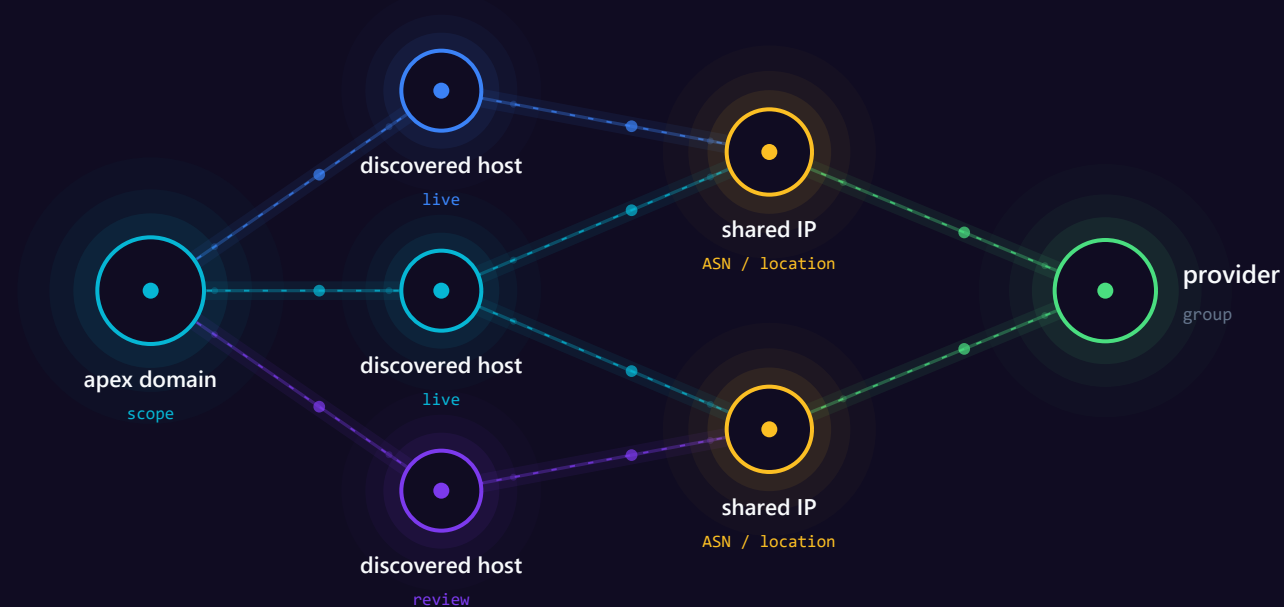
- 01 **Discover**
Collect hosts from several sources.
- 02 **Classify**
Show live state, IPs, and source evidence.
- 03 **Verify**
Review before creating an asset.
- 04 **Govern**
Create, scan, hide, or group.

NETWORK MAP

MOTION LAYER / DISCOVERY GRAPH

Watch relationships form around the asset.

Hosts, shared IPs, providers, and source evidence in one view.



SOURCE EVIDENCE

AYAsec Discovery

DNS

CT

REVERSE WHOIS

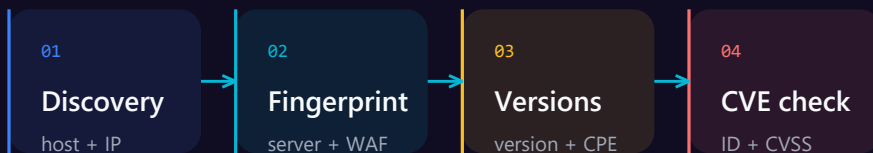
FILE IMPORT

From discovered host to CVE context.

AYAssec connects host discovery, HTTP fingerprints, open services, versions, CPEs, and CVE data so analysts can decide what needs attention and why.

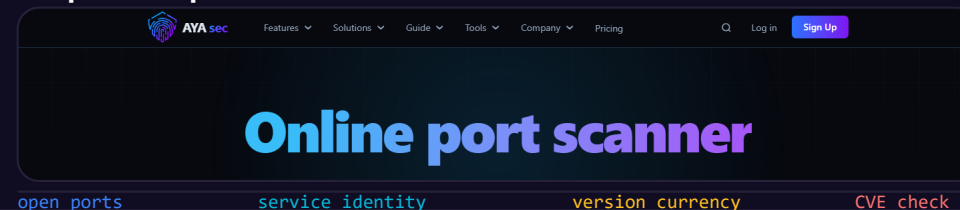
EVIDENCE PIPELINE

Keep the evidence with the finding.



