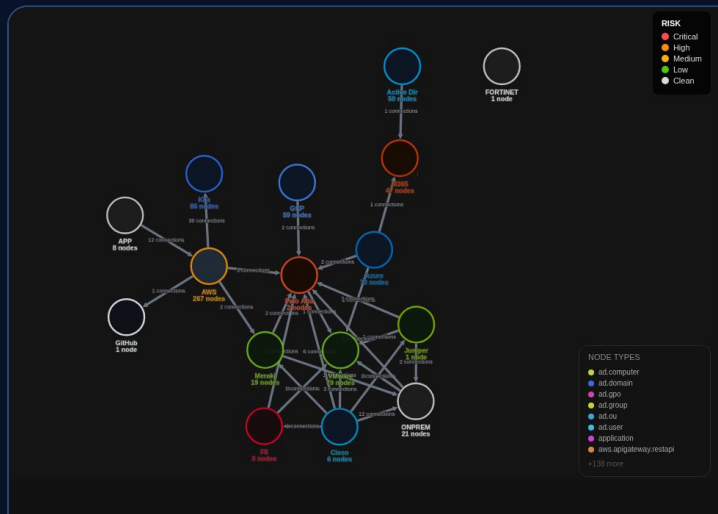


See the mission. Trace the risk. Support the assessment.

Connect discovered infrastructure to security findings, control evidence, and engineering deliverables. Give program, security, and assessment teams a shared view of what is deployed.



Actual demo topology · Sample data

INFRASTRUCTURE TO AUTHORIZATION EVIDENCE

Build the package from the environment.

Map cloud, on-premises, network, and identity relationships. Investigate potential attack paths using collected routing, security policy, and threat context.

Generate timestamped, digitally signed evidence and assessment documentation tied to discovered assets and findings.

01 / AGENCIES & PROGRAMS

Support the ATO lifecycle

Prepare SSP, SAR, SAP, and continuous monitoring materials. Carry findings into POA&Ms with owners, milestones, and evidence supporting closure.

02 / GOVERNMENT CONTRACTORS

Prepare for assessment

Support NIST 800-171 and CMMC assessment work with technical checks, questionnaires, evidence uploads, and review workflows.

03 / ARCHITECTS & INTEGRATORS

Align engineering with reality

Generate as-built diagrams and SysML v2 models from the same graph used for security analysis. Keep reviews grounded in discovered relationships.

Deploy where the mission requires.

Choose SaaS, private, or air-gapped deployment. An outbound-only relay supports connected on-premises collection. Isolated workspaces support multiple program or customer environments.

Assessment support NIST 800-53 · NIST 800-171 · FedRAMP · CMMC · DISA STIG

Workflow integrations eMASS · CSAM · ServiceNow GRC · Archer

Capabilities vary by plan, module, and deployment. Assessment materials require organizational input and review.

Explore the mission workflow →

infracast.io · info@azgardtek.com
Or start a 14-day Pro trial.

AZgardTek LLC
UEI KU5YY5CH2HV7 · CAGE 12RY3
NAICS 541512 · Patent pending