

Connect infrastructure exposure to business priorities.

Infracast maps hybrid infrastructure and connects assets, identity, findings, and business-service dependencies. Help security and operations teams prioritize remediation while compliance teams build evidence from the same discovered environment.

FROM VISIBILITY TO ACTION

Connect assets to business services

Discover cloud, on-premises, network, virtualization, container, and identity resources. Group them into applications and business services with dependencies, owners, and criticality.

Prioritize exposures in context

Evaluate potential attack paths against collected routing and security policy. Correlate IAM relationships, chained findings, EPSS, CISA KEV, and asset context to focus investigation.

Move from findings to resolution

Give teams actionable fix guidance. Use remediation plans, owners, milestones, and supporting evidence to track findings through verification and closure.

Track changes that affect posture

Inspect configuration and infrastructure-code drift. Correlate software inventory and CVE exposure with discovered assets; monitor DNS security and public-facing TLS certificates.

Prepare evidence for review

Combine technical checks with questionnaires, evidence uploads, and approval workflows. Generate signed artifacts, SOC 2 evidence packages, and ISO 27001 assessment materials.

BUILT AROUND BUSINESS OUTCOMES

Explain risk in business terms

Roll findings from resources into applications and services. Show which dependencies are affected and who owns the work, so remediation priorities reflect business importance.

Healthcare

Map infrastructure supporting patient care and ePHI. Use HIPAA-oriented checks, evidence collection, and risk-analysis documentation to support security and assessment teams.

Financial services and payments

Connect exposures to critical business services and their dependencies. Support PCI DSS, SOC 2, ISO 27001, and relevant regulatory assessment workflows.

Enterprise and managed services

Give security, infrastructure, and compliance teams a common view of risk. Isolated workspaces help MSSPs manage customer environments; ServiceNow GRC and Archer integrations fit existing processes.

DEPLOY AND INTEGRATE

Choose SaaS or private deployment, with air-gapped options where required. An outbound-only relay supports connected on-premises collection. Export as-built diagrams and supported core AWS Terraform for engineering review.

Assessment coverage: SOC 2 · ISO 27001 · HIPAA · PCI DSS · NIST CSF · GDPR · NIS2 · DORA. Select frameworks and controls appropriate to your organization.

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

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