

Connect mission infrastructure to assessment evidence.

Infracast connects infrastructure discovery, attack-path analysis, and compliance workflows in one graph. Support agency authorization work, contractor assessment preparation, and systems engineering with a shared view of deployed assets.

FROM DISCOVERY TO ASSESSMENT

Discover and scope the environment

Collect cloud, network, virtualization, container, and identity data through agentless discovery, with agents for deeper host detail. Group assets by application, program, or assessment scope.

Investigate paths to mission assets

Evaluate potential attack paths against collected routing and security policy. Correlate IAM relationships and chained findings; use EPSS, CISA KEV, and asset criticality to prioritize investigation.

Assess controls and preserve evidence

Combine technical checks with questionnaires, uploaded evidence, and reviewer workflows. Keep unassessed controls visible. Signed artifacts tie assessments to specific assets, findings, and timestamps.

Manage remediation through closure

Create Plan of Action & Milestones (POA&M) items from findings. Assign responsible parties, track milestones, and link closure to supporting evidence. Integrate status with existing GRC workflows.

Generate assessment and engineering outputs

Prepare SSP, SAR, SAP, and continuous monitoring materials, plus as-built diagrams and SysML v2 models. Keep deliverables grounded in the same discovered infrastructure relationships.

DISTINCT MISSIONS. SHARED EVIDENCE.

Agencies and federal programs

Support authorization and ongoing assessment with traceable evidence, reviewable documentation, and eMASS or CSAM integration.

Government contractors and the DIB

Support NIST 800-171 and CMMC assessment preparation with technical findings, evidence collection, and human attestations. Track remediation responsibilities and assessment gaps.

Systems engineers and integrators

Connect security analysis with architecture reviews through as-built diagrams and SysML v2 export. Generate Terraform for supported core AWS resources, with unsupported resources identified for review.

DEPLOYMENT AND ACCESS

Choose SaaS, private, or air-gapped operation. Use an outbound-only relay for connected on-premises collection without inbound firewall rules. Isolated workspaces support multiple programs and customers.

CONTINUOUS VISIBILITY

Inspect configuration drift, software inventory and CVE exposure, DNS and TLS posture. Track Zero Trust maturity and map findings to MITRE ATT&CK techniques.

Assessment coverage: NIST 800-53 · NIST 800-171 · FedRAMP · CMMC · DISA STIG. Applicable controls and deliverables depend on the system and assessment scope.

Fits existing workflows: eMASS · CSAM · ServiceNow GRC · Archer · SAML/OIDC authentication · SCIM provisioning · API and webhooks.

Capabilities depend on plan, modules, and deployment. Generated materials support assessment; organizational input and assessor review remain part of the process.