SERVICE EVIDENCE

Inspect exposed services and versions.



WHAT THE ANALYST CAN MANAGE

Software versions and CVEs stay connected to the asset.

● SOFTWARE INVENTORY

Store product, version, CPE, source, confidence for each detected service.

● VERSION CONTROL

Use the detected version or enter an exact version before running a CVE check.

● CVE PRIORITY

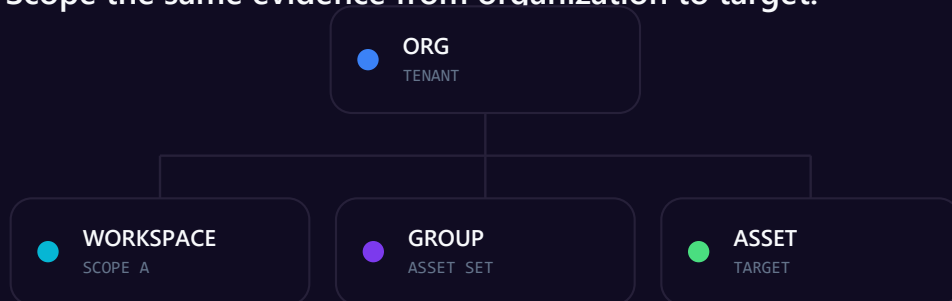
Review severity, CVSS, EPSS or KEV context, references, and the affected host.

Security teams can use one shared workflow.

The app keeps scope, access controls, and change history in one place.

WORKSPACE-AWARE MODEL

Scope the same evidence from organization to target.



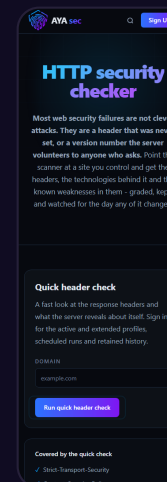
SECURITY CONTROLS

- SSO / SAML
- PASSKEYS / MFA
- CUSTOM RBAC
- AUDIT LOG
- SESSION CONTROL
- IP ALLOWLIST
- API TOKENS
- REPORT EXPORT

ONE PRODUCT, SEVERAL DELIVERY SURFACES

Use the same workflow across teams.

- WEB APP: dashboard, reports, actions
- MOBILE: parity for review and response
- PUBLIC API V1: bearer-auth, workspace-scoped
- MCP: agent-facing scan workflows
- INTEGRATIONS: Slack, Jira, Teams, Linear, Wazuh



THE INVESTOR TAKEAWAY

A scan becomes a system of record.

app.ayasec.ai

DISCOVERY AND ASSET GOVERNANCE

See the edge before the risk is visible.

AYAsec combines discovery sources, network relationships, and review decisions so teams can see what exists before they add it to inventory.

DISCOVERY INPUTS

- AYAsec Discovery
- DNS provider accounts
- Manual host file
- CT and reverse WHOIS

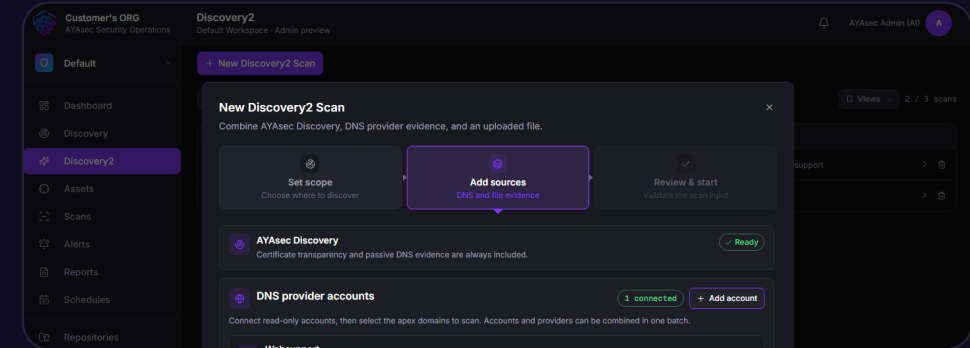
UNKNOWN ASSET MANAGEMENT

Every result has a next action.

- | | |
|---|--|
| 01 Discover
Collect hosts from several sources. | 02 Classify
Show live state, IPs, and sources. |
| 03 Verify
Review before creating an asset. | 04 Govern
Create, scan, hide, or group. |

REVIEW BEFORE ASSETS ARE CREATED

Choose what enters the workspace.



Create Scan Hide Add to group

NETWORK MAP

See how hosts are connected.

